TeamViewer

1E Platform on-premises 8.1 documentation

Table of Contents

1 Tachyon 15

1.1 Introducing Tachyon 15

1.1.1 Tachyon real-time features 15

1.1.2 Tachyon Inventory and Catalog features 21

1.1.3 Tachyon Features 22

1.1.4 Tachyon Architecture 40

1.2 Quick Start 55

1.2.1 Verifying Tachyon 55

1.2.2 Prepare 55

1.2.3 Install 72

1.2.4 Configure 81

1.2.5 Use 82

1.2.6 In conclusion 84

1.2.7 Next Steps 84

1.3 Planning for Tachyon 86

1.3.1 License requirements 86

1.3.2 Architectural requirements 118

1.3.3 Windows Server requirements 157

1.3.4 Certificate requirements 173

1.3.5 Directory requirements 186

1.3.6 Email and 2FA requirements 194

1.3.7 Product integration requirements 196

1.3.8 Network requirements 204

1.3.9 1E Client requirements 226

1.4 Installing Tachyon 235

1.4.1 Preparation 235

1.4.2 Tachyon Setup 282

1.4.3 Verifying 324

1.4.4 Tachyon Server post-installation tasks 355

1.4.5 Implementing a Tachyon DMZ Server 370

1.4.6 Deploying 1E Client 394

1.4.7 Uninstalling Tachyon Platform 394

1.4.8 Tachyon Product Pack Deployment Tool 399

1.5 Upgrading Tachyon Platform 403
1.5.1 Preparing for upgrade 404
1.5.2 In-place upgrade of Tachyon 405
1.5.3 Upgrading to Tachyon Platform 411
1.5.4 After upgrading to Tachyon Platform 415
1.5.5 In-place upgrade of ActiveEfficiency Server for Nomad 417
1.5.6 Side-by-side upgrade of ActiveEfficiency Server for Nomad 419
1.5.7 In-place upgrade of ActiveEfficiency Server for Shopping 422
1.5.8 Upgrading 1E Client 424
1.5.9 Role name changes 425
1.6 Using consumer applications 429
1.6.1 Included applications 430
1.6.2 Optional applications that require a license 430
1.7 Using Settings 430
1.7.1 Settings features 430
1.7.2 Configuration Menu 445
1.7.3 Monitoring Menu 692
1.7.4 Permissions Menu 715
1.7.5 Instructions Menu 787
1.8 Introducing Inventory 792
1.8.1 Inventory features 792
1.8.2 Hardware 794
1.8.3 Software Inventory 799
1.8.4 Manage associations 815
1.8.5 User Summary 825
1.8.6 The 1E Catalog 826
1.8.7 AI Powered Auto-curation 850
1.8.8 Configuring 1E Catalog connection to 1E Cloud 863
1.8.9 Rebuilding the 1E Catalog 875
1.9 Troubleshooting 880
1.9.1 1E Support contact details 880
1.9.2 The technical support process 881
1.9.3 Log files 883
1.9.4 Known issues 884
1.9.5 Server installation issues 936

1.9.6 Client issues 946
1.10 Extending Tachyon 946
1.10.1 The 1E Tachyon Toolkit 946
1.10.2 Using Tachyon in Configuration Manager 960
1.10.3 Configuring NightWatchman Online Status 972
1.10.4 Installing TIMS 972
1.10.5 Setting up custom Tachyon Instructions for the first time 972
1.10.6 1E ITSM Connect 973
1.11 Reference 976
1.11.1 Supported Platforms 976
1.11.2 Communication Ports 993
1.11.3 1E Companion Products 1017
1.11.4 Device View 1022
1.11.5 Log files 1067
1.11.6 Scripts 1074
1.11.7 Server installers 1101
1.11.8 Tachyon Server reference 1139
1.11.9 Client reference 1178
1.11.10 Settings reference 1178
1.11.11 Inventory reference 1200
1.11.12 Tachyon Product Packs reference 1232
1.11.13 Tachyon release information 1602
1.11.14 Glossary 1639
1.12 Increasing Azure SQL Server Performance 1663
2 1E Client 1663
2.1 Introducing 1E Client 1663
2.1.1 Deployment 1665
2.1.2 Supported Platforms 1665
2.1.3 Constraints of Legacy OS 1667
2.2 Planning for 1E Client 1668
2.2.1 Common client requirements 1670
2.2.2 Tachyon platform client requirements 1681
2.2.3 Nomad client requirements 1690
2.2.4 PXE Everywhere client requirements 1692
2.2.5 Shopping client requirements 1693

2.2.6 WakeUp client requirements 1695
2.3 Installing 1E Client 1697
2.3.1 Deploying 1E Client on Windows 1697
2.3.2 Deploying 1E Client on macOS 1730
2.3.3 Deploying 1E Client on Linux 1739
2.3.4 Deploying 1E Client on Solaris 1744
2.3.5 Reconfiguring 1E Client 1744
2.3.6 Verifying 1752
2.4 Upgrading 1E Client 1753
2.4.1 1E Client versions 1754
2.4.2 Upgrading legacy 1E agents to 1E Client 8.1 1754
2.5 Troubleshooting 1757
2.5.1 1E Support contact details 1758
2.5.2 The technical support process 1758
2.5.3 Client issues 1760
2.5.4 Known issues 1768
2.6 Reference 1782
2.6.1 1E Client configuration settings and installer properties 1782
2.6.2 1E Client command-line parameters 1960
2.6.3 Log files 1963
2.6.4 1E Client release information 1966
3 1E Client Deployment Assistant 1988
3.1 Introducing 1E Client Deployment Assistant 1988
3.2 Implementing 1989
3.2.1 Preparation 1989
3.2.2 Running the wizard 1997
3.2.3 Configuration Manager objects 2028
3.2.4 Advanced configuration 2032
3.2.5 Using client patch files with CDA 2036
3.3 Troubleshooting 2037
3.3.1 1E Support contact details 2037
3.3.2 The technical support process 2038
3.3.3 Known issues 2040
3.4 Reference 2041
3.4.1 Supported Platforms 2041

3.4.2 Installer properties 2047
3.4.3 1E Client Deployment Assistant release information 2061
4 Tachyon Explorer 2068
4.1 Introducing Tachyon Explorer 2068
4.1.1 Tachyon Explorer features 2069
4.2 Planning for Tachyon platform 2072
4.3 Installing Tachyon Explorer 2072
4.3.1 Tachyon Product Pack Deployment Tool 2072
4.3.2 Verifying 2077
4.4 Using Tachyon Explorer 2077
4.4.1 Introducing Explorer 2078
4.4.2 Explorer Features 2081
4.4.3 ExplorerHome page, questions and responses 2084
4.4.4 Instructions 2100
4.4.5 The action approval workflow 2117
4.4.6 Tagging client devices 2121
4.4.7 Using Device Criticality 2132
4.4.8 Using Location 2133
4.4.9 Exporting data from Explorer 2134
4.4.10 Investigating Devices 2137
4.4.11 Tachyon Activity Record 2179
4.4.12 Tachyon Quarantine 2182
4.5 Troubleshooting 2184
4.5.1 Troubleshooting table 2184
4.5.2 1E Support contact details 2185
4.5.3 The technical support process 2186
4.5.4 Known issues 2188
4.6 Reference 2189
4.6.1 Log files 2189
4.6.2 Explorer reference 2195
4.6.3 Glossary 2208
5 Tachyon Experience 2231
5.1 Introducing Tachyon Experience 2232
5.1.1 Tachyon Experience Features 2232
5.2 Implementing Tachyon Experience 2234

5.2.1 Requirements 2235
5.2.2 Installing Experience 2236
5.2.3 Verifying 2237
5.3 Using Tachyon Experience 2238
5.3.1 Personas 2239
5.3.2 Monitoring and investigating enterprise-wide experience 2239
5.3.3 Focusing on specific device experience 2242
5.3.4 Investigating enterprise-wide software experience 2251
5.3.5 Getting feedback via Sentiment Surveys 2259
5.3.6 Getting feedback via Info Surveys 2275
5.3.7 Investigating software crashes 2287
5.3.8 Broadcasting information via Announcements 2294
5.3.9 Investigating Network Performance 2305
5.3.10 Investigating Boot and Login Performance 2310
5.3.11 Creating your own dashboard 2313
5.3.12 Adding metrics to a dashboard 2316
5.4 Troubleshooting 2320
5.4.1 1E Support contact details 2321
5.4.2 The technical support process 2321
5.4.3 Configuration issues 2323
5.4.4 Known issues 2325
5.5 Reference 2328
5.5.1 Page reference 2328
5.5.2 Score reference 2415
5.5.3 Experience Product Packs reference 2434
5.5.4 Glossary 2434
5.5.5 Tachyon Experience release information 2440
6 Tachyon Dashboards 2446
6.1 Introducing Tachyon Dashboards 2446
6.1.1 Exec Dashboard 2447
6.2 Implementing Tachyon Dashboards 2448
6.2.1 Requirements 2448
6.2.2 Installing and upgrading 2455
6.2.3 Verifying 2459
6.3 Using Tachyon Dashboards 2462

6.3.1 Assessing how Tachyon contributes to company DEX performance 2462
6.4 Troubleshooting 2470
6.4.1 1E Support contact details 2470
6.4.2 Known issues 2473
6.4.3 Implementation Issues 2474
6.5 Reference 2475
6.5.1 Log files 2475
6.5.2 Page reference 2475
6.5.3 Dashboards Product Packs reference 2481
6.5.4 Glossary 2482
7 1E Patch Success 2488
7.1 Introducing Patch Success 2489
7.1.1 Patch Success features 2489
7.2 Quick Start 2490
7.2.1 Connector Usage Recommendations for Patch success customers 2490
7.3 Implementing Patch Success 2492
7.3.1 Requirements 2492
7.3.2 Configuring Patch Success 2495
7.3.3 Verifying 2959
7.4 Using Patch Success 2965
7.4.1 Title and filter bars 2965
7.4.2 Patch Success Overview page 2973
7.4.3 Patch pages 2979
7.4.4 Device pages 2983
7.4.5 Monitoring pages 2986
7.4.6 Reporting and successfully patching a management group for a single KB - tutorial 2992
7.5 Troubleshooting 2999
7.5.1 1E Support contact details 2999
7.5.2 The technical support process 3000
7.5.3 Known Issues 3002
7.6 Reference 3004
7.6.1 Patch Success release information 3004
7.6.2 1E Companion Products 3006
7.6.3 1E Patch Success product pack 3008
8 Guaranteed State 3011

8.1 Introducing Guaranteed State 3011
8.1.1 Guaranteed State Concepts 3011
8.1.2 Guaranteed State Features 3016
8.2 Implementing Guaranteed State 3018
8.2.1 Design Considerations 3018
8.2.2 Requirements 3019
8.2.3 Preparation 3019
8.2.4 Installing and upgrading 3019
8.2.5 Uploading Integrated Product Packs 3019
8.2.6 Configuring Guaranteed State 3021
8.2.7 Verifying 3022
8.3 Using Guaranteed State 3022
8.3.1 Integrated Product Packs 3022
8.3.2 Deploying a Policy 3030
8.3.3 Defining your own policy 3038
8.3.4 Using Explorer to investigate devices in Guaranteed State 3043
8.3.5 Guaranteed State Overview page 3044
8.3.6 Administration menu 3053
8.4 Troubleshooting 3087
8.4.1 Known issues 3087
9 1E Content Distribution 3090
9.1 Introducing Nomad 3090
9.1.1 New features in Nomad 3090
9.1.2 Nomad overview 3091
9.1.3 Nomad fundamentals 3094
9.2 Implementing Nomad 3108
9.2.1 Design Considerations 3108
9.2.2 Requirements 3130
9.2.3 Preparation 3133
9.2.4 Installing Nomad 3147
9.2.5 Upgrading Nomad 3189
9.2.6 Verifying 3209
9.3 Using Nomad 3211
9.3.1 Deploying software with Configuration Manager 3211
9.3.2 Deploying software in large networks 3220

9.3.3 Deploying software updates using Configuration Manager 3229
9.3.4 Deploying updates for Office 365 3238
9.3.5 Using Nomad with Operating System Deployment OSD 3244
9.3.6 Monitoring Nomad 3258
9.3.7 Ensuring Nomad is secure 3267
9.4 Nomad features 3274
9.4.1 Nomad features and concepts 3275
9.4.2 Content Distribution 3279
9.4.3 OS Deployment 3394
9.4.4 Nomad Management 3400
9.4.5 Client Health 3419
9.5 Troubleshooting 3421
9.5.1 1E Support contact details 3421
9.5.2 The technical support process 3421
9.5.3 The technical support process 3422
9.5.4 Log files 3423
9.5.5 Known issues 3424
9.5.6 Basic Nomad behavior in a simple environment 3453
9.5.7 Resolving common issues 3460
9.5.8 Resolving content integrity (hash checks) issues 3462
9.5.9 Reducing election notifications in Nomad log 3463
9.5.10 Resolving hard link issues 3464
9.5.11 Resolving Nomad peer election issues 3465
9.5.12 Resolving Peer Backup Assistant (PBA) issues 3466
9.5.13 Resolving peer copy over HTTP or HTTPS issues 3469
9.5.14 Resolving Remote Differential Compression (RDC) issues 3470
9.5.15 Resolving slow content transfer issues 3474
9.5.16 Resolving SoftwareUpdate metadata validation 3475
9.5.17 Resolving Configuration Manager Pre-caching and Nomad Pause error 3477
9.6 Reference 3478
9.6.1 Content Distribution Web API 3478
9.6.2 Nomad app 3485
9.6.3 Nomad tools 3574
9.6.4 Nomad OS Deployment task sequence actions 3594
9.6.5 Supported Platforms 3645

9.6.6 1E Companion Products 3654
9.6.7 Communication ports 3655
9.6.8 Log files 3664
9.6.9 Nomad architecture 3665
9.6.10 Nomad command-line switches 3671
9.6.11 Nomad installer properties 3691
9.6.12 Nomad registry values 3777
9.6.13 Nomad return codes 3882
9.6.14 FIPS compliant communication encryption 3884
9.6.15 Glossary 3885
9.6.16 Nomad Product Packs reference 3909
9.6.17 Nomad release information 3955
10 AppClarity 3974
10.1 Introducing AppClarity 3975
10.1.1 AppClarity Features 3975
10.1.2 AppClarity Architecture 3976
10.2 Implementing AppClarity 3976
10.2.1 Design considerations 3976
10.2.2 Requirements 3996
10.2.3 Preparation 3997
10.2.4 Installing and upgrading 3999
10.2.5 Verifying 4002
10.3 Configuring AppClarity 4008
10.3.1 Tachyon roles for configuring AppClarity 4008
10.3.2 Connectors page 4008
10.3.3 Repositories page 4014
10.3.4 SCCM Uninstall Provider 4017
10.3.5 Deploying Software Reclaimer 4018
10.4 Using AppClarity 4041
10.4.1 AppClarity user roles 4041
10.4.2 Running your first Compliance License Summary 4053
10.4.3 Viewing software install counts across all devices 4062
10.4.4 Viewing product usage 4066
10.4.5 Viewing product compliance 4069
10.4.6 Viewing your effective license position 4070

10.4.7 Creating a license entitlement 4072
10.4.8 Creating and linking a maintenance entitlement 4083
10.4.9 Creating an entitlement using a SKU 4087
10.4.10 Creating an agreement entitlement 4090
10.4.11 Importing entitlements from a folder 4094
10.4.12 Managing compliance for user-based licenses 4098
10.4.13 Calculating license demand 4104
10.4.14 Excluding devices from License Demand Calculation using Management Groups 4108
10.4.15 Reclaiming a product based on its usage 4114
10.4.16 Stopping a reclaim policy 4130
10.4.17 Viewing the software reclaim reports 4132
10.4.18 Scheduling AppClarity reports 4135
10.5 Troubleshooting 4136
10.5.1 1E Support contact details 4137
10.5.2 The technical support process 4137
10.5.3 Known Issues 4141
10.6 Reference 4147
10.6.1 Supported Platforms 4147
10.6.2 1E Companion Products 4150
10.6.3 Communication Ports 4151
10.6.4 Installer properties 4151
10.6.5 AppClarity page reference 4152
10.6.6 Usage categories 4344
10.6.7 Entitlement import files 4344
10.6.8 AppClarity release information 4364
10.6.9 Glossary 4373
11 Application Migration 4408
11.1 Introducing Application Migration 4408
11.2 Implementing Application Migration 4409
11.2.1 Design Considerations 4409
11.2.2 Requirements 4413
11.2.3 Installation 4419
11.2.4 Post-install configuration 4420
11.2.5 Upgrading Application Migration 4430
11.3 Using Application Migration 4432

11.3.1 Getting started with Application Migration 4432
11.3.2 Using the Installations page 4436
11.3.3 Managing migration rules 4441
11.3.4 Managing product exclusions 4470
11.3.5 Previewing post-OS migration application states 4473
11.3.6 Role Based Application Sets 4483
11.3.7 Setting the Install Sequence for applications 4495
11.3.8 Using Application Migration in a task sequence 4502
11.4 Troubleshooting 4517
11.4.1 The technical support process 4517
11.4.2 Known issues 4519
11.5 Reference 4523
11.5.1 Installer properties 4523
11.5.2 1E task sequence actions 4525
12 PXE Everywhere 4526
12.1 Introducing PXE Everywhere 4526
12.1.1 Support for networks with DHCP Snooping enabled 4527
12.1.2 PXE Everywhere components 4528
12.1.3 How it works 4528
12.2 Implementing PXE Everywhere 4530
12.2.1 Design Considerations 4530
12.2.2 Requirements 4535
12.2.3 Installing and Upgrading 4554
12.2.4 Verifying 4573
12.3 Using PXE Everywhere 4579
12.3.1 Preparing and deploying 1E PXE Everywhere boot images 4579
12.3.2 Deploying Microsoft ADK files 4591
12.4 Troubleshooting 4594
12.4.1 1E Support contact details 4595
12.4.2 The technical support process 4596
12.4.3 MSI Installer log 4597
12.4.4 Known issues 4598
12.4.5 Installation issues 4603
12.4.6 Resolving PXE Everywhere Agent issues 4604
12.5 Reference 4606

12.5.1 Supported Platforms 4606
12.5.2 Communication Ports 4610
12.5.3 PXE Everywhere Central installer properties 4623
12.5.4 PXE Everywhere Responder settings 4624
12.5.5 PXE Everywhere Agent settings 4632
12.5.6 PXE Everywhere tools 4644
12.5.7 PXE Everywhere release information 4648
12.5.8 Log files 4654

1 Tachyon

Tachyon platform is a systems management tool based on the concept that a device is aware of its own current state more accurately than any centrally held repository. Also, if you can query the device directly then the need to store masses of data becomes unnecessary.

1.1 Introducing Tachyon

An overview of the Tachyon is presented; what it does and how it can benefit your organization.

1.1.1 Tachyon real-time features

1.1.1.1 Introduction

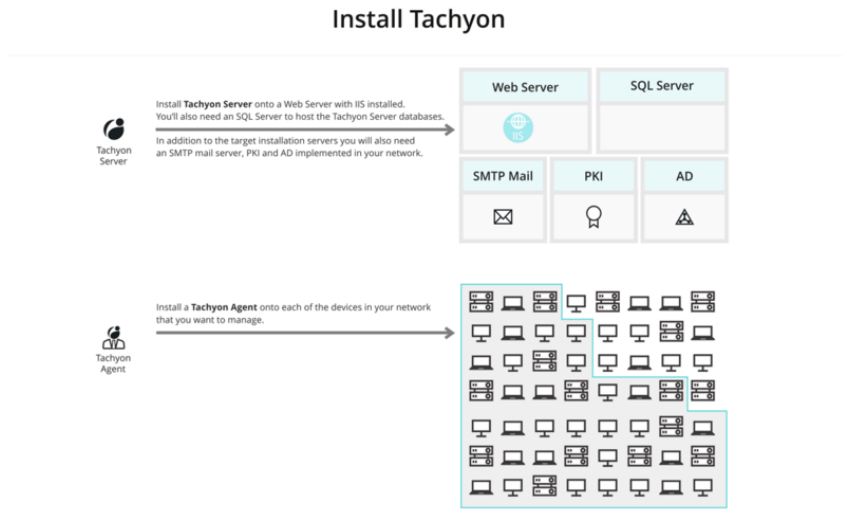
Tachyon is a systems management tool that turns the traditional systems management model on its head. It is based on the concept that a device is aware of its own current state more accurately than any centrally held repository. Also, if you can query the device directly then the need to store masses of data becomes unnecessary.

1.1.1.2 Implement Tachyon

To implement Tachyon you need to design, install and verify your installation. Full details can be found in Planning for Tachyon.

Broadly speaking, installation is done in two steps:

1. Install Tachyon onto an appropriate Windows server with IIS installed.
2. Install a 1E Client onto each of the devices you want to manage.



1.1.1.3 Add Instruction Definitions to Tachyon

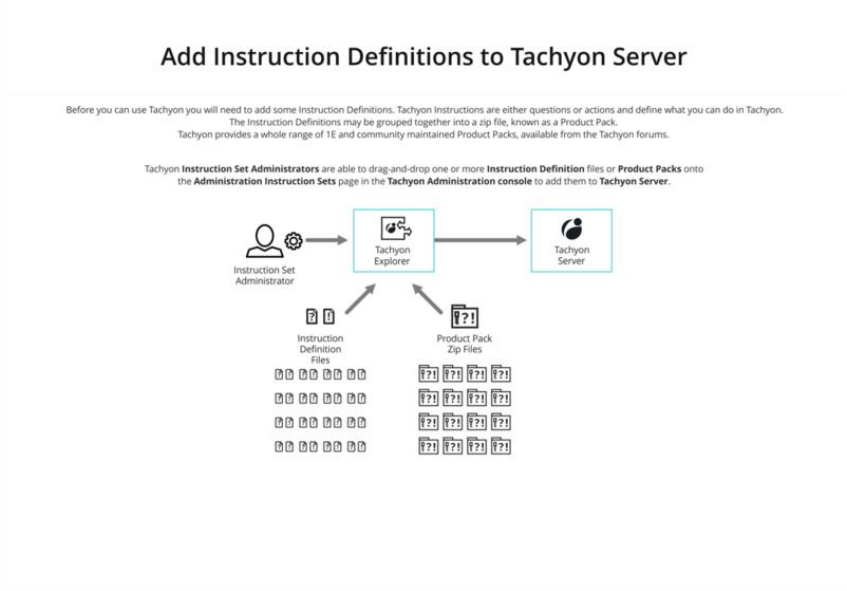
Using the Tachyon administration console, import Instruction Definitions into Tachyon. An Instruction Set Administrator can load Instructions by dragging and dropping one or more Instruction Definition files onto the interface. The Instruction Definitions may also be grouped together in a zip file, known as a Product Pack, and added in a single operation.

When uploaded, the administrator then assigns the instructions to one or more Instruction Sets. The administrator also assigns permissions to Instruction Sets to control who can ask questions, and perform and approve actions, as well as assigning Management Groups to control which devices the instructions can be sent to.

1E provides a number of Product Pack zip files available in the **Tachyon Platform Product Packs** zip (available on the 1E Support Portal) and from the Tachyon Exchange (https://exchange.1e.com/). Each Product Pack contains a related collection of Instruction Definitions.

Full details of adding Instruction Definitions can be found in Instruction sets page.

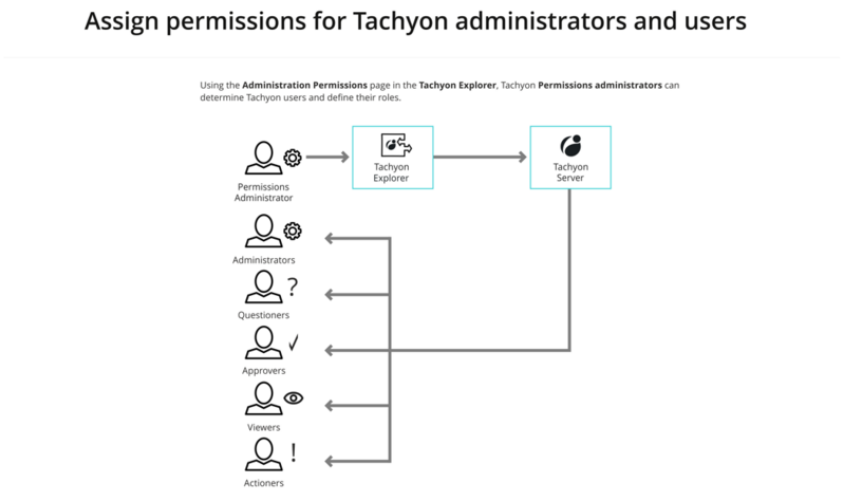
Integrated Product Packs provide ready-made policies for Guaranteed State but also include instructions. To upload these, please refer to -Uploading Integrated Product Packs.



1.1.1.4 Assign permissions for Tachyon administrators and users

Following on from installation you then assign permissions to particular users corresponding to the Tachyon administration roles and instruction set questioner, actioner, approver, and viewer roles.

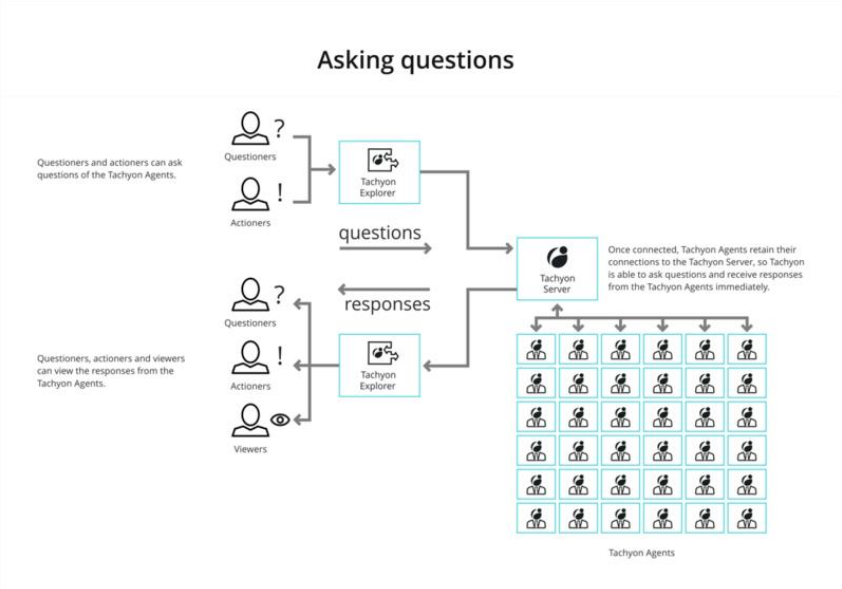
Full details of assigning permissions for Tachyon administrators and users can be found on the Users and Groups page and the Roles page.



1.1.1.5 Sending instructions - asking questions and performing actions

Using Tachyon Explorer questions can be asked of Tachyon client devices by users with the questioner or actioner roles. The responses can be viewed by viewers, questioners and actioners.

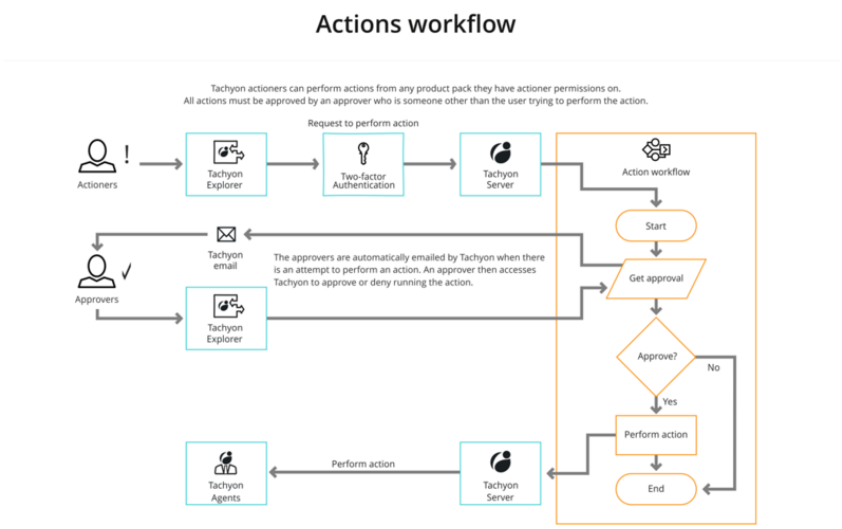
Details on asking questions can be found in [ExplorerHome page, questions and responses](#).



Using Tachyon Explorer, actions can be performed on Tachyon client devices by users with the actioner role on an instruction set, subject to the following:

- They will need to enter their password
- If the action has been configured to use two-factor authentication, they will need to enter the authentication code
- They will need the approval of someone other than themselves with an approver role.

Details on performing actions and the approval workflow can be found in The action approval workflow.

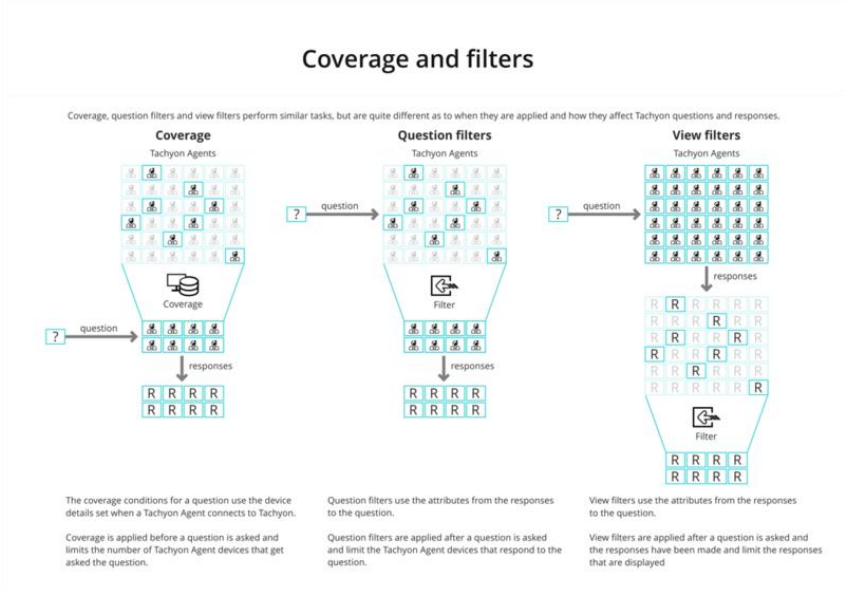


1.1.1.6 Coverage and filters

You can use coverage and filters to reduce the amount of network traffic caused by asking a question. They are also useful in reducing the amount of data that is presented to Tachyon users. Tachyon provides coverage, question filters, and view filters.

- Coverage is applied before a question is asked and reduces how many client devices get asked the question. Coverage uses the device properties that are sent by a client when it connects to Tachyon.
- Question filters are applied to the client after the question has been asked and use the attributes from the question responses to determine whether the client should send the response.
- View filters are applied in the Tachyon Explorer after the responses have been sent and reduce the responses that are displayed.

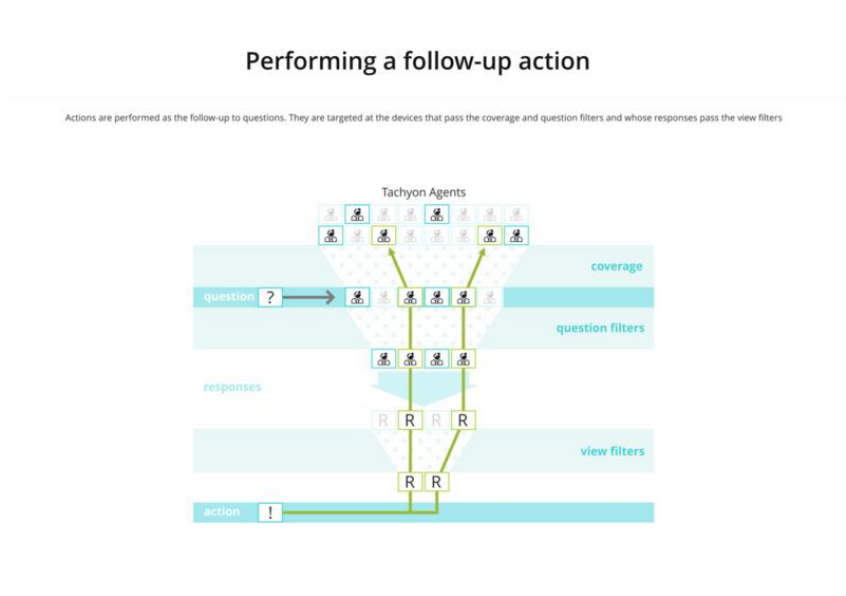
For more information see Coverage, question filters and view filters.



1.1.1.7 Performing follow-up questions and actions

You can perform a follow-up question or action after a previous question has been asked. Each follow-up causes the previous questions to be re-asked to detect any real-time changes. Any coverage, question, and view filters are applied to the responses, as shown.

For more information see Refining responses with follow-up questions and Performing an action - tutorial.

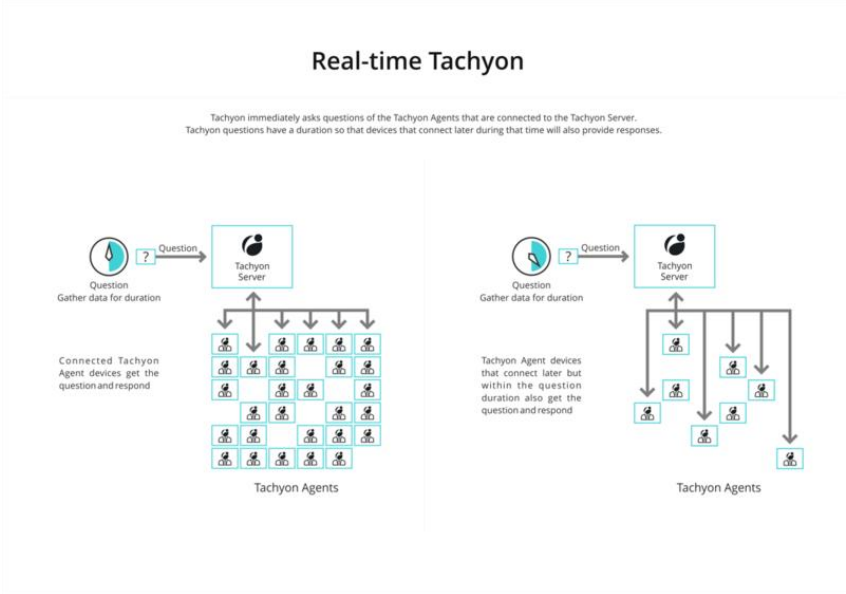


1.1.1.8 Real-time Tachyon

Tachyon works in real-time, so not all the devices may be connected at the time a question is asked. Tachyon questions have a configurable duration that they will gather data for - allowing devices that connect later, within the **gather data for** duration, to respond.

Questions also have a configurable **keep answers for** duration - given that the answers from a live network can potentially get stale quickly, and Tachyon questions are fast enough that you can simply ask again rather than relying on old answers.

Details on asking questions can be found in ExplorerHome page, questions and responses.



1.1.1.9 Basic Instruction flow

The picture shows the basic flow of Tachyon Instructions between its components. For simplicity, the workflow section, where the Instruction is authenticated and verified, has been omitted.

The basic Instruction flow is:

1. A Tachyon Consumer initiates an Instruction using a request to the Consumer API.
2. The Consumer API stores the Instruction in the Tachyon Master database.
3. The Instruction is authenticated and verified by the Workflow and becomes ready for processing by the Core.
4. The Core relays the Instruction to the Switch.
5. The Switch transmits the Instruction to the appropriate connected Tachyon clients.
6. The Tachyon clients process the Instruction on their devices and produce responses in real-time.
7. The Tachyon clients pass the responses to the Switch, intelligently minimizing bandwidth utilization.
8. The Switch relays the responses to the Core.
9. The Core stores the responses in the Responses database while intelligently minimizing the amount of data and maximizing the speed of retrieval.
10. The Consumer API fetches the responses from the Responses database and makes them available to the Consumer.

Tachyon architecture has been designed for the sending of Instructions and gathering of responses for thousands of devices in seconds.

1.1.1.10 Content delivery

To maximize the speed of Instruction delivery and gathering responses from its clients, Tachyon keeps the size of Instructions to a minimum fixed size. If you want to run an Instruction that requires a script or other sizable resource in order to carry out its functionality, this is made available using an alternative mechanism using the Background Channel.

The first step in the content delivery process actually occurs before the Instruction is used when the Instruction containing the resource is first loaded into Tachyon:

1. An Instruction Set Administrator loads an Instruction definition with an associated script, or other sizable resource, into Tachyon using Explorer.
2. The Consumer API copies the script or resource to the Background Channel.
3. The Consumer API stores the Instruction and resource in the Tachyon Master database.

After the Instruction has been loaded into Tachyon:

1. A suitably permissioned Tachyon Questioner or Actioner requests the Instruction.
2. The Instruction request flows through the Tachyon components as normal.
3. This time, when the Instruction gets to clients, they know that they need to download the Instruction's script or resource in order to process the Instruction.
4. The script or resource is downloaded from the Background Channel using HTTPS.
5. If Nomad is installed on the client device it will be used for the download, providing all its download optimization features to speed up the process.
6. Once the script or resource file has been downloaded to the client device it processes the Instruction and returns the responses made as a result of using the script or resource.
7. The responses flow back through the Tachyon components as normal.

1.1.2 Tachyon Inventory and Catalog features

1.1.2.1 Introduction

Tachyon is a systems management tool that turns the traditional systems management model on its head. It is based on the concept that a device is aware of its own current state more accurately than any centrally held repository. Also if you can query the device directly then the need to store masses of data becomes unnecessary.

Inventory features

Inventory captures data from different sources, then consolidates, normalizes, and stores it in Inventory repositories.

AI Powered Auto-curation

Describes the AI Powered Auto-curation feature that improves software inventory results.

Manage associations

Applications and Packages in Configuration Manager are identified by a name and optionally publisher and version arbitrarily determined by the Configuration Manager administrator that created them. Tachyon uses a standard Vendor, Title, Version, and Edition format to identify applications.

The **Manage Associations** section of Inventory enables an administrator to effectively normalize the Applications and Packages imported from Configuration Manager by associating them with a Vendor, Title, Version, and Edition defined in the 1E Catalog. These associations are then used to define migration rules in Introducing Application Migration and reclaim rules in Introducing AppClarity.

1E Catalog is a prerequisite for installing the SLA components of Tachyon. SLA uses 1E Catalog to normalize or match source inventory information, for example, software devices and processors.

1E Catalog allows you to:

- Have a consistent view of your estate
- Uniquely identify software deployed in your estate
- Identify device types (laptop, desktop, virtual machine), operating system, device family, device manufacturer, and maximum number of processors
- Normalize processor information like processor model, processor family, vendor name, and number of cores of processors running on your devices
- Define and apply bundling rules to identify suites and their components
- Define and apply entitlement rights, such as version upgrade/downgrade, edition downgrade, and software assurance rights which are used during license demand and compliance calculations
- Apply autofill entitlement information using software SKU.

1.1.3 Tachyon Features

An overview of Tachyon features and enhancements. The page provides a brief overview of each feature and links to other pages with more detail.

1.1.3.1 Installation

Tachyon provides a setup wizard that installs all the separate parts of the Tachyon platform using their individual installers. It is used to validate a server prior to running the installers, and supports a range of configurations as described in Tachyon configuration options.

1E Client installers are also provided for Windows and packages for supported non-Windows OS.

Introducing 1E Client Deployment Assistant is a wizard that assists Configuration Manager with deployment of 1E Client and other 1E Client agents, guiding you through common settings for clients and deployments.

1.1.3.2 Tachyon Explorer features

Explorer gives you the ability to investigate, remediate issues and manage operations across all your endpoints in real time. For more information, please refer to Using Tachyon Explorer.

Here's an overview of the features available in the Explorer application.

1.1.3.2.1 Questions, actions and their responses

Explorer lets you directly question connected devices to retrieve responses, run actions, and get real-time information from them. The Explorer front-end capabilities ensure fast querying, investigation, and remediation.

The questions, responses and actions feature includes:

- Graphical display of response information
- Instruction impact assessment
- Response history.

Note

For more information on Instructions and their responses, please refer to:

- ExplorerHome page, questions and responses
- Question parameters
- Instructions
- History.

1.1.3.2.2 Exporting data from Tachyon Explorer

Results visible in Explorer can be exported to files containing comma-separated values (CSV) or, in the case of the **Export all** option on the instruction response page, tab-separated values (TSV), and results can be marked for export at the point of asking a question to automate the process. Explorer lets you export the data on a number of pages to CSV files:

- Instruction history
- Responses - you can export a single page or all results once the Instruction has finished gathering responses - these can then be used for auditing purposes or to drive external programs
- Drill-down responses
- Device information.

Note

For more information on exporting data from Explorer, please refer to:

- Exporting data from Explorer.

1.1.3.2.3 Coverage, question filters, view filters and follow-on instructions

Questions and responses can be tailored to focus on specific ranges of devices through the use of coverage and filters:

- Coverage acts first to let you restrict the devices that will be asked a given question

- Question filters act before devices have responded to narrow the responses that are sent
- View filters act after the responses have been sent to focus the responses presented to the user and to determine the input into the follow-on instructions

The responses to initial questions can be further refined by asking follow-on questions or actions, allowing questioners and actioners to focus in on the results they want to see.

Note

For more information on coverage, question filters, view filters and follow-on instructions, please refer to:

- Coverage, question filters and view filters
- Limiting coverage using a Management group - tutorial
- Refining responses with follow-up questions.

1.1.3.2.4 Approval workflow

To enhance the safety of running actions in the Tachyon system, there is an approval workflow that ensures that every Tachyon action requires the approval of designated approvers before it can be run. To make it even safer, someone with approval permissions cannot approve their own action.

When an attempt is made to run an action, the Tachyon approval workflow sends an email and a notification to all the approvers associated with the action. Any of the approvers may approve or reject the request to run the action.

Note

For more information on the Approval workflow, please refer to:

- The action approval workflow
- Performing an action - tutorial.

1.1.3.2.5 Authentication

Users must provide their user credentials when attempting to run an action, this prevents unauthorized access by a third party attempting to make use of an unattended computer.

Actions can also be configured to require two-factor authentication. This is where the user attempting to run an action is challenged to enter a unique, one-time authorization code that has been sent to them by an alternative method such as email or a registered mobile.

Note

For more information on authentication, please refer to:

- Two-factor authentication.

1.1.3.2.6 Task-based organization for accessing and scheduling instructions

Tachyon provides a way of accessing the questions and actions that is organized around the way that network administrators typically interact with their network. This interface also lets you run the Instruction using a schedule.

The **Explorer→Instructions→Tasks** page in Explorer provides a structured view of the instructions defined in the Product Pack. It also lets you schedule the tasks so they can be run in the future or according to a particular schedule.

1.1.3.2.7 Using task groups

The benefit of using **Tasks** lies in the task group structure that is defined in the Product Pack. It is this structure that enables you to focus in on specific task areas to find the particular instruction that you want.

For example you may be interested in instructions related to particular software vendor's products. Depending on the Instructions that you have uploaded to your Tachyon system you may see the following structure:

- At the top-level there is a **Software Vendors** task group whose children are **1E** and **Microsoft**.
- Underneath the **1E** task group there is a **Tachyon** group that contains **Configuration**, **Diagnostics** and **Verification** groups as well as a couple of Instructions.
- Underneath the **Microsoft** task group is the **Configuration Manager** task group containing Instructions related to that product.

Note

For more information on using Task groups to access and schedule Instructions, please refer to:

- Tasks
- Scheduling instructions
- Scheduling instructions - a tutorial.

1.1.3.2.8 Inventory and connectivity

The **Devices** page in the Explorer shows you all the devices that have connected with Tachyon and their current connection status. There are two views provided that let you research the devices: the devices table and the devices dashboard, please refer to The Devices Table and The Devices Dashboard for more details.

Note

For more information on inventory and connectivity, please refer to:

- Investigating Devices
- Using the Devices dashboard - Tutorial.

1.1.3.3 Guaranteed State features

The Guaranteed State application gives you the ability to ensure device compliance with enterprise IT policies. For more information please refer to the Using Guaranteed State section of this documentation.

1.1.3.3.1 Policies and Rules

The Guaranteed State state of a device is enforced by the Tachyon client at the device. One or more policies are deployed to devices according to the management groups the devices belong to. Each policy consists of one or more rules that are either check rules or fix rules.

Rule	Explanation
Check	Allow you to verify that a device has a particular state, such as a registry key having a specific value. You can then view summary and detail reports which show devices that are compliant and not compliant with the check rules.
Fix	Allow you to define a desired state for the device and then enforce that state. For example, you could mandate that a registry key exists and contains a specific value. Again, you can report on the application of these fix rules to devices.

For an explanation of management groups, please refer to the Management Groups page. Management groups allow devices to be flexibly grouped, based on management group rules. This means you can easily administer devices based on, for instance, their Active Directory Organizational Unit, or their operating system version, or any other criteria supported by the management group rules.

Note

For more information on policies and rules please refer to:

- Defining your own policy
- Integrated Product Packs.

1.1.3.3.2 The Guaranteed State Overview page

The **Overview** page lets you view the current state of your enterprise in terms of the devices and policies that have been defined and applied. It consists of a number of charts that let you monitor the state in real-time.

Note

For more information on the Guaranteed State Overview page please refer to:

- Guaranteed State Overview page

1.1.3.3.3 Guaranteed State Reports

The Guaranteed State application provides three reports that let you view the details for the currently defined **Policies**, **Rules** and **Devices**. The information in these reports is consolidated into the **Guaranteed State Overview** page charts.

Note

For more information on the **Policies**, **Rules** and **Devices** reports pages please refer to:

- Guaranteed State Overview page

1.1.3.3.4 Exploring devices

Guaranteed State provides a **Devices** page where you can view the currently connected devices. On this page you can also select one or more of the devices and click an **Explore** button that launches the **Explorer** application. You can then run an instruction using the selected devices as the coverage for the instruction.

Note

For more information on exploring devices please refer to:

- Using Explorer to investigate devices in Guaranteed State.

1.1.3.3.5 Device Criticality

Device criticality is an attribute of a device that defines its importance within an organization. The default definition in Tachyon has these settings:

- Undefined (or not set)
- Non-critical
- Low
- Medium
- High
- Critical.

At present, criticality settings do not affect the primary operation of Guaranteed State. However, it is possible to use Tachyon to set device criticality and to view it within Guaranteed State.

Tachyon also supports the use of the criticality setting when defining coverage for an instruction. For example, you can target an instruction to be sent only to devices whose criticality is not **Critical**.

Note

For more information on device criticality please refer to:

- Using Device Criticality.

1.1.3.4 Settings features

The Settings application lets you configure Tachyon system and application settings. For more information please refer to Using Settings.

Here's an overview of the features available in the Settings application.

1.1.3.4.1 Instructions, product packs, Instruction sets and permissions

Tachyon lets you investigate your network using questions and actions, which are collectively known as Instructions.

You can load Instructions into Tachyon, either individually or using a Product Pack, which is essentially a zip file containing one or more Instructions. Tachyon comes with a range of pre-framed questions and actions in the form of Product Packs, providing extensive out-of-the-box capabilities that can be extended as new and updated Product Packs are made available.

Tachyon permissions for the Instructions are handled using Instruction sets. You create Instruction sets, then define roles which specify particular permissions on those sets and then assign the roles to users. Each Instruction is only allowed to reside in one Instruction Set, which associates it with a role and thereby the users that have that role and can run the Instruction. The roles have associated Management groups that determine the devices that users with the role have access to.

When Instructions are loaded into Tachyon they are placed in the default **Unassigned** Instruction Set, so you must move them into previously created Instruction sets before they can be run.

> **Note**
>
> For more information on uploading product packs into Tachyon and managing Instruction sets, please refer to:

- Instruction sets page

1.1.3.4.2 Connectors

Connectors are used to connect to other 1E and third party systems and populate repositories. When more than one connector to different data sources are used, the information from those different data sources is de-duplicated and normalized into a single cohesive view that is then stored in a repository. In this way you can use the data from different sources to augment each other and build a better picture of "what's out there?".

For example, you can sync inventory data from Configuration Manager into an inventory repository, which will fetch information about your Windows devices. You could then augment that with inventory data synced from Tachyon platform which could include information about non-Windows devices where the Tachyon client has been installed.

> **Note**
>
> For more information on connectors, please refer to:

- Connectors page

The following connectors are supported:

- BigFix connector — Connects to a BigFix Inventory database server.

- BigFixInv connector — Connects to a BigFix Inventory database.
- File Upload connector — Uploads inventory data from a folder containing tab (TSV) and comma (CSV) separated value file(s).
- Intune connector — Connects to an Intune application and collects inventory and usage data.
- Microsoft Office 365 connector — Connects to an Office 365 application in InTune and pulls in inventory and usage data.
- OpenLM connector — Connects to an OpenLM database server.
- Oracle LMS connector — Connects to Oracle LMS and queries it for inventory information.
- ServiceNow connector — Connects to a ServiceNow instance to import basic inventory data into SLA Platform.
- System Center Configuration Manager connector — Connects to a Configuration Manager database and pulls in inventory and usage data.
- Tachyon connector — Connects the Tachyon and SLA components to support Management group and Tachyon Powered Inventory features. The Tachyon Powered Inventory feature uses instructions to fetch inventory data from Tachyon clients, and is a prerequisite for Patch Success.
- vCenter connector — Connects to a vCenter server and pulls in inventory data.
- Windows Server Update Services connector — Connects to a WSUS database and pulls in patch data.

1.1.3.4.3 Repositories

Repositories are used by applications to process and store information. For example the Patch Success application uses both an inventory and a BI repository to process the information needed to report on how successful patching is in your enterprise. Normally a connector is used to connect a data source to an appropriate repository.

Tip

Repositories are also useful when you want to segregate different types of data. For example, you could have one inventory repository for Configuration Manager inventory data, and another one for BigFix data. Alternatively, you can have connectors to different inventory sources pushing data into one repository. Any Management Groups that you create will span all the repositories you have.

Note

For more information on managing repositories, please refer to:

- Repositories page

1.1.3.4.4 Device Tags

Device Tags are generally associated with Explorer and can be used when setting coverage to target Instructions to particular devices, but they can also be used to define Management Groups optionally used by all applications.

Device Tags must be defined by a **Full Administrator** before they can be used to tag devices or used to set the coverage of Instructions.

This is done from the **Settings**→**Configuration**→**Custom properties**→ **Device Tags** page, which can be viewed by users with the **Full Administrator** role.

Note

For more information on managing and using Device Tags, please refer to:

- Device Tags page
- Adding properties - tutorial
- Actions to set tags - tutorial
- Using tags to set the coverage for a question - tutorial.

1.1.3.4.5 Software Tags

Using Software Tags allows you to create custom labels and associate them with the software titles you have deployed in your estate.

You can do this from the **Settings**→**Configuration**→**Custom properties**→**Software Tags** page, which can be viewed by users with the **Full Administrator** role.

Using Software Tags allows you to create custom labels and associate them with the software titles you have deployed in your estate. An administrator with either the **Full Administrator** or **Group Administrator** role can set Software Tags in their environment, they can also create Management Groups based on the tag name and value. For details about configuring Tachyon users, Roles, and Management Groups refer to the Permissions Menu pages.

In short, you can work with Software tags by:

1. Creating your Software Tag.
2. Associating the new tag with a software title.
3. Creating a Management Group based on the Software Tag name and Tag value rules (This step can be run anytime before evaluation).
4. Evaluating the new Management Group by running a Basic Inventory Consolidation.

If an administrator adds or modifies Software Tags or associations, they will have to run the Management Group evaluation report again to see the updated devices reflected in Inventory.

1.1.3.4.6 Schedules

Schedules can be created to execute specific operations on repositories in Tachyon so that they are kept up to date with their data sources and processing. These operations include:

- Syncing data sources to repositories using connectors

- Processing the BI data cube.

Repository schedules are different to Instruction schedules that can be set in Explorer.

Note

For more information on setting schedules, please refer to:

- Schedules page.

1.1.3.4.7 Consumers, Applications, Components and Providers

There are pages in the Settings application for each of these. They are described in the following table:

Configuration objects	Description
Consumers	These can access Tachyon using the Tachyon Consumer API. To enhance the security of the Tachyon system. Only consumers that have been registered on the **Settings→Configuration→Consumers** page will be allowed to access Tachyon.
Applications	Features of that are hosted in the Tachyon Portal. Applications are generally Consumers as they need to interact with Tachyon using the Tachyon API. These are available on the **Switch App** menu.
Components	These form part of SLA and cannot be changed or altered by a user. These can be viewed using the **Settings→Configuration→Components** page.
Providers	These are components that can be configured to provide a particular operation in SLA. These can be viewed and configured using the **Settings→Configuration→Provider configuration** page.

Note

For more information on Consumers, Components and Providers, please refer to:

- Consumers page
- Components page
- Provider configuration table

1.1.3.4.8 Information pages

Information on your Tachyon license is available, as well as the ability to re-activate it following an update.

You can view information on the Tachyon system information for the Consumer, Coordinator, Background channel, Core and Switch.

Note

For more information please refer to:

- License information page
- System information page.

1.1.3.4.9 Monitoring log files

The monitoring pages let you view how Tachyon is performing its tasks. Four key log pages are provided:

Page	Description
Process log	Whenever you execute a sync or process a repository the steps are displayed here. This page is updated in real-time and shows the status of each step as it happens.
Sync log	The results of performing a sync are displayed here.
Infrastructure log	Information on the Tachyon infrastructure is displayed here, such as: license status and instruction workflow.
Audit information log	This page displays information on the Instructions that have been run in Explorer. This includes the instruction text and the user that requested it.

Note

For more information on monitoring please refer to:

- Process log page
- Sync log page
- Infrastructure log page
- Audit information log page.

1.1.3.4.10 Defining users and roles

Tachyon users or groups can be added from your IdP. They can be assigned roles that determine what aspects of Tachyon they can access. Custom roles can be created that let you associate particular permissions on particular Instruction sets for particular management groups.

Note

For more information on users and roles please refer to:

- Users and Groups page
- Roles page
- Configuring Access Rights - tutorial.

1.1.3.4.11 Management groups

Management groups use inventory-based rules to define groups of particular devices, they are implemented in SLA and then made available to Tachyon applications and other consumers. After a management group is defined, each time the inventory is updated the device membership of the groups is re-evaluated by applying the management group's rules to the new inventory.

Custom roles can be created that tie particular Instruction sets to particular management groups. This means you can not only set the permissions for users to access the Instructions in specific Instructions sets, you can also determine which devices they can target using those Instructions.

Once defined, management groups can then be used to set the coverage for Instructions in Explorer and also which devices can be targeted by particular users. Management groups are also used by other applications to determine which devices are being targeted.

> **Note**
>
> For more information on management groups, please refer to:

- Management Groups page
- Management Groups - tutorial.

1.1.3.4.12 Uploading Instructions into Tachyon and creating Instruction sets

You determine the capabilities of Explorer by uploading Instructions from Product Packs into Tachyon. Product Packs are either provided with the release or downloaded from the 1E Exchange. Once the Instructions have been uploaded into Tachyon you then need to put them into Instruction sets. The Instruction sets can then be associated with custom roles to determine the permissions applied to the Instructions. The custom roles are then applied to users to determine which Instructions each user has access to.

> **Note**
>
> For more information on uploading product packs into Tachyon and managing Instruction sets, please refer to:

- Instruction sets page

1.1.3.5 Inventoryfeatures

The Inventory app captures data from different sources, then consolidates, normalizes and stores it in Inventory repositories. The Inventory app is also used to view and export inventory, and manage associations.

Inventory uses connectors to capture software, hardware and other data from sources such as Tachyon, Configuration Manager, Big Fix and vCenter where it is consolidated, de-duplicated and normalized. Normalization uses software and hardware entries in The 1E Catalog.

An empty repository called **Default Inventory** is provided out-of-the box. You can optionally create additional inventory repositories to partition data by source, time periods, or other purpose. To populate a repository, you must use one or more inventory connectors, and either manually sync the data or schedule a sync. For more detail, please refer to Repositories page and Schedules page in Settings.

Inventory repositories are used by the following applications:

- Introducing Patch Success - reports on and ensures successful patching of your enterprise
- Introducing Application Migration - automates the migration of applications during a Configuration Manager OS deployment
- Introducing AppClarity - manages entitlements, compliance and reclaiming unused software
- Any application - if you need it to use Management Groups.

1.1.3.6 Consumer applications

Applications are categorized as follows:

- Configuration - applications required to configure Tachyon platform and required by all other applications
- Client - applications that communicate with devices in real-time
- Inventory – applications that use inventory features.

1.1.3.6.1 Applications that are included in the Tachyon Platform license

Application	Purpose	Type
Inventory Insights	View and export inventory, and manage associations. It uses the SLA databases.	Inventory, configuration
Settings	Configure and monitor platform features. It uses the Tachyon Master database.	Configuration
Endpoint Automation	Ensure endpoint compliance to enterprise IT policies. It uses the Tachyon Master and Responses database.	Client
Endpoint Troubleshooting	Investigate, remediate issues and manage operations across all your endpoints in real-time. It uses the Nomad Master and Responses database.	Client

1.1.3.6.2 Applications that require a license

Application	Purpose	Type
Appclarity	Manage software license compliance, License Demand Calculations, license entitlements, and for reclaiming unused software. It uses the SLA databases.	Inventory

Application	Purpose	Type
Application Migration	Intelligently automate the migration of applications during a Configuration Manager OS deployment. It uses the SLA databases.	Inventory
Content Distribution	Manage content distribution across your organization using a centralized dashboard. It uses the Content Distribution database. 1E Client requires Tachyon and Nomad features to be enabled on all clients. Content Distribution replaces the Nomad features of ActiveEfficiency Server, which is deprecated. Legacy Nomad clients continue to be supported by direct communication with the Content Distribution API, whereas Nomad 8.x clients communicate with the Content Distribution API via the proxy feature on Response Servers. Tachyon Setup is used to install Content Distribution, and the Nomad app, and no longer installs ActiveEfficiency. Nomad uses Content Distribution for the following features: • Nomad app provides visibility of content distribution activity • Single-site download - SSD • Single Site Peer Backup Assistant - SSPBA • High Availability PBA (HAPBA) • Get Migration Settings task sequence action used to manage computer associations • Nomad Pre-caching • Nomad Download Pause.	Client
Patch Success	Reports on and ensures successful patching of your enterprise. It uses the SLA and BI databases. Requires SLA Business Intelligence to be installed by Tachyon Setup, as described in 1E Business Intelligence above. It also needs	Inventory

Application	Purpose	Type
	connectors to get meta-data for patches from whichever of the following that you use to approve patches: • Configuration Manager (SCCM) if it is configured to manage WSUS • Windows Server Update Services (WSUS).	
Experience Analytics	Measure performance, stability and responsiveness for applications and devices to assess user experience across your enterprise. It uses the Tachyon Master and Experience databases.	Client

1.1.3.7 The 1E Client

The 1E Client provides functionality to Tachyon. On Windows devices, the 1E Client provides client features and modules for other 1E products. On non-Windows devices, the 1E Client only provides Tachyon features.

Tachyon enables rapid response to instructions using the 1E Client, which supports the retrieval of information, running actions and device tagging. The 1E Client can also be extended to support additional features. On Windows OS, the 1E Client is installed as a service, with a small footprint.

1.1.3.7.1 Supported Platforms

All 1E Client features are supported on the following Windows OS:

Windows

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows 11 CB 21H2
- Windows 10 CB 21H2
- Windows 10 CB 21H1
- Windows 10 CB 20H2

The zip for 1E Client for Windows is available for download from the 1E Support Portal, https://1e.my.site.com.

Professional and Enterprise editions are supported for Windows 10 and Windows 11.

All versions are provided with 32-bit & 64-installers, and can be installed on physical and virtual computers.

Note

This list is automatically updated to show only those OS versions in mainstream support by Microsoft, and therefore supported by 1E, and by 1E Client 8.1.

Please refer to Constraints of Legacy OS regarding the end of mainstream support.

For Microsoft product lifecycle details, please refer to https://support.microsoft.com/en-us/lifecycle/search.

Please refer to https://support.1e.com/ for details of which Current Branch versions are supported by 1E products, and known issues regarding specific versions.

The Tachyon client features of 1E Client are supported on the following non-Windows OS:

macOS

- macOS Monterey 12.0
- macOS Big Sur 11.0
- macOS Catalina 10.15
- macOS Mojave 10.14

Linux

- CentOS Stream 8
- Debian 10.4
- Fedora 34
- Red Hat Enterprise Linux 7.9
- Red Hat Enterprise Linux 8.5
- SUSE Linux Enterprise 15.2
- Ubuntu 18.04

Solaris

- Please use 1E Client 5.2

Other versions of these non-Windows OS should work but have not been tested by 1E.

1E Client packages for other Linux distributions can be requested, including Raspbian for Raspberry Pi.

The 1E Client for Linux supports the following architectures:

- Linux variations on Intel 64-bit platforms

1E Client packages for Linux are included in the non-Windows zip available for download from the 1E Support Portal, https://1e.my.site.com.

1E Client supports only Tachyon features on non-Windows devices.

1E Client 8.1 is ***not*** available for Solaris, please use 1E Client 5.2 instead.

The 1E Client 5.2 for Solaris supports for the following architectures:

- Solaris on Intel 64-bit and SPARC platforms

1E Client 5.2 package for Solaris is included in the non-Windows zip available for download from the 1E Support Portal, https://1e.my.site.com.

1E Client supports only Tachyon features on non-Windows devices.

1.1.3.7.2 Tachyon Activity Record feature

Tachyon clients capture certain types of event data in a local database (Persistent Storage) so that instructions can query later. Data is compressed and encrypted in a way that ensures a very low impact on device performance and security.

Tachyon Activity Record is similar to Windows Task Manager and Perfmon. On Windows client devices Tachyon continuously captures events, which enables all significant events to be captured as they happen. Other OS use polling, which requires the polling frequency to be regular enough to ensure brief events are captured.

1.1.3.8 System status bar and notification area

Tachyon includes a system status bar that displays the number of Tachyon instructions in progress and current and historical connectivity information for the total number of devices connected to Tachyon.

The notification area provides information on the logged on user or administrator and access to their notifications.

1.1.3.9 Certificates

Tachyon uses certificates on the Tachyon Server and client devices to maintain the security of the system. Any custom Instructions must be code-signed with a certificate that has been registered in your 1E license before they can be run in Tachyon.

The certificates feature includes:

- Support for Cryptographic Next Generation certificates
- Upgrade to the latest version of OpenSSL v1.0.2h
- Security to enforce 1E Client device certificates.

1.1.3.10 Tachyon integration

Tachyon can integrate with 3rd party products. It integrates seamlessly with Microsoft System Center Configuration Manager, it can use Content Distribution to add content download capabilities, provides a fully-featured consumer API and can even be used as a response delivery mechanism by 3rd party applications.

1.1.3.10.1 Consumer management

Tachyon provides a dedicated page where the 3rd party consumers can be enabled and managed by Tachyon Consumer Administrators, as described on the Consumers page.

1.1.3.10.2 Microsoft System Center Configuration Manager console integration

Configuration Manager users can use all the features of Tachyon from within the Configuration Manager console.

- Run questions and actions that target the devices in Configuration Manager collections.

1.1.3.10.3 1E Client integration with Content Distribution to enable efficient download of content

Tachyon can leverage the features of the industry-respected Content Distribution to enable content to be downloaded to the Tachyon client device. Using Content Distribution provides the following benefits:

- Significantly reduces the bandwidth required for delivering software
- Small offices or sites connected via poor network links can receive software updates more reliably
- Reduces the need for large numbers of Configuration Manager servers
- Faster Configuration Manager implementations because fewer servers are required
- Distribute software to home, mobile and remote office users
- Low cost – easy to deploy
- No new infrastructure or skills required
- Reduces software distribution costs

The feature is a set-and-forget option on the 1E Client . By default, it is enabled and means that Tachyon will automatically use Content Distribution to download content if it is installed on the 1E Client device (Content Distribution is currently supported on Windows devices only). The prerequisites for using Content Distribution are given on Supported Platforms. The options for configuring Content Distribution integration are NomadContentDownloadEnabled and NomadContentDownloadTimeoutSecs in the **1E Client configuration file**.

1.1.3.10.4 Tachyon consumer API

Tachyon implements a complete API for controlling the questions, answers, responses and workflows that implement the Tachyon features for third-party applications including ServiceNow.

The Tachyon API feature includes:

- Consumer API versioning
- Improved version and error reporting support in Consumer API
- Extended RBAC API extensions for consumers

1.1.3.10.5 Tachyon can offload responses directly to 3rd party applications

Tachyon can be used as the means to gather data for 3rd party applications. Using its fast response time to gather the data, it then be configured to pass the data on without storing it locally. The offloading is configured for each consumer on the Consumers page. To use this feature, the consumer must be configured to use the offloaded responses data.

1.1.3.11 Telemetry

Telemetry helps 1E to continually improve your experience with Tachyon. Only summarized statistical information is collected, which enables 1E to see how customers use features of the application. No personally identifiable data is collected. 1E use this information to:

- Understand how the product is being used to influence future development decisions
- Plan supported platforms (OS, SQL etc. versions) over time
- Deliver a smooth upgrade experience as we can focus testing on implemented scenarios
- Improve system performance
- Identify early warning signs of potential issues such as excessive growth of database tables, instruction failures etc. so we can pro-actively address them.

Server telemetry reports how the platform is used and data is compressed, encrypted and sent to 1E through email on a configurable schedule. Full details of the Server telemetry data sent to 1E is provided in Server telemetry data.

User Interface telemetry reports how the user interface is used, and data is sent directly from administrator browsers to the 1E Cloud.

Telemetry features are configurable using Tachyon Setup during installation or upgrade, and can be enabled or disabled as a post-installation task. 1E encourages customers to enable sending telemetry.

1.1.4 Tachyon Architecture

A description of Tachyon Stacks and their Tachyon components, the Tachyon clients, and how they connect to provide Tachyon features.

1.1.4.1 Tachyon deployment architecture

At the top-most level, Tachyon architecture consists of Tachyon Server components, grouped into Stacks, and clients that are deployed onto the devices that you want to manage.

1.1.4.1.1 Tachyon Server Stacks

Every Tachyon system has a single **Master Stack**, which provides web services for Tachyon applications. Master Stack components are typically all installed on a single **Master Server**.

Tachyon real-time features require **Response Stacks**, which are made up of one or more **Response Servers**. A **DMZ Server** is an example of a Response Server. Each Response Stack has at least one **Background Channel** for sharing resources and a single **Core** component that supports an associated set of up to five **Switches**.

Switches are the primary mechanism for rapidly requesting and retrieving responses from the **1E Client**. As each Switch can handle up to 50,000 devices there is a limit of 250,000 devices per Response Stack. Higher numbers can be achieved if you contact 1E for guidance. Switches may be local or remote to the other components in the Response Stack.

Databases for Tachyon, 1E Catalog, Nomad, Experience, SLA and BI, are installed on SQL Server database instance(s) that may also be local or remote to their respective Master and Response servers. It is also possible for multiple Response Stacks to share the same Responses database. The **Cube** used by Patch Success (SLA-BI) is installed on a local or remote SQL Server Analysis Services (SSAS) instance.

Please refer to the:

- Architectural requirements section for guidance on which architecture to choose
- Communication Ports reference page for connection details between components and ports necessary for firewalls.

1.1.4.1.2 Tachyon Single-Server system

In the most basic setup, there is a single server that hosts both a Master Stack and a Response Stack and this can be deployed by selecting the default settings in Tachyon Setup.

The following table shows the Tachyon platform components, including Tachyon Master and Response Stacks, and also shows the DMZ Server discussed in Tachyon architecture for Internet-facing devices.

Subsystem	Component	Web application	Master Stack	Response Stack	DMZ Server
Master Server	Tachyon Portal UI and applications	Tachyon	1		
Consumer API	Consumer	1			
Coordinator service		1			
Tachyon Master database		1 (optionally Remote)			
Experience	Experience API	Experience	1		
Experience database		1 (optionally Remote)			
Nomad	Nomad API	Nomad	1 (optional)		
Nomad database		1 (optionally Remote)			

Subsystem	Component	Web application	Master Stack	Response Stack	DMZ Server
1E Catalog	1E Catalog UI	CatalogWeb	1		
1E Catalog API	CatalogWeb				
1E Catalog Update Service					
1E Catalog database		1 (optionally Remote)			
SLA and Inventory	SLA Platform UI and SLA applications	Platform	1		
SLA Admin	Admin	1			
SLA Engine		1			
SLA Integrate services: • SLA Integrate Agent service • SLA Integrate Manager service		1			
SLA Operations Provider API	CoreExternal	1			
SLA databases (Data, Integrate, Shared)		1 (optionally remote)			
SLA Business Intelligence (BI) (for Patch Success)	MDX API (BI)		1		
SLA-BI database		1 (optionally Remote)			

Subsystem	Component	Web application	Master Stack	Response Stack	DMZ Server
SLA-BI cube (requires SSAS)		1 (optionally Remote)			
Response Server	Core	Core		1	
Background Channel	Background		1	1	
Switch(es) (also includes a single Switch Host service)			up to 5 (optionally Remote)	up to 5	
Tachyon Responses database			1 (optionally Remote)		

The picture shows a Tachyon Single-Server System with databases optionally installed locally or on remote SQL Server instance(s). Components colored green are optional in a Tachyon system.

The Response Stack can be installed on the same server as the Master Stack, and on remote servers.

The DMZ Server has only the Tachyon client-facing components of the Response Stack: the Background Channel and Switches.

1.1.4.1.3 Applications and Tools

Tachyon applications and tools are consumers, and all consumers connect to the Tachyon Consumer API.

The following consumer applications run on the Tachyon platform and are installed using Tachyon Setup. Please also refer to the License requirements page.

Applications are categorized as follows:

- Configuration - applications required to configure the Tachyon platform and required by all other applications
- Client - applications that communicate with devices in real-time
- Inventory – applications that use inventory features.

1.1.4.1.3.1 Applications that are included in the Tachyon Platform license

Application	Purpose	Type
Inventory Insights	View and export inventory, and manage associations.	Inventory, configuration

Application	Purpose	Type
	It uses the SLA databases.	
Settings	Configure and monitor platform features. It uses the Tachyon Master database.	Configuration
Endpoint Automation	Ensure endpoint compliance to enterprise IT policies. It uses the Tachyon Master and Responses database.	Client
Endpoint Troubleshooting	Investigate, remediate issues and manage operations across all your endpoints in real-time. It uses the Nomad Master and Responses database.	Client

1.1.4.1.3.2 Applications that require a license

Application	Purpose	Type
AppClarity	Manage software license compliance, License Demand Calculations, license entitlements, and for reclaiming unused software. It uses the SLA databases.	Inventory
Application Migration	Intelligently automate the migration of applications during a Configuration Manager OS deployment. It uses the SLA databases.	Inventory
#UUID39ecfb49a2e10e6f5820cc411d69d030	Manage content distribution across your organization using a centralized dashboard. It uses the Content Distribution database. 1E Client requires Tachyon and Content Distribution features to be enabled on all clients.	Client

Application	Purpose	Type
	Content Distribution replaces the Nomad features of ActiveEfficiency Server, which is deprecated. Legacy Nomad clients continue to be supported by direct communication with the Content Distribution API, whereas Nomad 8.x clients communicate with the Content Distribution API via the proxy feature on Response Servers. Tachyon Setup Setup is used to install Content Distribution, and the Nomad app, and no longer installs ActiveEfficiency. Nomad uses Content Distribution for the following features: • Nomad app provides visibility of content distribution activity • Single Site Download (SSD) • Single Site Peer Backup Assistant (SSPBA) • High Availability Peer Backup Assistant (HAPBA) • Get Migration Settings task sequence action used to manage computer associations • Nomad Pre-caching • Nomad Download Pause.	
/document/preview/763581#UUID-54875393-7855-5624-cbae-9ad5406e1c95	Reports on and ensures successful patching of your enterprise. It uses the SLA and BI databases. Tachyon Setup indstalls SLA Business Intelligence, which requires SQL Server Analysis Server.	Inventory

Application	Purpose	Type
	Patch Success also uses Inventory connectors to get meta-data for patches from whichever of the following that you use to approve patches: • Configuration Manager (SCCM) if it is configured to manage WSUS • Windows Server Update Services (WSUS).	
Introducing Tachyon Experience	Measure performance, stability and responsiveness for applications and devices to assess user experience across your enterprise. It uses the Tachyon Master and Tachyon Experience databases.	Client

The following types of application require 1E Client (with Tachyon features enabled) to be deployed to all in-scope devices.

- All Client applications
- Inventory applications if you intend using the Tachyon connector to populate your inventory.

The **AI Powered Auto-curation** feature is optionally used by Inventory applications to provide automatic curation of new products. This avoids having to manually add products to the 1E Catalog, or wait for it be updated. This optional feature requires additional memory on the Tachyon Server (Master Stack). Please refer to AI Powered Auto-curation: Memory requirements for details.

Some benefits of using AI Powered Auto-curation are that you can:

- Achieve significantly more normalized software from the first sync
- Reduce the manual effort required to normalize software
- Get an expanded SAM offering as more data is available for AppClarity
- Get additional coverage for Application Migration
- Identify more software to review for security threats.

1.1.4.1.3.3 Tachyon Tools

The following are tools included in Tachyon 8.1 platform. These tools are not installed using Tachyon Setup. They have either their own installers or are included in download zips.

- Tachyon ConfigMgr UI Extensions - installed as part of the Tachyon Toolkit, this is a right-click extension for the Configuration Manager console that provides the option to browse and run an instruction on devices in a specified Collection, refer to Preparing for the Tachyon extensions for the Configuration Manager Console. for details.
- Tachyon Run Instruction command-line tool - installed as part of the Tachyon Toolkit, it is used for sending instructions to the Tachyon server from a script or from a command prompt.
- Tachyon Product Pack Deployment Tool - included in the Tachyon platform zip ProductPacks folder.
- TIMS - used for the development of instructions using the Tachyon SDK, refer to /document/preview/736745#UUID-952f2552-fb04-d55c-6d12-fcf68313ecac for details.

A typical Tachyon license allows the use of all these tools.

1.1.4.1.4 Tachyon Multi-Stack system

The picture shows a Tachyon Multi-Stack System. Here the Tachyon Master Stack communicates with one or more Tachyon Response Stacks. A local Response Stack is not mandatory. Components colored green are optional in a Tachyon system.

As with a single-server system, the databases are optionally installed locally or on remote SQL Server instances(s).

1.1.4.2 Tachyon components

Let's take a look at each of the Tachyon components in slightly more detail.

Component	Description
IIS Components	The following components are IIS Web Applications that reside on a single-server. Other configurations - such as Response Stack and DMZ Server - have a subset of these. Under the Tachyon website: **Web Applications** • Admin (SLA Admin) • Background (Tachyon Background Channel) **Application Pools** • CatalogWeb • ContentDistribution • SLAPlatform.Admin

Component	Description
	• CatalogWeb • Consumer (Tachyon Consumer API) • ContentDistribution (Nomad) • Core (Tachyon Core) • CoreExternal (SLA Ops Provider API) • Experience (optional) • Platform (SLA Platform UI) • Tachyon (Tachyon Portal UI) • SLAPlatform.CoreExternal • SLAPlatform.Platform • Tachyon.Background • Tachyon.Consumer • Tachyon.Core • Tachyon.Experience • Tachyon.Portal
Core	The Core is a Tachyon Response Stack component which provides internal API and data processing. Core does the following: • Forwards workflow commands from the Workflow service to the Tachyon Switch • Generates and sends instrumentation data to the Instrumentation service • Forwards responses from the Switch to the Responses database.
Background Channel	The Background Channel is a Tachyon Response Stack component which provides a means for the Tachyon clients to retrieve large data items from Tachyon without loading the Tachyon Switch: • Stores Tachyon content provided by the Consumer API in the Background Channel for Tachyon clients to retrieve • Responds to Tachyon clients retrieving Tachyon content from the Background Channel.
Switch	The Switch is a Tachyon Response Stack component which provides the following: • Sends instructions to and retrieves responses from the Tachyon clients • Receives workflow commands from the Core component

Component	Description
	• Retrieves instruction definitions from the Core component • Forwards responses to the Core component • Sends instrumentation data to the Instrumentation component. The Switch Host service is responsible for starting local Switches.
Tachyon Portal UI	Tachyon users browse to the portal to access Tachyon applications. Applications that are Tachyon built-in applications: • Guaranteed State • Inventory • Settings • Explorer Applications that are optional: • AppClarity • Application Migration • Patch Success • Experience.
Tachyon Consumer API	The Tachyon Consumer API provides the following: • Processes the consumer requests from Explorer and other Consumers • Publishes Tachyon content to the Tachyon Background Channel • Forwards requests for instrumentation data from the Explorer to the Tachyon Instrumentation component • Forwards workflow commands from the Explorer to the Tachyon Workflow component.
Tachyon Coordinator	The Coordinator service is the coordinating service used by Tachyon components. It has two modules, Workflow and Instrumentation. The Workflow module provides the following:

Component	Description
	• Forwards workflow commands from the Consumer API to the Core • Stores workflow in SQL • Connects to remote SMTP to send emails used in the approval process for actions • The Workflow component contacts the Authentication component to manage the two-factor authentication process The Instrumentation module processes instrumentation data from the following components: • Core • Workflow • Switch. And responds to requests for instrumentation data from the Consumer API. Supports the two-factor authentication feature, with email.
Nomad	Content Distribution replaces the related features of ActiveEfficiency Server, which is deprecated. Legacy clients continue to be supported by direct communication with the Content Distribution API, whereas Nomad 8.x clients communicate with the Content Distribution API via the proxy feature on Response Servers. Tachyon Setup is used to install Content Distribution and the Nomad app, and no longer installs ActiveEfficiency. Nomad includes the following features: • Nomad app provides visibility of content distribution activity • Single-site download - SSD • Single Site Peer Backup Assistant - SSPBA • High Availability PBA (HAPBA) • Get Migration Settings task sequence action used to manage computer associations • Nomad Pre-caching

Component	Description
	• Nomad Download Pause.
1E Catalog UI	The website is used to view and interact with the 1E Catalog. Tachyon Setup supports the installation of 1E Catalog on the Tachyon Master Stack server. For customers that want to continue using an existing installation of 1E Catalog 2.0 then Tachyon Setup supports using a remote Catalog server as a custom setup option. Please contact 1E for details on how to use custom setup options.
Catalog Update Service	Service is used to connect to the 1E Cloud Catalog in order to download the latest catalog entries.
Catalog API	Consumer API is used to manage and update the 1E Catalog.
SLA Admin	Internal API used to manage SLA components.
SLA Platform UI	The website is used to view and interact with the Inventory.
SLA Engine	The Engine service is the coordinating service used by SLA components. This includes processing of Management Groups.
SLA Integrate Services	The SLA Integrate Agent sevice performs Connector functions by connecting to data sources and importing data into repositories. The SLA Integrate Manager service manages Agent operations including repository action schedules.
SLA Inventory	The inventory repositories. Each instance of a repository is stored in SLA-Data database, and is based on a template defined in the SLA-Data database.
SLA Operations Provider API	Consumer API and functions used by SLA clients, including Application Migration task sequence steps and AppClarity Software Reclaimer.
MDX (BI)	Internal API used by Patch Success application. Business Intelligence is an optional component installed by Tachyon Setup on the Master Stack, and requires SQL Server Analysis Services (SSAS). Business

Component	Description
	Intelligence is a prerequisite for the **Patch Success** application to support efficient presentation of visualizations on a large scale.
Consumer applications	The following Consumer applications are licensed: • AppClarity • Application Migration • Guaranteed State • Nomad • Patch Success • Experience • Explorer The following Consumer applications are included with Tachyon platform: • Inventory • Settings. Other consumers are Tachyon Configuration Manager Console extensions and other toolkit features.
SQL Server (Database Engine and Analysis Services)	Tachyon has two databases: • Tachyon Master • Tachyon Responses. Experience has one database: • TachyonExperience 1E Catalog has one database: • 1ECatalog SLA has three databases: • SLA-Data • SLA-Shared

Component	Description
	• SLA-Integrate SLA BI has two databases: • SLA-BI database • SLA-BI cube on a SQL Server Analysis Server (SSAS) instance Nomad has one database: • ContentDistribution
1E Client	1E Client includes clients for Tachyon, Nomad, PXE Everywhere Agent, Shopping/WSA, and WakeUp. All the above are supported on Windows devices, client features (excluding Experience and User Interaction) are also available on non-Windows devices. Tachyon clients communicate with the Tachyon Switches and the Background Channel to provide responses to instructions (questions and actions) and subscribe to policy events for Experience and Guaranteed State. Nomad clients use Tachyon Switches and the Background Channel as a proxy for communicating with the Content Distribution.

1.1.4.3 Tachyon architecture for Internet-facing devices

Enabling Tachyon to support devices that are external to your company network is done by slightly extending the default single-server architecture.

To enable external Tachyon client devices to interact with Tachyon, the DMZ requires at least one Background Channel and at least one Switch.

The Responses Stack handles communications between Master Stack and the platform clients. The Background Channel and Switch components handle the direct communication with the platform clients, the Core processes the information in both directions between the Master Stack and the Switches.

First, you need a working Tachyon system on the internal network, with a Response Stack that will provide the Core for the DMZ Server. The picture shows a Response Stack and Master Stack on the same server, located on the internal network. This serves clients when they are connected to the internal network.

Then configure the internal firewall to allow two-way communication between each of the following:

- The Core on the Internal Response Stack and the Switch(es) in the DMZ
- The Coordinator on the internal Response Stack and the Switch(es) in the DMZ
- The Consumer API on the internal Master Stack and the Background Channel in the DMZ.

Configure the external firewall to allow incoming connections for:

- The external platform clients and the Background Channel in the DMZ
- The external platform clients and the Switch(es) in the DMZ.

After you have provisioned a server in the DMZ, you need to make the following changes to the existing Tachyon system:

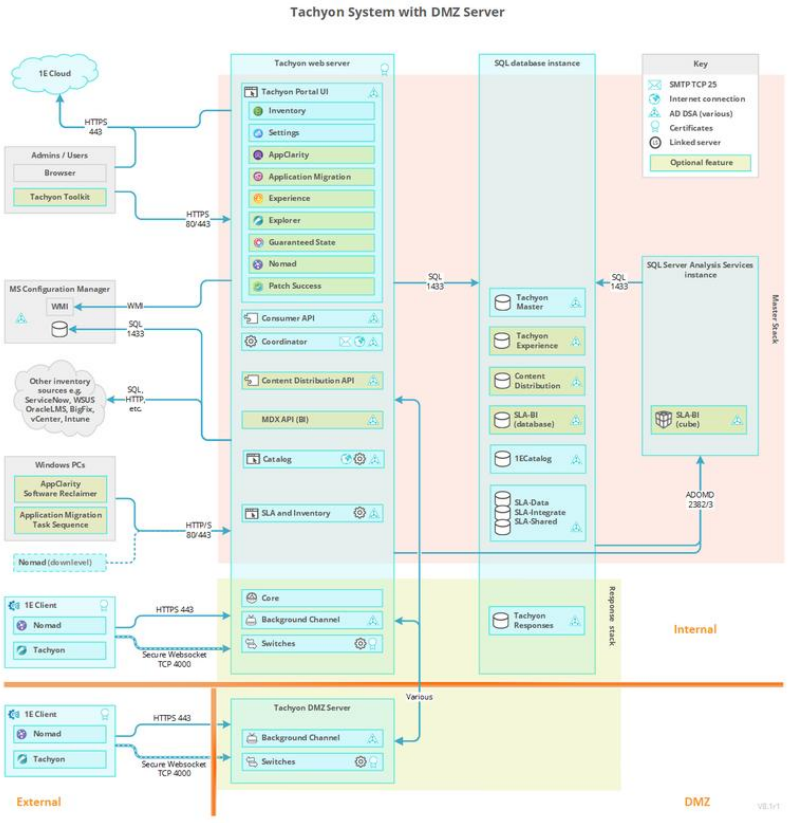
- Run Tachyon Setup on the Tachyon Response Stack to tell it about the DMZ Server, which will do the following:
  - Prepare the Master database with relevant details of the DMZ Background Channel and Switch(es)
  - Raise the security level of the Core and Switch communications
  - Produce a configuration file for the DMZ Server.
- Run Tachyon Setup on the DMZ Server using the pre-prepared configuration file, to complete the installation of DMZ Background Channel and Switch(es).

Detailed steps for the above process can be found on the Implementing a Tachyon DMZ Server page.

Tip

The DMZ picture shows a dual firewall design, but a single firewall is also supported.

In the picture, components colored green are optional in a Tachyon system.



1.2 Quick Start

How to quickly install, configure and run Tachyon for first use in a small-scale lab, evaluation, or pilot environment.

To simplify things, this quick start assumes a simple design in which you will install Tachyon components on a single web server, with SQL Server, installedTachyon components on a single web server, with SQL Server installed either locally or remotely (split). When implementing in a more complex environment you should instead follow the design, install and verify phases described in the Planning for Tachyon section.

This quick start is intended only for a fresh install. For upgrading or replacing an existing system, please see Upgrading Tachyon Platform.

There are four stages to the Tachyon quick start. Each of these stages touches upon the design, install, and verify phases described in the Planning for Tachyon section.

1.2.1 Verifying Tachyon

This quick start provides an outline for installing, configuring, and verifying a Tachyon system that is suitable for a lab-type environment. After the Prepare and Install sections, the Configure and Use sections provide steps that will verify the following aspects of Tachyon installation:

1. Configure quick start users - confirms integration with Active Directory and the basic RBAC capabilities of Tachyon.
2. Verification instructions - confirms the basic functionality for importing instruction definitions into Tachyon as well as confirming that licensing is working appropriately.
3. Viewing connected devices - confirms that Tachyon certificates have been correctly configured
4. Asking a question - confirms that Tachyon client communications are working
5. Performing an action - confirms that two-factor authentication, email connections, and the approval workflow are working. The stage 2 verification action also checks that the Tachyon client download mechanism is working and that the background channel has been correctly configured.

This run-through of basic Tachyon functionality works as a verification of Tachyon installation in a lab environment. If you see any issues when running through these steps please check the Troubleshooting section for a list of known issues. For production environments, a more formal verification process that uses the same **1E-TachyonPlatform.zip** file as used in this quick start guide is provided on the Verifying page.

1.2.2 Prepare

This quick start assumes a simple design in which you will be installing Tachyon components on a single web server, with SQL Server installed either locally or remote (split).

A summary of the preparation tasks:

1. Get a suitable license file for Tachyon, this should cover the Tachyon applications you want to use.
2. Review your Quick start infrastructure.

3. Prepare the Quick start Tachyon servers.
4. Create the DNS Name.
5. Install IIS on the Tachyon server.
6. Get and install the Tachyon Server's web server certificate - Request a Web Server certificate.
7. Get and install a certificate on the Tachyon Server with at least **Client Authentication Enhanced Key Usage**. You might find that your Tachyon Server web certificate has this already, but that will not usually be the case.
8. Get the Tachyon files that will be used to complete the quick start.
9. Prepare the Quick start Tachyon client devices.
10. Create the Quick start user accounts.

The below process assumes your quick start environment has a Microsoft Enterprise CA and you are familiar with how to:

- Configure your CA to use a CRL DP that supports HTTP or HTTPS
- Publish a Web Server certificate template or issue a PFX
- Use **certlm.msc** or the **mmc** certificates snap-in to request a web server certificate
- Deploy computer certificates to clients, optionally using auto-enrollment.

1.2.2.1 Quick start infrastructure

A Tachyon system consists of:

- Tachyon Server, which includes the Tachyon Switch component and website, hosted on an IIS web server
- SQL Server instance, which hosts the Tachyon Master and Responses databases, can be local or remote (split)
- Tachyon clients on supported devices
- Browsers used by Tachyon users and administrators to access the Explorer and Admin portal.

Your environment also requires:

- A correctly routed network environment where each device is configured with a genuine default gateway
- The server where your Tachyon Web Server will be installed also needs internet access so that the licensing will work, specifically to https://license.1e.com
- AD domain for the Tachyon Server and user accounts, but Tachyon client devices can be in workgroups or other domains
- SMTP email server - See Email and 2FA requirements for more details

- A PKI which serves the Tachyon Server and all Tachyon client devices
- Your CA(s) are able to issue certificates with a CRL DP that supports HTTP or HTTPS.

Remote SQL

If using a remote SQL Server in a test environment, and you want to configure the Tachyon Server to support more than 500 devices, then you can either ignore the warning that you should have an additional network interface used for SQL traffic, or you can install and configure an additional network interface as described in Configuring a persistent route for SQL traffic.

PKI notes

If you have an existing PKI and have just added a new CDP to support HTTP/S then you will need to re-issue certificates to your servers and devices.

Tachyon deliberately does not work with self-signed certificates for security reasons. Therefore, Tachyon Server cannot be installed on the same server as a Root CA, because its certificate is self-signed. For the same reason, client cannot be installed on a DC unless the client's Switch is configured to not require client certificates.

Tachyon uses TLSv1.2. If your PKI is using SHA512, then please ensure that your environment has relevant updates applied, as described in KB2973337. See Enabling SHA-512 to work with TLSv1.2.

If you want Tachyon to manage any legacy OS that Microsoft no longer supports, there may be issues with encrypted certificates described in Constraints of Legacy OS.

1.2.2.2 Quick start Tachyon servers

These are the servers required by Tachyon in addition to Quick start infrastructure.

Server	Software	Hardware
Tachyon Server	Windows Server 2016, 2019 or 2022 Full .NET Framework 4.8 or later	1 CPU Core, 1GB RAM if Web Server only. 2 CPU Core, 2GB RAM if using combined Web and SQL Server.
SQL Server	SQL Server 2017 or 2019, Standard or Enterprise	1 CPU Core, 1GB RAM if SQL Server only.

Server(s) can be physical or virtual, and must be domain joined.

If using any other version of Windows OS or SQL Server, or more detail is required, please refer to Windows Server requirements, and Server Provisioning.

If using a firewall on the Tachyon Server, then ensure the following incoming ports are open:

- Website HTTPS 443

- Switch Port 4000

If more detail is required, refer to Communication Ports in the Reference section.

1.2.2.3 DNS Name

Create the DNS Name for the Tachyon Server, for example **Tachyon.acme.local**

This can be a CNAME or a (A) Host record.

This DNS Name is used in the Web Server certificate (refer to Request a Web Server certificate) that needs to be installed on the TachyonServer.

1.2.2.4 Install IIS

Run the following PowerShell script on the Server. Do this even if IIS is already installed because it will ensure all the required features and roles are installed.

> **Note**
>
> If you intend to install Tachyon by running setup, then you may choose to let the setup program perform this operation for you instead of downloading and running the script manually. Just click on the **Install missing prerequisites** button after you have run the checks in the **Check prerequisites** page.

If more detail is required, refer to, Windows Server roles and features.

> **Note**
>
> View RolesInstall.ps1 ...
>
> Click here to download - RolesInstall.ps1
>
> **RolesInstall.ps1 - Configure IIS using PowerShell**

```
Import-Module ServerManager

Get-WindowsFeature | Out-file $PSScriptRoot\ServerManager-1.txt -Append
Install-WindowsFeature Web-Server,
Web-Http-Redirect,
Web-Dyn-Compression,
Web-Basic-Auth,
Web-IP-Security,
Web-Windows-Auth,
Web-Asp-Net45,
Web-Mgmt-Console,
Net-Framework-45-Core,
Net-Framework-45-ASPNET

Uninstall-WindowsFeature Web-DAV-Publishing

Get-WindowsFeature | Out-file $PSScriptRoot\ServerManager-2.txt -Append
```

> **Note**

When running the above command, if you receive an error that contains **The source files could not be downloaded** you will need to supply the source path to your Windows Server OS installation media \Sources\sxs folder.

Append **-source X:\Sources\sxs** or **-source \\Server\Path\Source\sxs** to the command line, adjusted for your drive letter or UNC path.

Note

PowerShell always uses **45** in the names of .NET Framework features, irrespective of the actual version of .NET Framework 4.X installed on the server, like:

- 4.8 in Windows Server 2022 (note: from Tachyon 8.1 onwards, any Tachyon component that requires .NET Framework, requires version 4.8)
- 4.7.2 in Windows Server 2019
- 4.6.2 in Windows Server 2016

For details of .NET Framework versions, please refer to https://docs.microsoft.com/en-us/dotnet/framework/get-started/system-requirements#supported-server-operating-systems.

Tip

Tip

If you prefer to use the Add Roles and Features Wizard to manually enable features then you can use the Display Names listed in the table Windows Server roles and features.

Note

Web-Http-Redirect is only required to support legacy Nomad clients after an In-place upgrade of ActiveEfficiency Server for Nomad.

Web-Basic-Auth is only required if you will be installing 1E ITSM Connect or 1E Core for integrating ServiceNow and Tachyon.

1.2.2.5 Request a Web Server certificate

You will need to have requested a Web Server certificate from your Certificate Authority. To get the certificate in your organization you will have either:

- Submitted a CSR and received a password protected PFX file
- Used the Certificate Enrollment wizard to request a suitable Web Server certificate.

Once the Web Server certificate has been provided it must be imported into the Tachyon Server's **local computer Personal Certificates** store.

Each server that has Tachyon Server components installed requires its own Web Server certificate (except for a remote SQL Server). This certificate is also used by the Tachyon Switch and the Tachyon Coordinator. Therefore, a single-server installation requires only one Web Server certificate. This certificate must be provided on the server prior to installation of Tachyon.

The Web Server certificate requires the minimum of the following:

1. Issued by a trusted Certificate Authority (CA)

- The certificate for the Root CA in the Certification Path must exist in the Trusted Root CA store of the server
- If the issuing CA is not the Root CA then the certificate for the issuing CA and any intermediate CA in the Certification Path must exist in the Intermediate CA store of the server
- The above CA certificates must exist on the Tachyon Web Server and Windows client devices
- Most organizations have automated distribution of these CA certificates to servers and clients, using Group Policy for example.

2. Has at least the following Key Usage:
   - Digital signature
   - Key encipherment
3. Has at least the following Enhanced Key Usages:
   - Server Authentication
4. Revocation information is included
   - References at least one CRL Distribution point that uses HTTP - see DMZ Server note below
5. Must have a private key available

Tip

The default template **Web Server** available with a Microsoft PKI is suitable for requesting a Tachyon Web Server certificate.

DMZ Server

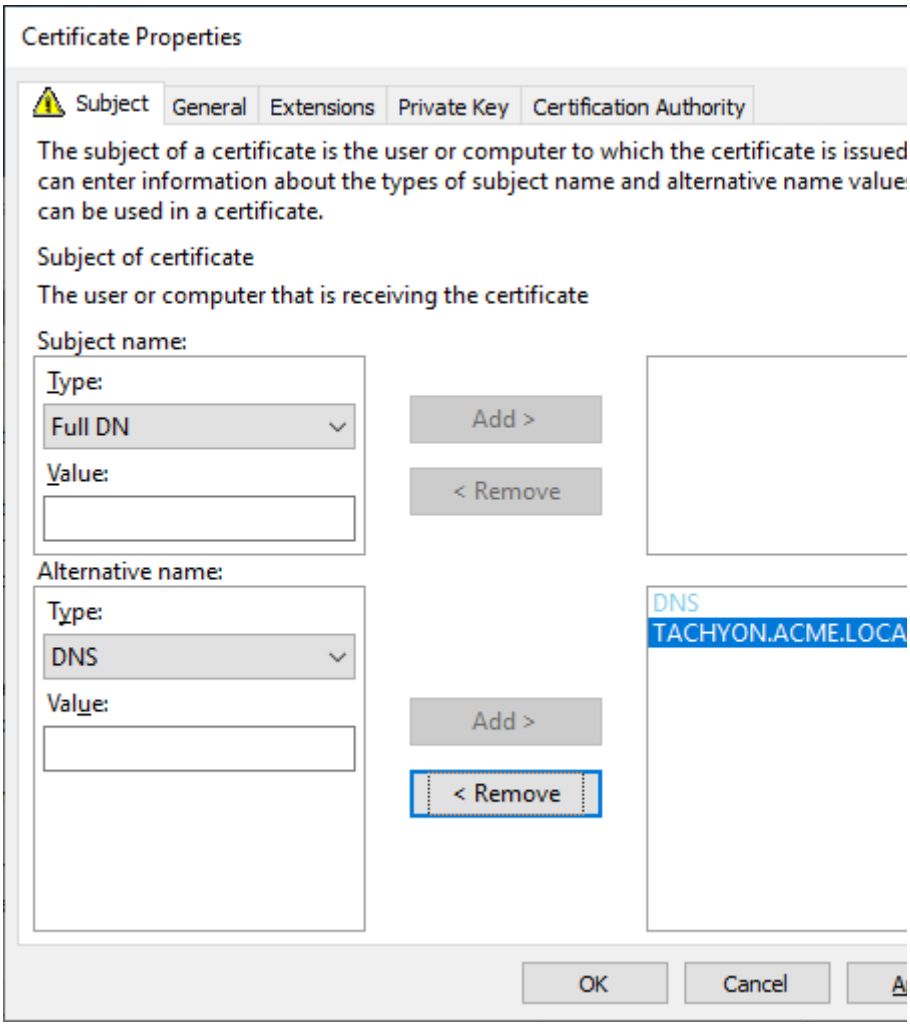
Please ensure you note the additional certificate requirements described below, when installing any server in a system that also contains a DMZ Server. Internal Master and Response Stack servers, and DMZ Server, each require **two** HTTPS bindings, as described in DNS Names. For even more detail, please refer Implementing a Tachyon DMZ Server.

Also note the requirement for server certificates to reference at least one CRL Distribution point that uses HTTP. These CRL DPs are likely to be in the internal network, and the firewall will need to allow the DMZ server to access these internal servers.

Web Server certificates used by a Tachyon Servers must be issued with their fields set as follows. Example **DNS Names** are discussed in DNS Names.

Fields	Example Option 3 type certificate
Subject Common Name Field (subject:commonName)	Subject (CN) can be any valid name, and is no longer mandatory as required by previous versions of Tachyon.

Fields	Example Option 3 type certificate
Subject Alternative Name Extension (extensions:subjectAltName), type dnsName	The **Tachyon Server DNS Name FQDN** (DNS Alias) of the server. This is mandatory, same as required by previous versions of Tachyon. On a Master Stack - example: **DNS Name=Tachyon.ACME.LOCAL** On a Response Stack - example: **DNS Name=TachyonRS.ACME.LOCAL** On a DMZ Server - example: **DNS Name=TachyonEXT.ACME.COM**
Subject Alternative Name Extension (extensions:subjectAltName), type dnsName	An **Alternate DNS Name FQDN** (DNS Alias) of the server. This is usually mandatory, for example if there is more than one server in your Tachyon system, as discussed in DNS Names. On a Master Stack, example: **DNS Name=TachyonALT.ACME.LOCAL**or**DNS Name=Tachyon.ACME.LOCAL** On a Response Stack - example: **DNS Name=TachyonALT.ACME.LOCAL** On a DMZ Server - example: **DNS Name=TachyonDMZ.ACME.LOCAL**

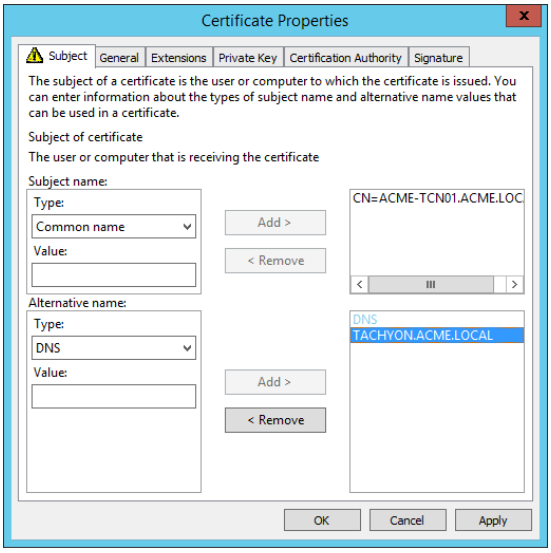
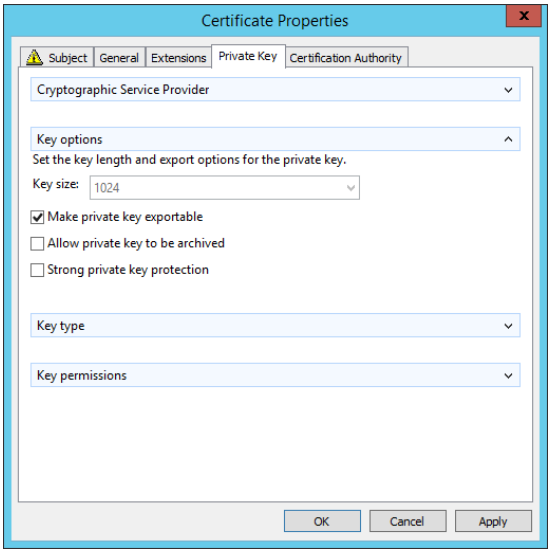
Fields	Example Option 3 type certificate
Example	

Note

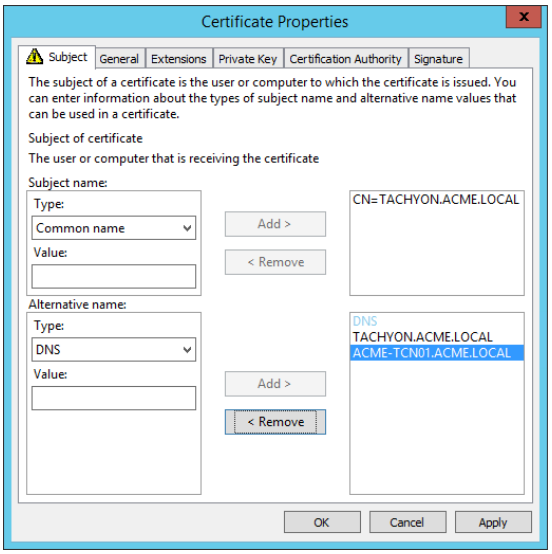
Earlier versions of Tachyon required the certificate to have a CN and used SAN fields differently. If you are upgrading your Tachyon server from an earlier version, it may still be using this type of certificate. When upgrading Tachyon, you can issue a replacement certificate, or continue using the old style certificate (because the new-style certificate requires only a SAN DNS Name that matches the DNS Alias, which are provided by the old style certificates).

Click here to see examples of old-style certificates...

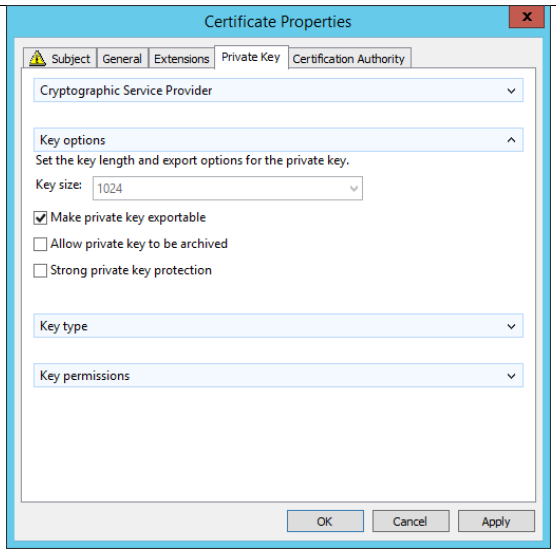
Fields	Example old Option 2 type certificate
Subject Common Name Field (subject:commonName)	The computername FQDN of the server

Fields	Example old Option 2 type certificate
	Example: **CN=ACME-TCN01.ACME.LOCAL**
Subject Alternative Name Extension (extensions:subjectAltName), type dnsName	The DNS Alias FQDN of the server Example: **DNS Name=Tachyon.ACME.LOCAL** **Tip** Add any additional DNS Names here.
Example certificate request	  **Note** Option 2 type certificates required the CN to be the computername FQDN, and the list of

Fields	Example old Option 2 type certificate
	Subject Alternate Names (SAN) to contain the DNS Alias. Also, prior to Tachyon 5.0 the certificate required its private key to be exportable. Tachyon 5.0 and later is able to use this type of certificate when upgrading from an earlier version of Tachyon.

Fields	Example of old Option 1 type certificate
Subject Common Name Field (subject:commonName)	The DNS Alias FQDN of the server Example: **CN=Tachyon.ACME.LOCAL**
Subject Alternative Name Extension (extensions:subjectAltName), type dnsName	The DNS Alias FQDN of the server Example: **DNS Name=Tachyon.ACME.LOCAL** The computername FQDN of the server Example: **DNS Name=ACME-TCN01.ACME.LOCAL**
Example certificate request	

Fields	Example of old Option 1 type certificate



Note

Option 1 type certificates required the CN to be the DNS Alias, and the list of Subject Alternate Names (SAN) to contain the computername FQDN.

Also, prior to Tachyon 5.0 the certificate required its private key to be exportable.

Tachyon 5.0 and later is able to use this type of certificate when upgrading from an earlier version of Tachyon.

1.2.2.6 Request a client certificate

You will need to have requested a client certificate from your Certificate Authority. This will be used to authenticate communications between the **Background Channel** and the **ContentDistribution** components to support Nomad features.

1.2.2.7 Get the Tachyon files

You will need to download the following to complete the quick start.

1.2.2.7.1 1E Client installers

The **1EClient zip** file can be downloaded from the 1E Support Portal https://1e.my.site.com/. The zip includes the following files used to install the 1E Client on Windows devices:

- **1E.Client-x64.msi**
- **1E.Client-x86.msi**

1.2.2.7.2 Tachyon Server installers

The **TachyonPlatform zip** file can be downloaded from the 1E Support Portal (https://1e.my.site.com/). Extracting the zip will create a folder structure containing the following, where the files highlighted in bold are required by Tachyon Setup.

- Licenses.txt
- Tachyon Release Information.html
- **Tachyon.Setup.exe**

Please refer to:

- Tachyon Setup, for detailed information about each screen in setup
- Quick Start if you want a brief overview of installing Tachyon .

Warning

Tachyon Setup is the only supported method of installing, upgrading, and patching a Tachyon server.

Installation using standalone **msi** or **msp** files is not supported unless advised by 1E, which may be necessary in complex installations, using non-interactive (quiet/silent) command-lines, and may require further post-install configuration steps.

- Installers**1ECatalog.msi**
- Installers**AppClarity.msi**
- Installers**ApplicationMigration.msi**
- Installers**ContentDistribution.msi**
- Installers**SLA.BI.Installer.msi**
- Installers**SLA.Platform.Installer.msi**
- Installers**TachyonServer.msi**
- Installers\TachyonToolkit.msi

This folder contains **msi installer files** for components and applications that will be installed by Tachyon Setup if their prerequisites are met.

- Installers\Apps\Experience**Experience.zip**
- Installers\Apps\Experience**metadata.json**

This folder contains **apps folders** for Tachyon consumer applications that will be installed by Tachyon Setup if their prerequisites are met.

- Installers\Apps\Explorer**Explorer.zip**
- Installers\Apps\Explorer**metadata.json**
- Installers\Apps\GuaranteedState**GuaranteedState.zip**
- Installers\Apps\GuaranteedState**metadata.json**
- Installers\Apps\Inventory**Inventory.zip**
- Installers\Apps\Inventory**metadata.json**
- Installers\Apps\Nomad**metadata.json**
- Installers\Apps\Nomad**Nomad.zip**
- Installers\Apps\PatchSuccess**metadata.json**
- Installers\Apps\PatchSuccess**PatchSuccess.zip**
- Installers\Apps\Settings**metadata.json**
- Installers\Apps\Settings**Platform.zip**
- ProductPacks\Newtonsoft.Json.dll
- ProductPacks\Tachyon.ProductPackDeploymentTool.exe
- ProductPacks\Tachyon.ProductPackDeploymentTool.exe.config
- ProductPacks\Tachyon.SDK.Consumer.dll
- ProductPacks\Classic\1E-ConfigMgrConsoleExtensions.zip
- ProductPacks\Classic\1E-Experience.zip

If you do not want to install a consumer application, then delete the folder before running setup.

Later, if you need to install the consumer application, then you can reinstate the folder and install the app using setup as described in Applications maintenance.

> **Note**
>
> Some consumer applications are installed using their msi instead of an apps folder, for example AppClarity and Application Migration.

These Product Pack are required to support various features, for more detail please refer to Tachyon Product Packs reference.

If your license permits, you can use additional Product Pack available from 1E Exchange (https://exchange.1e.com/) to meet specific use-cases.

Classic Product Packs	Contain instructions, for use in Explorer and other Tachyon applications. They can be uploaded using the **PPDT**, or using **Settings→Instructions→I**

- ProductPacks\Classic\1E-Explorer-TachyonAgent.zip
- ProductPacks\Classic\1E-Explorer-TachyonCore.zip
- ProductPacks\Classic\1E-Inventory.zip
- ProductPacks\Classic\1E-Nomad.zip
- ProductPacks\Classic\1E-Patch-Success.zip
- ProductPacks\Classic\1E-Tachyon-Platform.zip
- ProductPacks\Integrated\MEMCMClientHealth.zip
- ProductPacks\Integrated\NomadClientHealth.zip
- ProductPacks\Integrated\TachyonCore.zip
- ProductPacks\Integrated\WindowsClientHealth.zip

nstruction sets page in the Tachyon Portal.

Integrated Product Packs

Contain policies, rules and fragments for use by Guaranteed State , and may also include instructions.

They can only be uploaded using the **PPDT**.

Tip

The **Tachyon Product Pack Deployment Tool** can be started independently or at the end of the **Tachyon Setup** process via the Post-installation checks screen, where the screen contains a link that launches the tool. The **Tachyon Setup** method of starting the tool is recommended because Tachyon Setup ensures you have the correct permissions to upload the Product Packs.

1.2.2.8 Quick start Tachyon client devices

The Tachyon client is supported on the following Windows OS in a quick start environment.

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows 11 CB 21H2
- Windows 10 CB 21H2
- Windows 10 CB 21H1
- Windows 10 CB 20H2

If using any other OS then please refer to Supported Platforms and Tachyon client installation pages in the Reference section.

Tachyon users on client devices can connect to the Tachyon Explorer using any of the following browsers:

Latest version of:

- Google Chrome
- Microsoft Edge (Chromium)
- Mozilla Firefox.

PowerShell is used by some Tachyon Product Packs. If more detail is required, refer to Tachyon scripting requirements.

If you have configured Tachyon Server to require client certificates (Client certificates) then each device requires a certificate with the following properties, so the Tachyon client can be authenticated by the Tachyon Switch.

1. Issued by a trusted Certificate Authority (CA)
   - The certificate for the Root CA in the Certification Path must exist in the Trusted Root CA store of the client
   - If the issuing CA is not the Root CA then the certificate for the issuing CA and any intermediate CA in the Certification Path must exist in the Intermediate CA store of the client
   - If either of these CA certificates are different to those used by the Tachyon Web Server, they will need to be exported and imported on the Tachyon Web Server
   - Most organizations have automated distribution of these CA certificates to clients and servers, using Group Policy for example.
2. Has at least the following Enhanced Key Usage
   - Client Authentication
3. Has at least the following Key Usage
   - Digital Signature
   - Key encipherment
4. Has a private key
   - For workgroup and non-Windows devices, the **private key must be exportable**
5. Revocation information is included.
   - References at least one CRL Distribution point that uses HTTP.
6. Has a Subject Name of type Common Name (**CN=<computername>**) or Subject Alternative Name (**DNS Name=<computername>**) where <computername> depends on the type of device:
   - On domain-joined Windows PCs this must be the **computername FQDN** of the computer, for example **W701.ACME.LOCAL**
   - On workgroup Windows PCs and non-Windows devices, this must be the computername of the computer - as returned by the **hostname** command, for example on Windows PC this could be **W701**, and on a Mac this could be **MAC01.local**

Note

Tachyon clients and Switches use OpenSSL and its validation process to verify certificates.

1.2.2.9 Quick start user accounts

For simplicity in the quick start guide, we use just two Tachyon user accounts, the installation account and another full administrator account.

Note

To get things up and running quickly in a lab environment, you may want to make use of the full administrator role. This will help minimize the number of users required for an evaluation and reduce the initial configuration required.

To further minimize the number of users needed, you can also enable the Windows account used to install Tachyon to assume the Tachyon full administrator role. The installation account is added as the system principal user in Tachyon by the installer, and its permissions are locked down by default. You can allow it to assume the full administrator role using the following steps:

1. Create a Tachyon user from an existing AD security group.
2. Apply the Tachyon full administrator role to the user.
3. Add the installation account to the AD security group.

In the short term it's fine to make use of full administrators in this way, but this practice is not really suitable for large-scale deployments and should be used with care for the following reasons:

- The full administrator role has permissions to do everything in Tachyon. It has across the board permissions to all Instruction Sets and therefore can be used to run actions that can have a major impact on your network.
- The full administrator accounts receive emails for all the transactions that are performed by Tachyon.

For the purposes of the quick start, which uses two-factor authentication, each account must have its AD account configured with an email address.

Note

If two-factor authentication is enabled (as it is by default) email is required for any user who intends to run an action, in this case **TCNInstaller01**.

Using just the following accounts we can perform all the installation, administration, verification questions, actions and approval tasks shown in this quick start guide.

Account	Description	Tachyon roles
TCNInstaller01	Server installation account, used to install Tachyon Server and	The roles for this account cannot be changed directly, but this account

Account	Description	Tachyon roles
	configure initial security user and roles settings. This account requires the following rights: • Full Administrator rights on the Tachyon Server • **Sysadmin** rights on the SQL Server instance • **Read-only Analyst** permissions in Configuration Manager. This account should be a member of the **TCNGAdministrators** group	may be added to AD groups with other Tachyon permissions assigned.
TCNAdmin01	A user account that will be used in combination with the **TCNInstaller01** user to enable the request and approval of actions.	No direct roles applied to this account.
TCNGAdministrators	An AD **Universal** group with two members: **TNCInstaller01** and **TCNAdmin01**.	**Global Administrators** role.

1.2.2.10 Quick start service accounts

The table below describes all the service accounts and where they are used. Where domain accounts are required, you should create separate domain user accounts for each service.

Account	Description
CATSVC	1E Catalog Update Service account. Used by the 1E Catalog Update service to connect to the 1E Cloud service via the Internet to download catalog updates and upload anonymous details about newly detected software. Used by the Catalog web application pool to connect to the 1ECatalog database on the SQL Server database instance.

Account	Description
BISSASSVC	Business Intelligence (BI) SSAS user account. Used to access the BI cube on the SSAS instance by services on the web server and the linked server on the SQL Server database instance.
SLATACHYON	A Tachyon user account that will be used by the 1E Platform Connector, which provides the Tachyon Inventory. This account will be a member of the **1E Inventory** custom role, which has questioner permissions on the **1E Inventory** instructions set. The instruction set contains four instructions. You can choose different names for this role and instruction set.
Network Service	On local servers, this is **NT AUTHORITY\Network Service**; on remote servers, this is: **ACME\computer$** where computer is the computer name of the Tachyon Server. Used by the following for connection to databases on the SQL Server database instance: • All web application pools for Tachyon and SLA, except where noted elsewhere in this table • All Windows services for Tachyon and SLA except where noted elsewhere in this table. Used by the Tachyon Coordinator service to connect to the 1E license cloud to validate and activate your license. Used by the System Center Configuration Manager (SCCM) Connector if the connector configuration has **Use Windows Authentication** enabled instead of a SQL Login.
Local System	Used by the Tachyon Switch Host service.

1.2.3 Install

1.2.3.1 Tachyon Server

After obtaining your **Tachyon.lic** file from 1E you should store it in a secure location. In our example we've placed the **Tachyon.lic** file in the installation directory where **Tachyon.Setup.exe** is located.

1. Logon to the server using the server installation account **TCNInstaller01**.

2. Install interactively using **Tachyon.Setup.exe**.

3. Launch the setup wizard by double-clicking on **Tachyon.Setup.exe**. Then fill out the screens of the wizard using the following information.

Screen	Actions
Welcome	Click **Next** to skip to the next screen.
Documentation	This page provides some links to some online information about Tachyon. Click **Next** to skip to the next screen.
License agreement	Accept the license agreement by checking the **I accept the terms of the license agreement** checkbox and click **Next**.
License File	Enter the location for your Server **Tachyon.lic** license file, or click **Browse** to locate the file using the system file browser. When the **.lic** file is selected, it will be verified with the Tachyon license server. If everything is OK, click **Next**.
Select configuration	This screen lets you select the configuration you want to install, which determines which components are installed on the server. The quick start example installs all the Tachyon Server components onto a single-server with the databases on a remote SQL instance, so ensure that the **All components on a single server** option is selected and then click **Next**.
Check prerequisites	This screen performs prerequisite checks on the local server and user account. Click **Start checking** to start the checks. If any of the checks fail, **Tachyon Setup** may be able to install the missing prerequisites. To install these, click the **Install missing prereqs.** button. Not all prerequisite checks have automated fixes. If your environment fails a check and the **Install missing prereqs.** button has not been enabled, you will need to fix the conditions for that check by hand. You can click **Check Again** to re-run the checks once any remediation steps have been made.
Server certificate	This screen displays a list of certificates from the **Local Computer\Personal** certificate store, and you select the certificate created earlier, as described in the Request a Web Server certificate heading. **Tachyon Setup** will then evaluate the suitability of the selected certificate according to how specific properties of the certificate have been configured.

Screen	Actions
	In this quick start example, we select the certificate with the friendly name of **Tachyon Web Certificate**, confirm all checks pass and click **Next** to continue.
Client certificates	On this screen, you can set whether client certificates are required to be presented by the Tachyon clients. If your clients do not have certificates, then uncheck the **Switches require client certificates to be presented by Tachyon client features of the 1E Client** checkbox. If your clients have certificates issued by different Certificate Authorities than the Tachyon Server certificate, then you must ensure clients and Switch servers each have the others CA certificates in their certificate stores. For the quick start, client certificates are required from the Tachyon clients, and as all the clients in the quick start example use the same certificate authority as the Tachyon Server, you can skip this screen by clicking **Next** to continue.
Database servers	Select the SQL server instance name for the Tachyon Master and Responses databases as well as the SQL server instance names for the 1E Catalog, SLA and BI databases. In the quick start example, these will all be installed on the **ACME-SQL01** instance. It's also a good idea to click the **Validate** button to ensure that the specified instance is valid before continuing by clicking **Next**.
SSAS servers	Here you need to set the domain account details for the BI SSAS user. This user will be used to create a linked server for the BI database to access the BI cube and enable BI services on the server to query the cube. You also enter the SQL Server Analysis Service (SSAS) instance, where the BI cube will be created. In the quick start example, the account name and password for the domain account **ACME\BISSASSVC** are used. The SSAS instance for BI is set to **ACME-SQL01**, where an SSAS instance has been set up alongside the SQL Server instance used for the main Tachyon databases.
Number of devices	Enter the number of devices to match your license key. The quick start example is limited to 15 by the **Tachyon.lic** file selected on the **License File** screen. You can change this number from the default, but it should not be set larger than your permitted licenses.

Screen	Actions
Switch configuration	The default switch configuration displayed is determined by the number of devices set on the **Number of devices** page. For the quick start, we leave this as the suggested default. In the quick start example we click **Validate** to check that the selected configuration is appropriate, all the checks pass, so we then click **Next** to continue.
Website configuration	Verify the following details for **Main website bindings**: HTTP Host Header: Hostname FQDN of the Tachyon Server. In the quick start example, this is set to **ACME-TCN01.acme.local**. HTTP Port: 80 HTTPS Host Header: DNS Name FQDN of the Tachyon Server. In the quick start example, this is set to **Tachyon.acme.local**. HTTPS Port: 443 For the quick start, the **Alternate website bindings** are not used, so you can leave these at their default settings. Verify the following service ports: Workflow port: 8081 Integrate REST port: 6002 Click **Next** to continue.
Active Directory and email	Enter the following: Active Directory: GC:// Enable email: Emails are used to inform approvers of pending notifications, and users of pending results expiry. **Note** You should only enable this if you have a working email system which supports SMTP.

Screen	Actions	
	SMTP Server	FQDN of your SMTP gateway. In the quick start example, this is **ACME-EXC01.ACME.LOCAL**.
	SMTP Port	25
	Mail From	Mail-from email address used by the Tachyon Server when it sends emails to users. In the quick start example, this is set to **Tachyon@acme.local**.
	Enable two-factor authentication	Emails are used to send authentication codes to users who submit actions. **Note** ONLY enable this if you have a working email system which supports SMTP.
	In the quick start example, we click **Validate** to check that the options are valid, and then click **Next** to continue.	
SLA and 1E Catalog	On this screen, you can enable or disable the AI Powered Auto-curation feature. This is supported by SLA but also involves downloading the AI files using 1E Catalog. In the quick start example, we leave this in the default state, where the **Enable AI-based auto-curation** checkbox is not checked, and the feature is disabled, and then click **Next**. You should only enable this feature if you have appropriate hardware. You can enable this feature later. For more information, please refer to AI Powered Auto-curation.	
Nomad	If you selected to install **Content Distribution** on the **Select Configuration** screen you will need to provide the server name for a Microsoft Endpoint Manager Configuration Manager (MEMCM, ConfigMgr) site server. In the quick start example, we enter **ACME-CM01** as the Configuration Manager Site server and leave the Nomad sync at its default value of **30**. Clicking **Validate** checks the connection to the CM Site Server. We then select the Client Authentication certificate, requested earlier under the Request a client certificate heading, that will be used to authenticate	

Screen	Actions
	communications between the Background Channel and the ContentDistribution components. The clients authentication we leave at the default of **Windows authentication**. Clicking the **Validate** button verifies the selected Client Authentication certificate. Then click **Next** to continue.
Ready to install	Having entered all the necessary values, click the **Install!** button to begin the installation.
Installation results	The **Installation results** screen displays the log messages from the installer as they occur. Confirm that the installation has succeeded by checking that the concluding log message says: **The installer exited and reported successful completion** then click **Next**.
Post-installation checks	Run the post-installation checks by clicking the **Start checking** button. Confirm that all checks pass. **Note** You can click on the **Open** link to the right of the **Tachyon Portal web application responds** check to open the Tachyon Portal. If you get green ticks all the way down, then your Tachyon Server installation has been successful, and you can now close the setup wizard by clicking the **Close** button. If any of the checks failed, you can see more information about the check in the **Info** column. Which you can then use in combination with the Troubleshooting section to help track down the cause of the issue. If you have unzipped the contents of the **TachyonProductPacks** zip file to a **ProductPacks** folder in the same folder where **Tachyon.Setup.exe** resides, a **Product Packs are available** check will be displayed with a link that launches the **Tachyon Product Pack Deployment Tool**. In this initial quick start video, we pause the setup at this point and continue with the process under the Uploading with the Tachyon Product Pack Deployment Tool heading.

Screen	Actions
Maintenance	This section of setup is used to configure Tachyon post-installation. Here you can uninstall components, configure applications and replace certificates.

For more detail on the setup wizard, read Tachyon Setup in Installing Tachyon.

> **Note**
>
> You can now choose to launch the Tachyon Portal by browsing to: **https://<TachyonDNSName>/Tachyon**, where **<TachyonDNSName>** is the DNS name you have configured for Tachyon in your environment. In our example, this is **https://tachyon.acme.local/Tachyon**.

1.2.3.2 Uploading with the Tachyon Product Pack Deployment Tool

Continuing from the previous section, we select to run the **Tachyon Product Pack Deployment Tool** using the following steps:

1. In setup click on the **Deploy** link next to the **Product Packs are available** check on the **Post-installation checks** screen.
2. The **Tachyon Product Pack Deployment Tool** appears, showing all the **Available Product Packs** that were found in the **ProductPacks** folder.
3. There are two types of Product Pack displayed, **Classic** and **Integrated**. **Classic** Product Packs contain Instruction definitions, and **Integrated** Product Packs also include Policies.
4. You can select the Product Packs you want to load by checking the box in the **Selected** column for each entry. In our example, we'll leave all the Product Packs selected to load them all.
5. To load the Product Pack, click on the **Upload selected** button.
6. When the upload has completed, the text **Done** will appear in the **Results** field.
7. At this point, you can click the **Close** button to close the **Tachyon Product Pack Deployment Tool**.
8. Then click the **Close** button in setup, and click **OK** in the confirmation dialog to exit the wizard.

Signing in to the Tachyon Portal to check the Instructions from the uploaded Product Pack:

1. Enter the URL for the Tachyon Portal into a suitable browser for example **https:\\Tachyon portal.acme.local\Tachyon**.
2. Sign in using your installation account credentials, for example **ACME\TCNInstaller01**.
3. When the Tachyon Portal has finished loading, click on **Settings** at the bottom of the list of applications.
4. When the **Settings** application has opened, click on **Instructions** and then **Instruction sets**.
5. On the **Instructions sets** page, you will be able to see Instruction sets that have been created for each Product Pack that was in the **ProductPacks** folder.

1.2.3.3 Verification instructions

By following the steps provided in Uploading with the Tachyon Product Pack Deployment Tool you will have loaded the **1E-Tachyon-Platform.zip** Product Pack into the **1E Tachyon Platform** Instruction set, containing the two verification instructions **Tachyon Platform verification stage 1** and **Tachyon Platform verification stage 2 (all platforms)**, along with a number of other instructions that are used to populate data in the Device View. The verification instructions are used later in the quick start guide to perform a quick verification of Tachyon and demonstrate how to ask questions and run actions.

1.2.3.4 Tachyon clients

When installing 1E Client (with Tachyon features enabled) the following installation settings are mandatory and must be supplied. Other client configuration settings are optional and have been assigned default values.

The following properties can be entered manually when installing from the Windows Installer wizard. Alternatively, the properties can be included as part of a Windows msiexec command-line launch.

Property	Mandatory	Setting
BACKGROUNDCHANNELURL	Yes	Set to the previously configured Tachyon DNS Name FQDN. You will also need to specify the port and the rest of the background channel URL. By default, the port is set to 443. In our example, this would be set to: `https://TACHYON.ACME.local:443/Background/`
SWITCH	Yes	Set to the previously configured Tachyon DNS Name FQDN. From version 3.1 onwards, you will also need to specify the port. By default, this is set to 4000. In our example, this would be set to: `TACHYON.ACME.local:4000`

1.2.3.4.1 Example which enables only Tachyon client

Example Windows 1E Client installer command-line with only the 1E Client features enabled, other client modules are not enabled. Tachyon uses HTTPS only.

```
msiexec /i 1E.Client-x64.msi SWITCH="tachyon.acme.local:4000" BACKGROUNDCHANNEL
URL="https://tachyon.acme.local:443/Background/" /qn /l*vx C:\Windows\temp\1ECl
ient-install.log
```

1.2.3.4.2 Example which enables only Nomad client

Example Windows 1E Client installer command-line with only **Nomad** module enabled, which also requires Tachyon client features to be enabled. Tachyon uses HTTPS only.

```
msiexec /i 1E.Client-x64.msi SWITCH="tachyon.acme.local:4000" BACKGROUNDCHANNEL
URL="https://tachyon.acme.local:443/Background/" MODULE.NOMAD.ENABLED=true MODU
LE.NOMAD.CONTENTREGISTRATION=1 MODULE.NOMAD.SSDENABLED=1 /qn /l*vx C:\Windows\t
emp\1EClient-install.log
```

1.2.3.4.3 Example which enables only PXE Everywhere Agent

Example Windows 1E Client installer command-line with only **PXE Everywhere Agent** client module enabled, and Tachyon features disabled (by setting SWITCH and BACKGROUNDCHANNELURL to none). PXE Everywhere uses only HTTP.

```
msiexec /i 1E.Client-x64.msi SWITCH=none BACKGROUNDCHANNELURL=none MODULE.PXEEV
ERYWHERE.ENABLED=true MODULE.PXEEVERYWHERE.CONFIGSERVERURL="http://pxecentral.a
cme.local/PXELite/PXELiteConfiguration.asmx" /qn /l*vx C:\Windows\temp\1EClient
-install.log
```

1.2.3.4.4 Example which enables only Shopping client

Example Windows 1E Client installer command-line with only **Shopping client** module enabled, and Tachyon features disabled (by setting SWITCH and BACKGROUNDCHANNELURL to none). Ensure you use HTTP or HTTPS as appropriate.

```
msiexec /i 1E.Client-x64.msi SWITCH=none BACKGROUNDCHANNELURL=none MODULE.SHOPP
ING.ENABLED=true MODULE.SHOPPING.SHOPPINGCENTRALURL="https://appstore.acme.loca
l/shopping" MODULE.SHOPPING.LOOPBACKEXEMPTIONENABLED=true /qn /l*vx C:\Windows\
temp\1EClient-install.log
```

1.2.3.4.5 Example which enables only WakeUp client

Example Windows 1E Client installer command-line with only **WakeUp client** module enabled, and Tachyon features disabled (by setting SWITCH and BACKGROUNDCHANNELURL to none).

```
msiexec /i 1E.Client-x64.msi SWITCH=none BACKGROUNDCHANNELURL=none MODULE.WAKEU
P.ENABLED=true MODULE.WAKEUP.REPORTINGSERVER="nwmserver.acme.local" /qn /l*vx C
:\Windows\temp\1EClient-install.log
```

Use **1E.Client-x64.msi** for 64-bit Windows and **1E.Client-x86.msi** for 32-bit Windows. For non-Windows platforms, platform specific packages for Linux, Solaris and Mac are available.

When installing interactively through the Windows installer wizard, logon using an account that has local administrator rights.

For details of step-by-step interactive and command-line installation, please see Deploying 1E Client on Windows.

For details of how to deploy the 1E Client to macOS platforms, see Deploying 1E Client on macOS.

For details of how to deploy the 1E Client to Linux platforms, see Deploying 1E Client on Linux.

1.2.3.5 Export all responses feature

This step is optional, only if you require this feature. Please refer to Tachyon Server post-installation tasks for details.

1.2.4 Configure

1.2.4.1 Set security roles

After installation you will only be able to log onto the Tachyon Explorer using the installation account. This account is purposefully restricted to just allowing the configuration of security roles. So the first step must be to add other users to access the other capabilities of Tachyon.

1.2.4.1.1 Users for administration

We suggest that you add a user or group to handle the administration tasks for your evaluation environment.

1.2.4.1.2 Users for performing actions

To perform actions you will need at least two other users. One an actioner and the other an approver, otherwise you won't be able to perform actions.

1.2.4.1.3 A Tachyon AD group tutorial

For this quick start guide we use two specific accounts and a security group to assign to the roles we need. You may want to use AD groups to define Tachyon access and we have provided a complete tutorial on adding users and roles via AD groups, on the Configuring Access Rights - tutorial page, which you may find useful.

1.2.4.2 Configure quick start users

At this point we will configure the user accounts, as listed in Quick start user accounts, to their different roles in Tachyon.

Using these accounts the user roles configuration is done using the following steps:

1. Logon to Tachyon using the installation account. The Tachyon Portal website will be available after installation using the Tachyon DNS Name FQDN, configured during the prepare phase of the quick start. In our quick start environment this is **tachyon.acme.local**. So the URL for the Tachyon Portal is:

   Note

   https://tachyon.acme.local/Tachyon

   The first time you log in the Tachyon applications will be set up.

2. Initially the installer account has purposefully limited Tachyon permissions and the permissions for this account cannot be modified directly. This means that the account cannot access any of the applications. To resolve this for the quick start guide, we need to create a new Tachyon user account for the **TCNGAdministrators** group and assign global administrator permissions to that user. To do this you need to navigate to the **Settings** application page using one of the following methods:

   a. If you're on the home page click on the **Settings** item.

   b. If you've already navigated to another application, click on the **Settings** item on the **Switch app** menu.

3. Once you're in the **Settings** application, to add the **TCNGAdministrators** group Tachyon user:

    a. Expand the **Permissions** node.

    b. Click on **Users** to display the **Users** page.

    c. Click the **Add** button to display the **Add user** popup.

    d. Enter some text in the **Select AD user or security group** field (for example, **TCNG**) that matches the required user or group name. In our example we know we will be adding a security group, so we can uncheck the **User** option so that the search only returns security groups.

    e. After clicking the search icon, a list of matching users and groups from AD will be displayed. Select **TCNGAdministrators** and click **Add**.

4. To set the full administrator role for the new **ACME\TCNGAdministrators** Tachyon user:

    a. Click on the new **ACME\TCNGAdministrators** username link to display its details.

    b. On the **Roles** tab click the **Edit** button to display the **Edit roles assigned to user** popup.

    c. Select **Full Administrator** from the list of available roles.

    d. Click the **Save** button to assign the selected roles to the user.

You can check which users belong to the group by clicking on the **Group members** tab. In our example, you can see that there are two users in the group: **TCNAdmin01** and **TCNInstaller01**. Both of these accounts should now have the **Full Administrator** role applied.

In our example, to demonstrate this for the logged on **TCNInstaller01** account all they need to do is refresh the page in the browser. They now have all the permissions related to the **Full Administrator** role and will therefore be able to see all the configuration items in the **Settings** application, and they can also now browse to Tachyon Explorer.

1.2.5 Use

1.2.5.1 Using Tachyon

Having configured the users who will access Tachyon we can now go on to demonstrate the basic functionality of Tachyon including: viewing connected devices, asking a question and seeing the responses, requesting to perform an action and the associated approval process.

1.2.5.2 Viewing connected devices

Perhaps one of the first things you should do after installing and configuring role-based access to Tachyon is to check what devices are connected. This gives you instant feedback on whether the Tachyon client devices have been installed correctly and are able to communicate back to Tachyon.

In our quick start example we were previously logged on to Tachyon as **TCNInstaller01**, and have already navigated to **Explorer**. In order to view the **Devices**->**Table** page expand the **Devices** node and select **Table**.

1.2.5.3 The quick start example

To illustrate the workflow for asking questions, filtering responses and performing follow-up actions we will use a simple example where we ask the **Tachyon Platform verification stage 1** question. We'll then run the **Tachyon Platform verification stage 2** action to complete the verification.

1.2.5.4 Asking a question

The first step in the example is to ask the question and view the responses in Tachyon Explorer. The question we want to ask is **Tachyon Platform verification stage 1**. The following steps show how to select and ask the question then view the responses. Still logged on as the **TCNInstaller01** account, the steps are:

1. The usual way to run instructions is from the **ExplorerHome** page, click on **Home** to view the **Home** page.
2. Type some letters from the name of the stage 1 question into the Explorer field, in our example we type the text **verif**. This will display a list of questions that match the text. You will see the two instructions; the stage 1 question and the stage 2 action.
3. Select the **Tachyon Platform verification stage 1** question from the list of matches.
4. The question is added to the Explorer window. Depending on the question you may need to set some attributes and for all questions you can set parameters, such as the duration, coverage and question filters. In our example this simple question has no attributes and will be asked of all the devices with no filtering, so we click on the **Ask this question** button directly.
5. The question gets asked of all Tachyon client devices. If they are currently connected they will respond immediately. If they are offline they will respond if they connect within the duration of the question.

1.2.5.5 Performing an action

From Tachyon v4.0 you no longer need to ask a question before you can run an action from the **Explorer** home page.

1. In the edit field of the **Home** page type **verif** and select the **Tachyon Platform verification stage 2** action from the list displayed.
2. Run this action with default parameters by clicking the **Perform this action** button. Doing this triggers the action approval workflow.
3. Tachyon will ask you to confirm your user name and password credentials. This is a safeguard to prevent actions from being run on unlocked devices where you are temporarily absent.
4. By default, if email has been configured, Tachyon provides two-factor authentication - so after the credentials have been set and the **Confirm and send** button is clicked, you will see that the instruction requires authentication. You will then need to check your email for the authentication code.
5. After retrieving the authentication code, return to Tachyon and enter it into the prompt. The instruction will then go into a pending approval state and a notification will be sent to the approver. As a further safeguard, Tachyon actions cannot be approved by the person requesting the action. In our

example this means that **TCNInstaller01** cannot approve their own action, approval must be done by the other user **TCNAdmin01**.

6. The approver will receive an email saying that the action is pending their approval. If the approver logs on to Tachyon using the link provided in the email, they will be directed to their **Notifications** page.

7. Scrolling to the bottom of the **Notifications** page the approver gets an opportunity to provide a comment for their approval or rejection decision. If they want to approve the action they must first check the **I understand approving my request impacts my IT environment** checkbox and then click the **Approve** button. In our example **TCNAdmin01** enters a suitable comment, checks the box and clicks **Approve** to approve the service start action.

8. The approver is then immediately notified that their decision has been implemented.

9. At the same time, Tachyon also enables the action to go ahead. In our example, the results of running the action are displayed, showing that all twelve connected devices responded and were able to run the verification of the background channel.

1.2.6 In conclusion

In this quick start guide we've shown how to configure an example environment, how to implement the Tachyon Server and Tachyon clients onto the environment, how to configure the Tachyon users and import Product Packs. Finally we've shown those users accessing the Explorer to investigate the devices that are currently connected and then asking a question and performing and approving an action.

1.2.7 Next Steps

1.2.7.1 Using applications that are installed by default

The following applications are always installed by Tachyon Setup, although you may have limited access to features depending on your license.

- **Settings** - please refer to Using Settings
- **Inventory** - please refer to Introducing Inventory
- **Explorer** - please refer to Using Tachyon Explorer
- Guaranteed State - please refer to Using Guaranteed State
- **Experience** - please refer Using Tachyon Experience.

Please refer to Using consumer applications for a summary of these and other optional applications.

Use the Connectors page in the Inventory application to configure connectors and populate the inventory repository. Introducing Inventory describes how to view the normalized inventory data, which can then be used by the following applications that depend on inventory.

- AppClarity
- Application Migration

- Patch Success.

1.2.7.2 Installing and Using AppClarity

You can use Tachyon Setup to install AppClarity during or after you install or upgrade Tachyon using setup. Please refer to Implementing AppClarity.

1.2.7.3 Installing and Using Application Migration

You can install Application Migration during or after you install or upgrade Tachyon using setup. Please refer to Introducing Application Migration.

1.2.7.4 Installing and Using Patch Success

Use must use Tachyon Setup to install and configure Patch Success when you install or upgrade Tachyon. Further configuration is then required as described in Implementing Patch Success.

1.2.7.5 Installing and Using Nomad

You can install Nomad during or after you install or upgrade Tachyon using setup. Please refer to Implementing Nomad.

1.2.7.6 Using Configuration Manager Console Extensions

If you have **Microsoft System Center Configuration Manager** (SCCM, ConfigMgr) then you can install the 1E Tachyon Toolkit on each computer that has Configuration Manager Console installed, in order to add right-click tools. Please refer to The 1E Tachyon Toolkit.

1.2.7.7 Creating your own instructions

You will need your own code signing certificate, and have it registered in your Tachyon license, if you want to develop your own custom Tachyon instructions, or modify those of other authors. Instructions that are provided in the Tachyon Platform zip or downloaded from the 1E Exchange have already been code signed using the Platform and Exchange certificates from 1E. Your license controls whether you can use these instructions.

Ideally, all of your Tachyon instruction developers should share a single **code signing certificate** between them. Each code signing certificate must be registered in your license and associated with your organization's **instruction name prefix**. When you have chosen your prefix and have your code signing certificate(s) you then need to send details of these to 1E, who will update your license. This will then automatically activate on your Tachyon Server (assuming it has a connection to the Internet).

For a getting-started guide to configuring and verifying your Tachyon system so that you can run customized Instructions, refer to /document/preview/736871#UUID-66857689-bfb0-8dbc-ae8d-1de40c66fad9.

The Tachyon SDK (refer to /document/preview/736743#UUID-33c212b3-863e-21bc-bc5d-52e41a0492b3) is where you can find comprehensive resources for using Tachyon Instruction Management Studio (TIMS) and authoring your instructions.

1.3 Planning for Tachyon

Everything you need to know about planning your implementation of Tachyon.

Below is a summary of the design decisions you need to make when planning your Tachyon implementation. Further detail is available below each topic.

1.3.1 License requirements

To be able to use a Tachyon application or tool, you must ensure it is registered as a consumer in your Tachyon licence.

If any consumer, such as Tachyon Explorer, is required to run an instruction, then the instruction's prefix must also be registered in the licence.

> **Tip**
>
> If you want to develop your own instructions in-house, or modify downloaded instructions, you will need to contact 1E to add your custom instruction prefix to your license file, along with the thumbprint of your Code signing certificates , that you must provide.

1E will provide you with a **Tachyon.lic** license file that defines the applications, tools, and features your system is able to use, for how long, and how many devices it supports, this may be an evaluation or subscription license.

- The license must be activated. Once activated, it may be used only by the system that activated it.
- Licenses can be renewed or updated, but if allowed to expire, then the affected products or features will not be usable.
- For a new installation, the Tachyon Setup program will let you select the license file from any folder on disk.
- For an existing installation, the license file is copied into the folder: %PROGRAMDATA%\1E\Licensing on your Tachyon master server.

1.3.1.1 License requirements for consumer applications

For any application, tool or feature to use instructions, its consumer and prefix pattern must be registered in your license. The table below shows the consumers and prefix patterns that are typically included in a Tachyon license. The table also includes other applications where instructions - and therefore licensing - are not applicable. Tachyon expects to find the license file in: **%PROGRAMDATA%\1E\Licensing** on your Tachyon (Master Stack) Server.

Applications and features are included in the standard Tachyon License unless otherwise stated in the notes below as being an additional cost.

License requirements for consumer applications

Application or Feature	Consumer name	Prefix patterns	Where to obtain the Product Pack	Notes
Endpoint Troubleshooting	Explorer	You will need prefixes for any Tachyon instructions and you want to use, including custom prefixes for your own and/or third party. Included in the base license are: • 1E-Exchange-* • 1E-Explorer-* • 1E-TachyonPlatform-*	• **Tachyon Platform** zip available on the Support Portal https://support.1e.com/ includes the following classic Product Packs and instruction sets: – **Instructions** – **Instructions** – **Instructions** • 1E Exchange is an online library containing lots of other Product Packs containing instruction	**Explorer** application provides functionality to run, approve and schedule instructions, view Tachyon managed devices. Used to investigate, remediate issues and manage operations across all your endpoints in real-time. **Tip** If you want to use instructions developed by third parties, your own developers, or 1E devel

Application or Feature	Consumer name	Prefix patterns	Where to obtain the Product Packs for various use-cases.	Notes
				opers on your behalf, then you must ask 1E to register the third party and customer prefixes in your license. Please refer to Developing your own instructions. You cannot create or update instru

Application or Feature	Consumer name	Prefix patterns	Where to obtain the Product Pack	Notes
				ctions using other prefixes because they must be signed by others.
Endpoint Automation	Guaranteed State	You will need prefixes for any Guaranteed State fragments you want to use, including custom prefixes for your own and/or third party. Included in the base Guaranteed State license are: • 1E-Explorer-* • 1E-GuaranteedState-* Guaranteed State requires licensing for its instruction fragments from v5.1 onwards.	• **Tachyon Platform** available on the Support Portal https://support.1e.com/ includes the following Integrated Product Packs (which contain Policies for Guaranteed State): – MEMCM Client Heal	**Guaranteed State** application ensures endpoint compliance to enterprise IT policies. The application allows you to manage rules and policies, and report on compliance.

Application or Feature	Consumer name	Prefix patterns	Where to obtain the Product Pack	Notes
			th integrated product pack – 1E Nomad product pack – Tachyon Core integrated product pack – Trigger templates and preconditions reference – Windows Client Heal	

Application or Feature	Consumer name	Prefix patterns	Where to obtain the Product Pack	Notes
			th integrated product pack	
Inventory Insights	Inventory	• 1E-Inventory-*	• **Tachyon Platform** available on the Support Portalhttps://support.1e.com/ includes the following classic Product Pack and instruction set: – **Instructions** includes 1E Inventory instructions for Tachyon	**Patch Success** application is used to view and export inventory, and manage associations (new in 5.0). Inventory data can be captured from various sources using Connectors, refer to the Connectors page. Data is consolidated, normalized and stored in Repositories, refer to the Repositories page. The Tachyon connector is one method of collecting data, and this uses four inventory instructions which are available in the

Application or Feature	Consumer name	Prefix patterns	Where to obtain the Product Pack	Notes
			Powered Inventory	**1E Inventory Product Pack**. This pack also includes another instruction used by Patch Success.
Settings	Platform	N/A	N/A	The **Settings** application is used to administer Tachyon. For example, permissions management, instruction set management, connector management, repository management, sync scheduling etc.
Dashboards	Dashboards	• 1E-ExecutiveDashboard-*	• The latest **Hotfix Bundle** for Tachyon platform (which you can download from the Support Portal https://support.1e.com/)	The Exec Dashboard lets you gain fresh DEX insights from 1E apps. It is the first dashboard available in the **Dashboards** application. This product pack contains a

Application or Feature	Consumer name	Prefix patterns	Where to obtain the Product Pack	Notes
			is used to install the app and its product pack: – 1E ExecutiveDashboard product pack	special type of instruction called **Server question**. These questions cannot be run or scheduled in Explorer. These instructions are not sent to devices, instead they query data already held in Tachyon databases. They are run whenever the Exec Dashboard is refreshed if the previous cache of responses has expired.
Experience Analytics	Experience	N/A	• **Tachyon Platform** available on the Support Portal https://support.1e.com/ includes the following classic Product Packs and	Experience helps you visualize your end-users' experience of IT service delivery across your enterprise. It is centered around the experience score, which is based on

Application or Feature	Consumer name	Prefix patterns	Where to obtain the Product Pack	Notes
			instruction sets: – Instructions	metrics that cover four categories: • **Stability** - derived from the frequency of operating system and software crashes, hangs and service failures. • **Responsiveness** - based on the speed of operating system startup, system resource creation and availability. • **Performance** - a weighted

Application or Feature	Consumer name	Prefix patterns	Where to obtain the Product Pack	Notes
				indication of load and throughput for device processor, memory and disk resources. • **Sentiment** - an aggregated measurement of users feelings or opinions of their device's performance, stability and responsiveness based on user surveys.
AppClarity	AppClarity	N/A	N/A	AppClarity is a Tachyon application aimed at

Application or Feature	Consumer name	Prefix patterns	Where to obtain the Product Pack	Notes
				Software Asset Management (SAM) users, helping you get to grips with software waste, take control of license compliance and manage application portfolios easily. It offers an immediate reduction in software costs by helping you manage your software assets on desktops more effectively and maintain software license compliance. The main benefits of using AppClarity are: • Software license compliance – provides at a summary on

Application or Feature	Consumer name	Prefix patterns	Where to obtain the Product Pack	Notes
				whether a particular product is license compliant or not • Efficient management of entitlements and agreements for an organisation • Software waste identification – shows unused or rarely used software which are probably the two largest form of software waste and

Application or Feature	Consumer name	Prefix patterns	Where to obtain the Product Pack	Notes
				enables to reclaim • License Demand based on different metrics for vendors • Efficient application management – identifies version sprawl where there are many versions of the same product in use. Now, you can financially quantify all software waste by identifying and controlling unused software across your enterprise

Application or Feature	Consumer name	Prefix patterns	Where to obtain the Product Pack	Notes
				and improve your compliance status. **Note** AppClarity is an additional cost to the standard Tachyon Platform license.
Patch Insights	Patch Success	• 1E-PatchSuccess-*	• **Tachyon Platform** available on the Support Portal https://support.1e.com/ includes the following classic Product Pack and instruction sets:	Patch Success is an application that lets you maximize success of enterprise-wide patch deployment. It provides a view of patch state of your estate, as well as supplementing your existing patch deployment methods.

Application or Feature	Consumer name	Prefix patterns	Where to obtain the Product Pack	Notes
			– Instructions – Instructions also includes a Patch Success instruction	Required instructions need to be licensed as well as the consumer. Three instructions are available in the **1E Patch Success Product Pack** and another one in the **1E Inventory Product Pack.** **Note** Patch Success is an additional cost to the standard Tachyon Platform license.
1E ConfigMgr UI Extensions	CmConsoleExtensions RunInstructionUI	• 1E-ConfigMgrConsoleExtensions-*	• **Tachyon Platform** available on the Support Portal	The Configuration Manager Console extensions is

Application or Feature	Consumer name	Prefix patterns	Where to obtain the Product Pack	Notes
			https://support.1e.com/includes the following classic Product Pack and instruction set: – **Instructions**	installed as part of The 1E Tachyon Toolkit.
The 1E Tachyon Toolkit	TachyonRunInstruction	You will need prefixes for any Tachyon instructions you want to use, including custom prefixes for your own and/or third party.	N/A	The Tachyon Run Instruction command-line tool is installed as part of The 1E Tachyon Toolkit.
1E ITSM Connect	ServiceNowCore	You will need prefixes for any Tachyon instructions you want to use, including custom prefixes for your own and/or third party.	N/A	1E ITSM Connect (with 1E Core) provides a User Interface in ServiceNow similar to **Tachyon Explorer**, that allows ServiceNow users to use any instruction that is permissioned for the **1E ITSM Connect app user role**. **Note**

Application or Feature	Consumer name	Prefix patterns	Where to obtain the Product Pack	Notes
				1E ITSM Connect is an additional cost to the standard Tachyon Platform license.
1E Service Catalog Connect	ServiceNowCore	You will need prefixes for any Tachyon instructions you want to use, including custom prefixes for your own and/or third party.	N/A	1E Service Catalog Connect (with 1E Core) provides a User Interface in ServiceNow similar to the **1E Shopping** app portal, that allows ServiceNow users to use any instruction that is permissioned for the **1E ITSM Connect app user role**. **Note**

Application or Feature	Consumer name	Prefix patterns	Where to obtain the Product Pack	Notes
				1E Service Catalog Connect is an additional cost to the standard Tachyon Platform license.
Application Migration and WSS	Nomad	N/A	N/A	Application Migration intelligently automates the migration of applications during a Configuration Manager OS deployment. Using migration rules (defined by an administrator), previously installed applications can be reinstalled,

Application or Feature	Consumer name	Prefix patterns	Where to obtain the Product Pack	Notes
				upgraded or replaced with an alternative during an OS deployment task sequence. These rules can include usage criteria, allowing you to choose to only install previously installed applications if they were being used, or perhaps replace a rarely used application with a less costly alternative. This functionality enables applications to be actively rationalized during an OS migration exercise, standardizing on products and versions and reclaiming unused software. **Note**

Application or Feature	Consumer name	Prefix patterns	Where to obtain the Product Pack	Notes
				Application Migration is an additional cost to the standard Tachyon Platform license.
Content Distribution	Nomad	• 1E-Nomad-*	• **Tachyon Platform** available on the Support Portal https://support.1e.com/includes the following classic Product Pack: – **Instructions**	**Nomad Download Pause** requires an installation of the Content Distribution service on Tachyon platform. The feature is available as: • A right-click option in the Nomad Admin tools for the Configuration Manage

Application or Feature	Consumer name	Prefix patterns	Where to obtain the Product Pack	Notes
				r Console • Instructions in Explorer. Nomad Admin tools for the Configuration Manager are installed using the **NomadBranchAdminUIExt.msi** installer. **Note** Nomad is an additional cost to the standard Tachyon Platform license.
Nomad	• 1E-GuaranteedState-Check-	• **Tachyon Platform** available on the Support Portal https://support.1e.com/ includes the following	Many businesses rely on Microsoft Endpoint Manager Configuration Manager	

Application or Feature	Consumer name	Prefix patterns	Where to obtain the Product Pack	Notes
	MEMCM* • 1E-GuaranteedState-Check-Network* • 1E-GuaranteedState-Check-Service* • 1E-GuaranteedState-Check-Software* • 1E-GuaranteedState-Check-WindowsUpdate* • 1E-GuaranteedState-	Integrated Product Pack: – MEMCM Client Health Policy	(MEMCM) to deploy software, patches and updates across their company networks. It is crucial that Configuration Manager is working effectively. The MEMCM Client Health policy monitors Configuration Manager client health and performance. It checks for cache availability, inventory cycles, service availability and Configuration Manager WMI integrity - common causes of Configuration Manager client problems on devices. The MEMCM Client Health policy replaces the previous SCCM Client Health policy and covers the following:	

Application or Feature	Consumer name	Prefix patterns	Where to obtain the Product Pack	Notes
	Check-Wmi* • 1E-GuaranteedState-Fix-MEMCM* • 1E-GuaranteedState-Fix-Service* • 1E-GuaranteedState-Fix-WindowsUpdate* • 1E-GuaranteedState-Fix-Wmi* • 1E-GuaranteedState-Precondition*		• Ensure the correct version of the CM client is installed and running and assigned to the correct site • Ensure the CM client is not stuck in provisioning mode • Ensure that heartbeat discovery, inventory and state messages are being sent regularly • Ensures the CM client cache is set to the correct size • Ensure the CM client log settings are correct	

Application or Feature	Consumer name	Prefix patterns	Where to obtain the Product Pack	Notes
			• Ensure the BITS service exists, configured to start up automatically and is running • Ensure the Windows Time service exists with correct startup settings • Ensure the Windows Management Instrumentation (WMI) service exists, configured to start automatically and is running • Ensure WMI is healthy, the core CIMv2 and ccm	

Application or Feature	Consumer name	Prefix patterns	Where to obtain the Product Pack	Notes
			namespaces and classes exist and that the WMI repository is consistent • Ensure the Windows Update service exists with correct startup settings, is configured to use the correct source (CM, WSUS or Microsoft Update) and that the service can connect to the source **Note** This policy is intended for deploym ent to	

Application or Feature	Consumer name	Prefix patterns	Where to obtain the Product Pack	Notes
			Windows devices only.	
Nomad	• 1E-Explorer-NomadClientHealth-* • 1E-GuaranteedState-Nomad*	• **Tachyon Platform** available on the Support Portal https://support.1e.com/ includes the following Integrated Product Pack: – **Nomad Client Health Policy**	Nomad is included as part of the 1E Client, and as part of that integration, we offer a Nomad client health compliance policy in Guaranteed State. This verifies common Nomad requirements such as ACP registration, disk availability, firewall exceptions, crash notifications and cache monitoring. The Nomad client health policy replaces the client health tile in the Nomad dashboard plus additional remediation steps: • Keeps content distribution services up and running on Nomad clients, so that users	

Application or Feature	Consumer name	Prefix patterns	Where to obtain the Product Pack	Notes
			are secure and productive • Ensures Alternative Content Provider (ACP) registration configuration is set • Maintains optimal disk availability and monitors cache size for storage capacity planning • Enforces Firewall exceptions. **Note** This policy is intended for deployment to Windows devices only.	

Application or Feature	Consumer name	Prefix patterns	Where to obtain the Product Pack	Notes
Nomad	• 1E-Explorer-MSSCCMClientHealth-* • 1E-Explorer-NomadClientHealth-* • 1E-Explorer-WindowsClientHealth-* • 1E-GuaranteedState-ClientHealth* • 1E-GuaranteedState-General-Check-ServiceState* • 1E-Guaran	• Required if all the following apply: – You have a Nomad license instead of a full Tachyon license, – And you upgraded from an earlier version of Tachyon – And using legacy**Microsoft SCCM Client Health Policy** (which has been replaced by the MEMCM Client Policy, for more details please refer to:**MEMCM Client Health Policy**).		

Application or Feature	Consumer name	Prefix patterns	Where to obtain the Product Pack	Notes
		teedState-MSSCCMClientHealth-*		
NightWatchman Online Status	NightWatchman	N/A	N/A	The NightWatchman console uses Tachyon to display traffic lights live status of its clients – indicating whether they are currently online or offline (or unknown). You can also check the status of groups within the NightWatchman client hierarchy. **Note** NightWatchman is an additional cost to the standard Tachy

Application or Feature	Consumer name	Prefix patterns	Where to obtain the Product Pack	Notes
				on Platform licens e.
Shopping integration with Tachyon	Shopping	You will need prefixes for any Tachyon instructions you want to use, including custom prefixes for your own and/or third party.	N/A	Shopping integrates with Tachyon by allowing users to shop for Tachyon instructions, in the same way as they can for applications served by Configuration Manager and Intune. This is most useful to allow users to fix or reconfigure their computers for issues that users commonly understand (such as disk space or Outlook issues). However, it can also be used to quickly deploy software to users or anything else that

Application or Feature	Consumer name	Prefix patterns	Where to obtain the Product Pack	Notes
				instructions can do. Shopping integration also extends the Shopping's order tracking feature, particularly for client-side notifications and status monitoring. To enable these features, please refer to Shopping 6.1 - Enabling Tachyon integration and Shopping 6.1 - Managing Order Tracking. **Note** Shopping is an additional cost to the standard Tachyon Platform

Application or Feature	Consumer name	Prefix patterns	Where to obtain the Product Pack	Notes
				licens e.
Third party and custom er integra tion softwa re	See notes	N/A	N/A	You must ask 1E to add consumer names to your license if you intend to use third party or your own custom software to integrate with Tachyon and leverage its real-time client-based features, for example: • Splunk • QRadar • Rapdid7 • LogRhyt hm • EUCDas hboard You will probably also require your own custom prefixes for instructions and/or Guaranteed State fragments

Application or Feature	Consumer name	Prefix patterns	Where to obtain the Product Pack	Notes
				used by these Consumers, theefore you will need to ask 1E to add these prefixes too, as described the top of this table.

Tip

Additional consumers and tools can be developed by third parties, your developers, or 1E developers on your behalf. 1E must register their consumer names in the Tachyon license.

1.3.1.2 Developing your own instructions

You will need your own code signing certificate, and have it registered in your Tachyon license, if you want to develop your own custom instructions, or modify those of other authors. Instructions that are provided in the Tachyon platform zip, or in Product Packs you download from the 1E Exchange, have already been code signed using the Platform and Exchange certificates from 1E. Your Tachyon license controls whether you can use these instructions.

Ideally, all of your Tachyon instruction developers should share a single **code signing certificate** between them. Each code signing certificate must be registered in your Tachyon license and associated with your organization's **instruction name prefix**. When you have chosen your prefix and have your code signing certificate(s) you then need to send details of these to 1E, who will update your Tachyon license. This will then automatically activate on your Tachyon master server (assuming it has connection to the Internet).

For a detailed step-by-step process, please refer to /document/preview/736871#UUID-66857689-bfb0-8dbc-ae8d-1de40c66fad9 (in the Tachyon SDK).

/document/preview/736743#UUID-33c212b3-863e-21bc-bc5d-52e41a0492b3 is where you can find comprehensive resources for developing your instructions.

You can download Product Packs containing more instructions from the 1E Exchange, and ask questions in the support.1e.com/.

1.3.2 Architectural requirements

You need to decide which architecture your Tachyon system will use, and which configuration options. Your architectural decisions will include the types of Tachyon servers you will need, and how many, as well as how you will provide SQL services.

Tip

This documentation covers installation on-premises and on your own cloud-based servers. Alternatively, please contact your 1E Account team if you wish to use 1E's SaaS solution and avoid having to install and maintain servers.

SQL Server can be local or remote from your Tachyon servers.

Tachyon supports the following High Availability (HA) options for SQL Server:

- AlwaysOn Availability Group (AG) using an AG Listener
- Failover Cluster Instance (FCI)

Tachyon Setup is a configuration wizard which must be run on *each* server in your architecture, to install the required components. Tachyon Setup supports the following types of Tachyon server:

- **All components on a single server** - a single-server installation comprises Master Stack and Response Stack, which is the most common choice for a system of any size supporting Tachyon real-time features.
- **Master Stack** - you would install a Master Stack on its own if you do not require real-time features, or you want one or more remote Response Stacks.
- **Response Stack** - this choice allows you to install a Response Stack after you have completed a single-server installation or installed a Master Stack, and is required to support Tachyon real-time features.
- **DMZ Server** - this choice is used on when installing a DMZ Server to provide real-time features for Internet-facing clients. For design and configuration steps, please refer to the Implementing a Tachyon DMZ Server page.

The number of devices you need to support influences the number of Switches and Response Stacks you will need, and their server specifications. Each Switch can handle up to 50000 devices, and you can have up to five Switches on a single Response Stack server, handling a maximum of 250000 devices.

Multiple Response Stacks provide a degree of high availability, but are not intended for that purpose. Instead, Response Stacks are required for security, geographic or other network reasons. For example, because your organization covers multiple geographies and you do not want 1E Client traffic to go beyond the boundaries of each region, or because you have Internet-facing devices and need a Tachyon DMZ Server on-premises.

1.3.2.1 Tachyon Architecture

The pictures below show the most common architectural implementations of Tachyon that are supported by Tachyon Setup. Organizations with less than 50000 devices will typically have a single-server system with one Switch, but there may be reasons why a more complex configuration would be required. Key factors are the location of servers and how devices and users will connect to them.

Every Tachyon system has a single **Master Stack**, which provides web services for Tachyon applications. Master Stack components are typically all installed on a single **Master Server**.

Tachyon real-time features require **Response Stacks**, which are made up of one or more **Response Servers**. A **DMZ Server** is an example of a Response Server. Each Response Stack has at least one **Background Channel** for sharing resources, and a single **Core** component that supports an associated set of up to five **Switches**. Switches are the primary mechanism for rapidly requesting and retrieving responses from the **clients**. As each Switch can handle up to 50,000 devices there is a limit of 250,000 devices per Response Stack. Higher numbers can be achieved if you contact 1E for guidance. Switches may be local or remote to the other components in the Response Stack.

Databases for Tachyon, 1E Catalog, Nomad, Experience, SLA and BI, are installed on SQL Server database instance(s) that may also be local or remote to their respective Master and Response servers. It is also possible for multiple Response Stacks to share the same Responses database. The **Cube** used by Patch Success (SLA-BI) is installed on a local or remote SQL Server Analysis Services (SSAS) instance.

The pictures of the single-server and internet-facing configurations each show a system with a single Response Stack. The internet-facing system is special because the components of its Response Stack are split over two servers. Splitting a stack across multiple servers is not usually necessary except in special circumstances, for example the Switch and Background Channel on a DMZ Server is remote from its Core. The DMZ picture shows a dual firewall design, but single firewall is also supported.

The databases for Tachyon Master and Response Stacks can exist on local or remote installations of SQL Server. Local is the simplest implementation. A local Responses database offers the best performance, whereas a remote Responses database requires an additional network interface and network routing explained in Network requirements.

Tachyon can be installed on-premises on physical and virtual servers, and also on AWS and Azure cloud servers.

For an explanation of Tachyon components, please refer to Tachyon components.

> **Note**
>
> Click on a picture to enlarge. Click on a link to take you to the relevant part of the Tachyon Architecture page for more detail along with a description of the various components.
>
> Components colored green are optional when installing a Tachyon system.

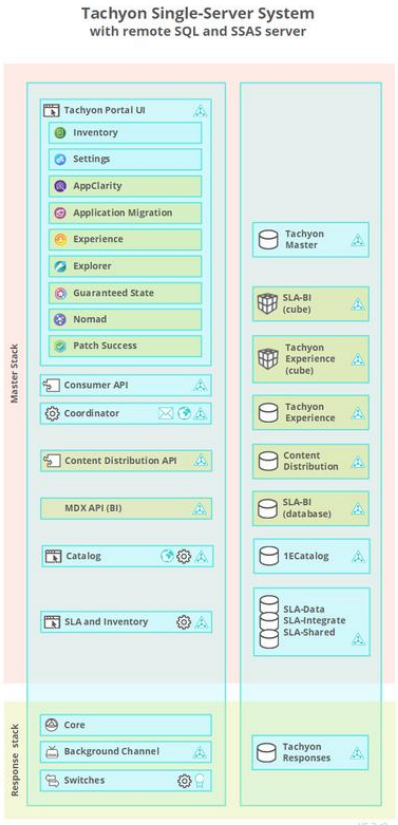
1.3.2.2 Tachyon configuration options

Tachyon Setup configuration wizard has several standard options described above. There is also a custom installation option to support different configurations to those described.

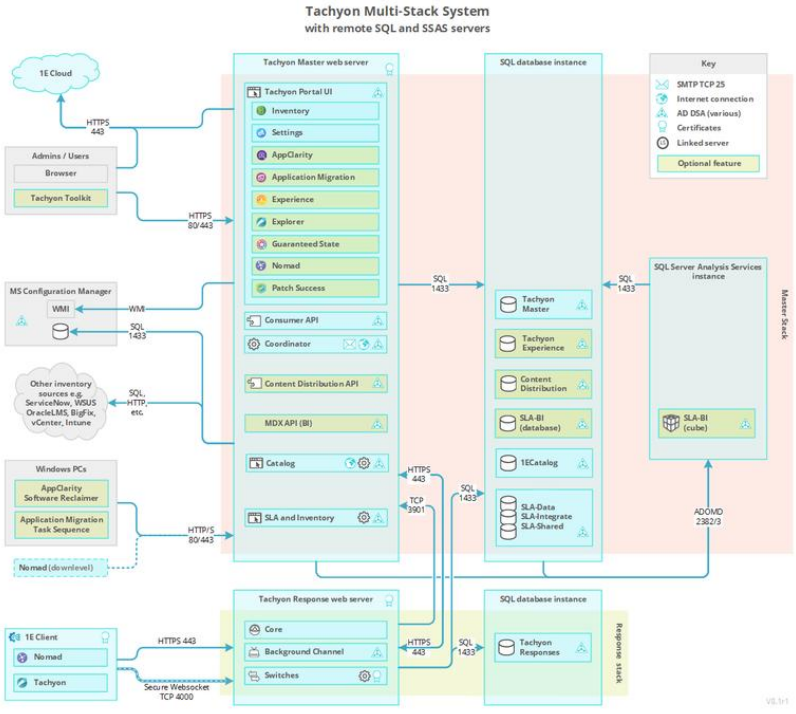
> **Note**
>
> Please contact your 1E Account Team if you need help with this.

SQL Cluster and SQL Always On are supported, but require additional steps, described in High Availability options for SQL Server.

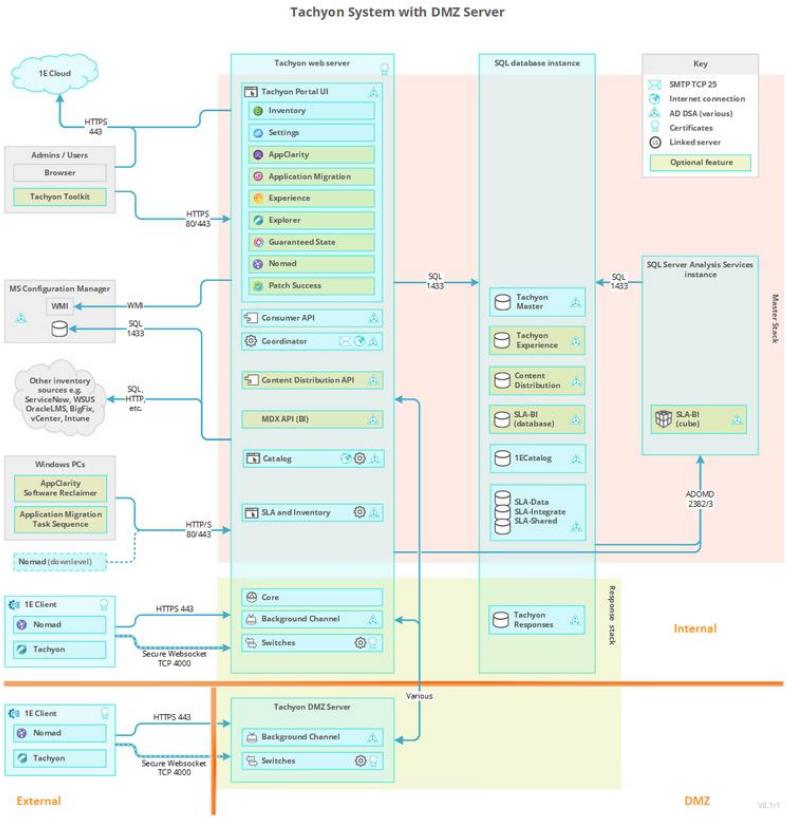
> **Note**
>
> Please contact your 1E Account Team if you need help with this.



[Tachyon Single-Server system]



[Tachyon Multi-Stack system]



Tachyon architecture for Internet-facing devices

1.3.2.2.1 1E Business Intelligence

Business Intelligence is an optional component installed by Tachyon Setup on the Master Stack, and requires SQL Server Analysis Services (SSAS). Business Intelligence is a prerequisite for the **Patch Success** application to support efficient presentation of visualizations on a large scale.

1.3.2.2.2 Applications and Tools

Tachyon applications and tools are consumers, and all consumers connect to the Tachyon Consumer API.

The following consumer applications run on Tachyon platform and are installed using Tachyon Setup. Please also refer to the License requirements page.

Applications are categorized as follows:

- Configuration - applications required to configure Tachyon platform and required by all other applications
- Client - applications that communicate with devices in real-time
- Inventory – applications that use inventory features

1.3.2.2.2.1 Applications that are included in the Tachyon Platform license

Application	Purpose	Type
Inventory	View and export inventory, and manage associations. It uses the SLA databases.	Inventory, configuration
Settings	Configure and monitor platform features. It uses the Tachyon Master database.	Configuration
Guaranteed State	Ensure endpoint compliance to enterprise IT policies. It uses the Tachyon Master and Responses database.	Client
Explorer	Investigate, remediate issues and manage operations across all your endpoints in real-time. It uses the Tachyon Master and Responses database.	Client

1.3.2.2.2.2 Applications that require a license

Application	Purpose	Type
AppClarity	Manage software license compliance, License Demand Calculations, license entitlements, and for reclaiming unused software. It uses the SLA databases.	Inventory
Application Migration	Intelligently automate the migration of applications during a Configuration Manager OS deployment. It uses the SLA databases.	Inventory
#UUID39ecfb49a2e10e6f5820cc411d69d030	Manage content distribution across your organization using a centralized dashboard. It uses the Content Distribution database.	Client

Application	Purpose	Type
	1E Client requires Tachyon and Content Distribution features to be enabled on all clients. Content Distribution replaces the Nomad features of ActiveEfficiency Server, which is deprecated. Legacy Nomad clients continue to be supported by direct communication with the Content Distribution API, whereas Nomad 8.x clients communicate with the Content Distribution API via the proxy feature on Response Servers. Tachyon Setup Setup is used to install Content Distribution, and the Nomad app, and no longer installs ActiveEfficiency. Nomad uses Content Distribution for the following features: • Nomad app provides visibility of content distribution activity • Single Site Download (SSD) • Single Site Peer Backup Assistant (SSPBA) • High Availability Peer Backup Assistant (HAPBA) • Get Migration Settings task sequence action used to manage computer associations • Nomad Pre-caching • Nomad Download Pause.	
/document/preview/763581#UUID-54875393-7855-5624-cbae-9ad5406e1c95	Reports on and ensures successful patching of your enterprise.	Inventory

Application	Purpose	Type
	It uses the SLA and BI databases. Tachyon Setup indstalls SLA Business Intelligence, which requires SQL Server Analysis Server. Patch Success also uses Inventory connectors to get meta-data for patches from whichever of the following that you use to approve patches: • Configuration Manager (SCCM) if it is configured to manage WSUS • Windows Server Update Services (WSUS).	
Introducing Tachyon Experience	Measure performance, stability and responsiveness for applications and devices to assess user experience across your enterprise. It uses the Tachyon Master and Tachyon Experience databases.	Client

The following types of application require 1E Client (with Tachyon features enabled) to be deployed to all in-scope devices.

- All Client applications
- Inventory applications if you intend using the Tachyon connector to populate your inventory.

The **AI Powered Auto-curation** feature is optionally used by Inventory applications to provide automatic curation of new products. This avoids having to manually add products to the 1E Catalog, or wait for it be updated. This optional feature requires additional memory on the Tachyon Server (Master Stack). Please refer to AI Powered Auto-curation: Memory requirements for details.

Some benefits of using AI Powered Auto-curation are that you can:

- Achieve significantly more normalized software from the first sync
- Reduce the manual effort required to normalize software
- Get an expanded SAM offering as more data is available for AppClarity
- Get additional coverage for Application Migration

- Identify more software to review for security threats.

1.3.2.2.3 Tachyon Tools

The following are tools included in Tachyon 8.1 platform. These tools are not installed using Tachyon Setup. They have either their own installers or are included in download zips.

- Tachyon ConfigMgr UI Extensions - installed as part of the Tachyon Toolkit, this is a right-click extension for the Configuration Manager console that provides the option to browse and run an instruction on devices in a specified Collection, refer to Preparing for the Tachyon extensions for the Configuration Manager Console. for details.
- Tachyon Run Instruction command-line tool - installed as part of the Tachyon Toolkit, it is used for sending instructions to the Tachyon server from a script or from a command prompt.
- Tachyon Product Pack Deployment Tool - included in the Tachyon platform zip ProductPacks folder.
- TIMS - used for the development of instructions using the Tachyon SDK, refer to /document/preview/736745#UUID-952f2552-fb04-d55c-6d12-fcf68313ecac for details.

A typical Tachyon license allows the use of all these tools.

1.3.2.3 Telemetry

Telemetry helps 1E to continually improve your experience with Tachyon. Only summarized statistical information is collected, which enables 1E to see how customers use features of the application. No personally identifiable data is collected. 1E use this information to:

- Understand how the product is being used to influence future development decisions
- Plan supported platforms (OS, SQL etc. versions) over time
- Deliver a smooth upgrade experience as we can focus testing on implemented scenarios
- Improve system performance
- Identify early warning signs of potential issues such as excessive growth of database tables, instruction failures etc. so we can pro-actively address them.

Server telemetry reports how the platform is used and data is compressed, encrypted and sent to 1E through email on a configurable schedule. Full details of the Server telemetry data sent to 1E is provided in Server telemetry data. **User Interface telemetry** reports how the user interface is used, and data is sent directly from administrator browsers to the 1E Cloud.Please refer to Whitelisting connections to 1E Cloudfor details of URL that must be whitelisted for administrator browsers.

Telemetry features are configurable using Tachyon Setup during installation or upgrade, and can be enabled or disabled as a post-installation task. 1E encourages customers to enable sending telemetry.

Please also refer to Enabling or disabling Telemetry features.

1.3.2.4 Server sizing requirements

1.3.2.4.1 Objectives

The objective of this document is to outline prescriptive guidance for Tachyoncustomers implementing the solution, either on-premises servers, or in the Amazon AWS or Microsoft Azure cloud platforms.

There are many possible hardware server configurations, or cloud instance types and storage options, that customers can choose from, but the aim of this document is to recommend prescriptive guidance, and detailed configuration of the best performant implementation that customers, of varying client count sizes, should use to implement Tachyon.

This document focuses heavily on the SQL Server implementation and required storage for Tachyon, as this is singly the most performance demanding component of the system.

The default Tachyon configuration assumes, and recommends, a single Tachyon server and a separate remote SQL Server in a standard two server setup. There are sections for additional and complex implementations for separate Switch and Background Channels servers (DMZ), plus the extreme scenario where multiple Tachyon servers in a split, Response and Master Stack server configurations could be deployed, depending on the specific requirements for larger customers, for reasons of scale and higher availability.

1.3.2.4.2 Assumptions

The key assumption in this document for sizing guidelines is that the customer is using all components of Tachyon, that is, Explorer, Guaranteed State, Experience, Patch Success, Inventory, and Content Distribution.

The sizing guidelines are based on extensive testing of all components of the Tachyon platform, at different client count scales, using representative test data to simulate typical customer environments and their administrative and reporting usage.

Therefore, the following sizing guidelines should be used as the *minimum* hardware requirements for the specific numbers of managed clients in the respective size environments.

- In terms of CPUs, the test environment used Intel Xeon E5-2687 v3 @3.1Hz, though any server-level CPU from 2016 should meet the performance needs for the cores specified in the following tables. Additional or newer and faster speed CPUs will improve performance, and the Tachyon platform will SQL Server will utilize all the CPU resources available.
- In terms of data sizing, actual customer data and individual requirements will vary greatly. The data sizing is provided only as general guidance and assumes that some amount of storage will remain as free space, most of the time, when not at peak loads.

1.3.2.4.3 Performance load modelling

To simulate 100,000s of actual 1E Clients, 1E developed a Load Generation tool (loadgen) that maintains the same number of persistent connections and can respond with the same data responses as would actual real-world clients.

In reality, loadgen generates more data and creates greater data storms at the Tachyon servers than, offline and latent 1E Client responses would generate, so can be considered as producing a more extreme and worst-case scenario performance loads on the Tachyon servers.

Assumptions used when creating the sizing guide

Component	Feature	Assumptions
Explorer	Instructions	An average of 1,000 instructions per day (including Synchronous instructions). Peak loads of 10 simultaneous small and some large instructions, targeted at both small and large device sets. Small instructions (<4K) can be received and processed from all online clients in less than 15 seconds.
Guaranteed State	Policies	Around 20 deployed policies totaling 300 active rules and remediations. An average of up to 100 rule state changes per device per day.
Experience	Events and metrics	Each device reports an average of 300 Device and Software Performance, User Interactions and Windows events per day. The Experience Dashboards and UI drill-down queries should be able to display and filter required data views, within a few minutes.
Inventory (also known as SLA)	Hardware and software inventory	At least two connectors are configured (for example SCCM or BigFix) in addition to the Tachyon connector. An average of 200 software installations and 100 patches per device and up to 50,000 distinct software products, per 50k devices. Up to 50 distinct Management Groups per 50,000 Devices.
Patch Success	Patch data	Clients process a maximum of 20 patch state changes per month for Windows and other related Microsoft Updates.
Content Distribution	Downloads	For every 50,000 clients there are 100 sites containing around 2,500 distinct subnets. At peak loads (that is, during a critical patch deployment) there could be up to 20,000 content download requests

Component	Feature	Assumptions
		(and their responses) per minute handled by the platform and content registrations.

An overall assumption is that long duration and high impact batch processing operations, such as SLA inventory sync consolidations and Experience sync processing, are run primarily out of business hours (typically overnight) when there would be little potential impact on other Tachyon traffic and administrative interactive query and analytical reporting.

1.3.2.4.3.1 Using AI Powered Auto Curation with SLA Inventory Sync

Additional RAM is required if this feature is enabled, based on the total number of distinct software titles found in a specific customer environment. Please refer to the table detailed at AI Powered Auto-curation, which explains how to calculate the memory requirements. You must then add this to the figures in the following sizing tables.

1.3.2.4.4 On-premises installation

The Tachyon platform is recommended to be installed on a dedicated server, with a separate dedicated SQL Server, and can be installed on either virtual server or physical hardware.

For every 50,000 clients, Tachyon requires a separate instance of the Tachyon Switch component, which requires a dedicated Network Interface (NIC) for each switch instance. In a virtualized environment, this should a dedicated vNIC that preferably maps to a dedicated physical NIC, on the host.

Tachyon is a high-intensity database application and so requires a highly performant Microsoft SQL Server setup, with fast storage, and this is the most important component to size correctly. Storage could be presented locally, but it is expected that the more likely scenario is that this is presented from a customer Enterprise Storage Area Network (SAN), or cloud-based managed storage.

As per Microsoft SQL Server best practice, 1E recommends to provision at least three separate disk volumes for SQL Data, Logs, and TempDB. These volumes may be made up from multiple dedicated disks, striped in a RAID Volume for both resilience and performance, for example RAID 10, depending on the standard operational configuration of the customer's on-premises storage sub-systems.

Data and log drives disk volumes should be formatted to use 64 KB allocation unit size. It is assumed the customer is using fast SSD based storage to achieve the necessary disk throughput in MB/s and IOPS, at least 6Gb/s SATA, but preferably 12Gb/s SAS or NVMe drives at higher scale.

Microsoft SQL Server should be configured according to the Microsoft best practice documentation. The default installation of SQL Server 2017 or later, will make automatic configuration settings for memory, TempDB, and processing parallelism. However, the best single index to overall Microsoft recommendations for SQL Server can be found at https://docs.microsoft.com/en-us/sql/relational-databases/performance/performance-center-for-sql-server-database-engine-and-azure-sql-database?view=sql-server-ver15.

Note

One setting to make over and above the SQL Server installation defaults is to set **Maximum SQL Server Memory** to a value that reserves some memory at the server for the Operating System itself, and any additional running processes. A reasonable rule of thumb to use, for a dedicated SQL Server configuration as defined in the following server

tables, would be to set **Maximum SQL Server Memory** to 85% of total memory of the server.

Cloud based SQL Database deployment templates, may configure most, but not all, memory optimizations automatically, but some of the key recommendations to note, are as follows.

- Server memory configuration options (https://learn.microsoft.com/en-us/sql/database-engine/configure-windows/server-memory-server-configuration-options)
- Configure the max degree of parallelism Server Configuration Option (https://learn.microsoft.com/en-us/sql/database-engine/configure-windows/configure-the-max-degree-of-parallelism-server-configuration-option)
- optimize for ad hoc workloads server configuration option (https://learn.microsoft.com/en-us/sql/database-engine/configure-windows/optimize-for-ad-hoc-workloads-server-configuration-option)

In addition, it is essential that a Backup and Maintenance strategy of SQL server must be defined, and backup and maintenance jobs configured accordingly. These must be run during low peak hours or when server is not in use (such as over-night or weekends) and should include the following.

- At least weekly full backups and then daily differentials, as required
- Daily Update statistics job and weekly Rebuild index followed by DBCC Checkdb

1.3.2.4.4.1 SQL Server Analysis Services (SSAS)

In addition to SQL Server databases, Patch Success requires a SSAS instance, in multi-dimensional mode, that can be co-located with SQL Server Database installation, using the same data and log drives. The disk space required for the SSAS cubes is typically only 10's of MBs, so can largely be ignored in terms of disk space sizing.

SSAS settings and configuration can be left at the installation defaults, but additional best practice performance optimizations for SSAS can be found in the following Microsoft guidance at http://download.microsoft.com/download/d/2/0/d20e1c5f-72ea-4505-9f26-fef9550efd44/analysis%20services%20molap%20performance%20guide%20for%20sql%20server%202012%20and%202014.docx

When SSAS is being used, set **Memory Limit Low**: 90% and **SSAS Memory Limit High**: 95%. Both of these settings can be set at the Server properties via SQL Server Management Studio.

1.3.2.4.4.2 Small server sizing (<10K clients, on-premises and cloud)

For small systems with less than 10,000 seat counts and Proof-of-Concept installations, it is allowable for simplicity for all the Tachyon server components and SQL Server to be installed onto a single server - though it should be noted that this may mean higher SQL per core licensing costs than a split two server installation.

In a single server, as per Microsoft SQL Server best practice, it is still recommended to have a minimum of 3 separate disks (OS Drive, SQL DB and Logs, and TempDB) to gain optimum disk performance.

VM and storage sizing for both on-premises and cloud platforms

Platform	On-Premises	Microsoft Azure	Amazon AWS
CPU Cores	4	4	4
RAM	32 GB	32 GB	32 GB
Tachyon Switches	1	1	1
NICs	1	1	1
Disks			
OS Drive disk size	64 GB	64 GB	64 GB
DB and Logs disk size	500 GB	500 GB	500 GB
MBs/IOPS	250/15,000	170/3,500	250/16,000
TempDB disk size	150 GB	150 GB	180 GB
MBs/IOPS	250/15,000	242/38,500	250/16,000

Note

For a combined single-server installation, **Maximum SQL Server Memory** max memory should be capped at 50% of available memory, to ensure the set of Tachyon databases has its own, dedicated pool of memory.

IOPS is calculated at standard 16k Block Size, although SQL Data volumes/disks should be formatted in Windows at 64k allocation units, according to Microsoft SQL Server best practice guidance.

For Cloud implementations, to achieve the required disk throughput, the above assumes using premium storage SSD based disks. For example, for Azure use Premium SSDs, and for AWS use EBS gp3 volumes.

1.3.2.4.4.3 Medium and large on-premises design patterns

On-premises VM and storage sizing for different customer sizes

	Medium 1	Medium 2	Large 1	Large 2	Large 3
CPU Cores	4	8	16	32	63

	Medium 1	Medium 2	Large 1	Large 2	Large 3
RAM	16 GB	32 GB	64 GB	128 GB	256 GB
Tachyon Switches	1	1	2	4	10
NICs	2	2	3	5	11
Remote SQL Server					
CPU Cores	4	8	16	24	64
RAM	32 GB	64 GB	128 GB	256 GB	512 GB
Disks					
DB Size	500 GB	1,000 GB	2,000 GB	4,000 GB	8,000 GB
MBs/IOPS	250/15,000	500/30,000	1,000/60,000	2,000/120,000	4,000/240,000
Logs Size	100 GB	200 GB	500 GB	1,000 GB	2,000 GB
MBs/IOPS	170/10,000	250/15,000	500/30,000	1,000/60,000	2,000/120,000
TempDB Size	150 GB	300 GB	600 GB	1,200 GB	2,000 GB
MBs/IOPS	250/15,000	500/30,000	1,000/60,000	2,000/120,000	4,000/240,000

Note

Customers with intervening seat counts should choose the closest higher number. For example, a 150,000-seat implementation should be treated as **Large 2** rather than **Large 1**.

IOPS is calculated at standard 16k Block Size, although SQL Volumes should have a 64k block size, and disks/volumes should be formatted in Windows at 64k allocation units, according to Microsoft best practice guidance.

1.3.2.4.4.4 Network considerations

A server hosting a Tachyon Response Stack requires a dedicated network interface for each Switch, and for the connection to the remote SQL Server, to keep incoming traffic from clients separate from the outgoing traffic to the Response and other Tachyon SQL databases. It is expected that this Server-to-Server network traffic, would be over a Data Center backbone network of 10Gb or more.

Accelerated Networking which provides enhanced NIC performance, using Receive Side Scaling (RSS) should be enabled on all NICs. Please refer to https://docs.microsoft.com/en-us/windows-hardware/drivers/network/introduction-to-receive-side-scaling.

Also, its better performant to increase the transmit (TX) and receive (RX) buffer sizes to their maximum under the Windows network adaptor advanced properties.

1.3.2.4.5 Microsoft Azure

1.3.2.4.5.1 Out of scope

This document only focuses on implementing Tachyon components and SQL Server on individual Azure VMs, and configurations using Azure Premium storage.

It doesn't consider using Microsoft SQL as part of Azure Platform as a Service (PAAS) offerings, either SQL Server Managed Instances or Native Azure SQL (https://docs.microsoft.com/en-us/azure/azure-sql/azure-sql-iaas-vs-paas-what-is-overview) as these solutions are not currently supported by 1E as a means to implement SQL Server for Tachyon.

In addition, it does not consider using Azure instances that do not rely on Azure premium storage, but have local NVMe drives, like the Lsv2-series. Although these instance types have very high performing storage and data transfer bandwidth, the NVMe disks are ephemeral or non-persistent, so only practical for single SQL Server instance for TempDB.

In the future, 1E plan to provide guidance in using non-persistent storage solutions or SQL Business Critical Managed Instances, as part of a **SQL Server Always on Availability Group** cluster, that would provide storage resilience and redundancy as described in https://docs.microsoft.com/en-us/sql/database-engine/availability-groups/windows/overview-of-always-on-availability-groups-sql-server?view=sql-server-ver15. However, since these solutions require a cluster of minimum 3 nodes, it should be noted that these solutions would be much more expensive to implement than individual VMs.

1.3.2.4.5.2 Azure VM Selection

This document should be read in conjunction with the Azure documentation, especially with the guidance on Maximizing Microsoft SQL Server Performance with on Azure VMs https://docs.microsoft.com/en-us/azure/azure-sql/virtual-machines/windows/performance-guidelines-best-practices.

Azure Premium storage recommendations for SQL Server workloads are also detailed more completely in https://docs.microsoft.com/en-us/azure/virtual-machines/premium-storage-performance#optimize-IOPS-throughput-and-latency-at-a-glance.

Based on these factors, 1E recommend using Azure Dsv4 VMs for the Tachyon server and Edsv4-series VMs for SQL Server, to achieve the optimum ratio of vCPU and memory count for the separate requirements.

Dsv4 and Edsv4-series sizes run on the Intel® Xeon® Platinum 8000 series (Cascade Lake) processors. In addition, the Edsv4 virtual machine sizes feature up to 504 GiB of RAM, in addition to fast and large local SSD storage (up to 2,400 GiB). These virtual machines are ideal for memory-intensive enterprise applications and applications that benefit from low latency, high-speed local storage in the following specifications.

Azure Dsv4 VMs for the Tachyon server

Dsv4 Series							
Standard_D2s_v4	2	8	0	4	3200/48	2	1000
Standard_D4s_v4	4	16	0	8	6400/96	2	2000
Standard_D8s_v4	8	32	0	16	12800/192	4	4000
Standard_D16s_v4	16	64	0	32	25600/384	8	8000
Standard_D32s_v4	32	128	0	32	51200/768	8	16000
Standard_D48s_v4	48	192	0	32	76800/1152	8	24000
Standard_D64s_v4	64	256	0	32	80000/1200	8	30000

1.3.2.4.5.3 Azure VM constrained core CPU options

At some VM sizes, it is possible to reduce the CPU count to therefore lower SQL license requirements, whilst maintaining the higher storage throughput of the VM. Selecting constrained core SQL VMs, specifically to get the higher required storage throughput, although with the same VM and OS license pricing, will provide half the actual presented vCPU core count, but therefore minimise SQL Server license costs.

Please refer to https://learn.microsoft.com/en-us/azure/virtual-machines/constrained-vcpu.

1.3.2.4.5.4 Azure Premium storage selection

For any solution based on Microsoft SQL Server, storage throughput is normally the major bottleneck to performance, and Tachyon is no exception to this.

The maximum storage throughput in terms of MB/s and IOPS for specific Azure EdsV4 VMs is detailed in the table below, and this will determine the maximum equivalent MBs/IOPS for the selected Azure Premium storage volumes.

For example, if you attach a two P30 disks volume (200MB/s provisioned throughput each) to an E16ds_v4 VM, you reach the instance limit of 384 MB/s before you reach the volume limit of 400 MB/s total throughput.

Azure EdsV4 VMs for the Tachyon SQL Server

Edsv4 Series				
Standard_E2ds_v4	75	4	19000/120(50)	3200/48
Standard_E4ds_v4	150	8	38500/242(100)	6400/96

Edsv4 Series

Standard_E8ds_v4	300	16	77000/485(200)	12800/192
Standard_E16ds_v4	600	32	154000/968(400)	25600/384
Standard_E20ds_v4	750	32	193000/1211(500)	32000/480
Standard_E32ds_v4	1200	32	308000/1936(800)	51200/768
Standard_E48ds_v4	1800	32	462000/2904(1200)	76800/1152
Standard_E64ds_v4 [1]	2400	32	615000/3872(1600)	80000/1200

The recommended Azure Premium storage type are Premium SSDs as these deliver the best high-performance and low-latency disk support for virtual machines at the lowest storage cost. Please refer to https://learn.microsoft.com/en-us/azure/virtual-machines/disks-types.

Another option would be to use Azure Ultra disks, but these are much more expensive and do not benefit from read caching. Though, some additional benefits of Ultra disks include the ability to dynamically change the performance of the disk, without the need to restart the VM.

As per Microsoft SQL Server best practice, 1E recommends to provision at least three separate Azure disk volumes for SQL Data, Logs and TempDB. In the Azure Edsv4 virtual machine, it is possible to use the fast and large local SSD storage for TempDB, as this does not need to be persistent and is re-created automatically every time SQL Server starts.

The Data volumes may be made up from multiple Premium disks (in the higher spec Configurations), striped in a Basic Array using Windows Storage Spaces. This configuration allows for the local NVMe SSDs to act as a read-ahead cache for these striped volumes and gain better read performance. Please refer to https://learn.microsoft.com/en-us/azure/azure-sql/virtual-machines/windows/performance-guidelines-best-practices-storage.

> **Note**
>
> If the VM is created using the Azure SQL VM template, then the relevant disks will be automatically created as Windows Storage space volumes, with read-ahead caching enabled.
>
> Overall, these storage volumes should have the combined MBs throughput, equal to or above the total MBs supported by the given VM size, to gain maximum storage performance.

1.3.2.4.5.5 Increasing Azure SQL Server Performance

The latest Azure Ev5 series VMs provides up to three times an increase in remote storage performance compared with previous generations: https://azure.microsoft.com/en-us/blog/increase-remote-storage-performance-with-azure-ebsv5-vms-now-generally-available/.

For larger scale Tachyon environments, achieving the best storage throughput provides the best performance for long running data consolidation operations.

In addition, the latest Ev5 Series VMs support disk busting which provides the ability to boost disk storage IOPS and MB/s performance: https://learn.microsoft.com/en-us/azure/virtual-machines/disk-bursting

On-demand disk bursting in Azure is only available for premium disks of 1TB in size or greater (P30), but by enabling this on SQL data disk(s), allows you to achieve the maximum storage throughput available to the VM on high-intensity operations: https://learn.microsoft.com/en-us/azure/virtual-machines/disks-enable-bursting.

1.3.2.4.5.6 Azure prescriptive design patterns

Azure VM and storage sizing for different customer sizes

	Medium 1	**Medium 2**	**Large 1**	**Large 2**	**Large 3**
CPU Cores	4	8	16	32	64
RAM	16 GB	32 GB	64 GB	128 GB	256 GB
Tachyon Switches	1	1	2	4	10
NICs	2	2	3	5	11*
Remote SQL Server					
VM Type	**Std E4ds v4**	**Std_E8ds v4**	**Std E16ds v4**	**Std_E20ds_v4**	**Std_E64ds_v4**
CPU Cores	4	8	16	20	64
RAM	32 GB	64 GB	128 GB	160 GB	504 GB
Max MB/s	96	192	384	480	1,200
Max IOPS	6,400	12,800	25,600	32,000	80,00
DB Size	500 GB	1,000 GB	2,000 GB	4,000 GB	8,000 GB
MBs/IOPS	170/3,500	340/7,000	400/10,000	800/20,000	1,600/40,000
Logs Size	128 GB	256 GB	500 GB	1,000 GB	2,000 GB
MBs/IOPS	170/3,500	170/3,500	170/3,500	200/5,000	250/7,500

	Medium 1	Medium 2	Large 1	Large 2	Large 3
TempDB Size	150 GB	300 GB	600 GB	750 GB	2,000 GB
MBs/IOPS	242/38,500	485/77,000	968/154,000	1,211/193,000	3,872/615,000

Note

For customers with inter-meaning seats count, they should choose the closest higher number. For example, a 150,000-seat implementation should be treated as **Large 2** rather than **Large 1**.

As noted above, to reach the required throughput in MBs, for the data drive especially, multiple P20, P30 or P40 Premium disks should be used and these disks, striped using Windows Storage space to present a single volume.

The high MBs/IOPS for the TempDB drives is because they are using the built-in high throughput of the fast, local SSD based (non-persistent) storage that the Edsv4-series provides.

1.3.2.4.5.7 Azure network considerations

A server hosting a Tachyon Response Stack requires a dedicated network interface for each of its Switches, and for the connection to the remote SQL Server instance used for the Responses database to keep incoming traffic from clients separate from the outgoing traffic to the Response database.

Accelerated Networking which provides enhanced NIC performance using SR-IOV should be enabled on the SQL VM Network Interface and Platform VM Network Interface that communicates with it. Detailed steps on how to configure this are given here https://docs.microsoft.com/en-us/azure/virtual-network/create-vm-accelerated-networking-powershell.

Also increase the transmit (TX) and receive (RX) buffer sizes to their maximum under the network adaptor advanced properties.

If connecting to an Azure based Tachyon Switch via external public Azure IP addresses or Azure Load Balancers you will need to extend the default TCP timeout from 4 minutes to 15 minutes. Detailed steps on how to do this can be found here https://azure.microsoft.com/en-us/blog/new-configurable-idle-timeout-for-azure-load-balancer.

1.3.2.4.6 Amazon AWS

1.3.2.4.6.1 Out of scope

This document only focuses on AWS elastic cloud (EC2) instances and configurations using AWS Elastic Block Storage (EBS).

It does not consider using Microsoft SQL as part of AWS Platform as a Service (PAAS) offerings such as Amazon Relational Database Service (RDS) (https://aws.amazon.com/rds/) as this not currently supported by 1E as a means to implement SQL Server for Tachyon.

In addition, it does not consider using AWS instances that do not use the EBS platform but have local NVMe based storage such as I3en and R5d instance types.

Although these instance Types have very high performing storage and data transfer bandwidth, the NVMe disks are ephemeral or non-persistent, so only practical for SQL Server use for TempDB.

In the future, 1E plan to provide guidance in using non-persistent storage solutions as part of a **SQL Server Always on Availability Group** cluster, that provides storage resilience and redundancy as described in https://learn.microsoft.com/en-us/sql/database-engine/availability-groups/windows/overview-of-always-on-availability-groups-sql-server. However, since these solutions require a cluster of minimum 3 nodes, it should be noted these solutions would be much more expensive to implement.

1.3.2.4.6.2 AWS instance selection

This document should be read in conjunction with the AWS documentation, especially with guidance on Maximizing Microsoft SQL Server Performance with Amazon EBS https://aws.amazon.com/blogs/storage/maximizing-microsoft-sql-server-performance-with-amazon-ebs.

In recommending the desired AWS instance type and size 1E, has followed the following guidance.

- Instances are based on the latest AWS Nitro Systems https://aws.amazon.com/ec2/nitro
- Amazon EBS Optimized systems were selected, so that these can have the best possible storage throughput performance in terms of MB/s and IOPS https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-optimized.

Based on these factors 1E recommend using the EC2 M5 instances for the Tachyon server and R5 instances for the SQL server, to get the optimum ratio of vCPU and memory count.

EC2 M5/R5 instances have 3.1 GHz Intel Xeon® Platinum 8000 series processors with new Intel Advanced Vector Extension (AVX-512) instruction set and following specifications.

AWS EC2 M5 instances for the Tachyon server

Instance Size	vCPU	Memory (GiB)	Instance Storage(GiB)	Network Bandwidth (Gbps)	EBS Bandwidth (Mbps)
m5.xlarge	4	16	EBS-Only	Up to 10	Up to 4,750
m5.2xlarge	8	32	EBS-Only	Up to 10	Up to 4,750
m5.4xlarge	16	64	EBS-Only	Up to 10	4,750
m5.8xlarge	32	128	EBS Only	10	6,800
m5.12xlarge	48	192	EBS-Only	12	9,500

Instance Size	vCPU	Memory (GiB)	Instance Storage(GiB)	Network Bandwidth (Gbps)	EBS Bandwidth (Mbps)
m5.16xlarge	64	256	EBS Only	20	13,600
m5.24xlarge	96	384	EBS-Only	25	19,000

1.3.2.4.6.3 AWS instance CPU options

The above table shows the default number of vCPUs provisioned for a specific AWS instance type at creation time.

Amazon EC2 instances support multi-threading, which enables multiple threads to run concurrently on a single CPU core. By disabling hyper-threading, it is possible to get less vCPUs (and therefore lower SQL license requirements) whilst maintaining the higher storage throughput. Please refer to https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/instance-optimize-cpu.

1.3.2.4.6.4 AWS EBS storage selection

For any solution based on Microsoft SQL Server, storage throughput is normally the major bottleneck to performance, and Tachyon is no exception to this.

The maximum storage throughput in terms of MB/s and IOPS for specific AWS M5 instances is detailed in the table below and this will determine the maximum equivalent IOPS for the selected AWS storage volumes.

For example, if you attach a single 20,000-IOPS volume to an r5.4xlarge instance, you reach the instance limit of 18,750 IOPS before you reach the volume limit of 20,000 IOPS.

AWS EC2 R5 instances for the Tachyon SQL Server

Instance size	Maximum storage bandwidth (Mbps)	Maximum throughput (MB/s, 128 KiB I/O)	Maximum IOPS (16 KiB I/O)
r5.xlarge	4,750	593.75	18,750
r5.2xlarge	4,750	593.75	18,750
r5.4xlarge	4,750	593.75	18,750
r5.8xlarge	6,800	850	30,000

Instance size	Maximum storage bandwidth (Mbps)	Maximum throughput (MB/s, 128 KiB I/O)	Maximum IOPS (16 KiB I/O)
r5.12xlarge	9,500	1,187.5	40,000
r5.16xlarge	13,600	1,700	60,000
r5.24xlarge	19,000	2,375	80,000

The recommended AWS EBS storage type is Provisioned IOPS SSD (io1 and io2) volumes. These (io1 and io2) SSD volumes are designed to meet the needs of I/O-intensive workloads, particularly database workloads, that are sensitive to storage performance and consistency.

Unlike General Purpose EBS Storage (gp2), which uses a bucket and credit model to calculate performance, io1 and io2 volumes allow you to specify a consistent IOPS rate when you create volumes, and Amazon EBS delivers the provisioned performance 99.9 percent of the time. For more details see https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-volume-types.html.

As per Microsoft SQL Server best practice, 1E recommends to provision at least three separate AWS disk volumes for SQL Data, Logs and TempDB. These volumes may be made up from multiple Io1 disks, striped in a Basic Array using Windows Storage Spaces to create a single higher performance volume, with the combined IOPS of all individual disks in the Storage Pool. For an example of this, see https://d1.awsstatic.com/whitepapers/maximizing-microsoft-sql-using-ec2-nvme-instance-store.pdf.

The configured volumes should have the combined MBs/IOPS throughput, equal to or above, the total MBs/IOPS supported by the given instance type, to gain maximum storage throughput performance possible for the given instance type.

1.3.2.4.6.5 Increasing AWS SQL Server Performance

The latest AWS R5b EC2 instances are specifically designed for larger SQL Server deployments that require higher EBS performance per instance. R5b instances deliver up to 60 Gbps bandwidth and 260K IOPS of EBS performance, the fastest block storage performance on EC2: https://aws.amazon.com/blogs/compute/sql-server-runs-better-on-aws/.

For larger scale Tachyon environments, achieving the best storage throughput provides the best performance for long running data consolidation operations.

In addition, the latest Amazon EC2 R5b Instances benefit from the highest block storage performance with a single storage volume using io2 Block Express: https://aws.amazon.com/ebs/provisioned-iops/.

AWS R5b instances and block express EBS storage allows you to achieve the maximum storage throughput available to the VM for high-intensity SQL Server operations.

1.3.2.4.6.6 AWS EC2 prescriptive design patterns

AWS Instance and storage sizing for different customer sizes

	Medium 1	Medium 2	Large 1	Large 2	Large 3
AWS Instance	M5.xLarge	M5.2xlarge	M5.4xlarge	M5.8xlarge	M5.16xLarge
CPU Cores	4	8	16	32	64
RAM	16 GB	32 GB	64 GB	128 GB	256 GB
Switches	1	1	2	4	10
NICs	2	2	3	5	11
Remote SQL Server					
AWS Instance	R5.xlarge	R5.2xlarge	R5.4xlarge	R5.12xlarge	R5.16xLarge
CPU Cores	4	8	16	24*	64
RAM	32 GB	64 GB	128 GB	384 GB	512 GB
Max MB/s	593.75	593.75	593.75	1,187.5	1,700
Max IOPS	18,750	18,750	18,750	40,000	60,000
DB Disk Size	500 GB	1,000 GB	2,000 GB	4,000 GB	8,000 GB
DB Disk IOPS	10,000	10,000	12,000	24,000	48,000
Logs Disk Size	150 GB	300 GB	600 GB	1,200 GB	2,000 GB
Log Disk IOPS	5,000	5,000	6,000	8,000	16,000
TempDB Size	150 GB	300 GB	600 GB	1,200 GB	2,000 GB
TempDB IOPS	6,000	6,000	8,000	10,000	20,000

Note

Customers with intervening seats count, should choose the closest higher number. For example, a 150,000-seat implementation should be treated as **Large 2** rather than **Large 1**.

The **Large 2** sizing (*) uses a larger Instance size to get the necessary storage throughput but assumes disabling hyper-threading in the instance to reduce the vCPU count, and therefore, SQL license costs.

1.3.2.4.6.7 AWS network considerations

A server hosting a Tachyon Response Stack requires a dedicated network interface for each of its Switches, and for the connection to the remote SQL Server instance used for the Responses database to keep incoming traffic from clients separate from the outgoing traffic to the Response database.

Enhanced networking (SR-IOV) must be enabled on both NICs which should be the default. Also increase the transmit (TX) and receive (RX) buffer sizes to their maximum under the network adaptor advanced properties. Detailed steps on how to verify this are detailed here https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/sriov-networking.

1.3.2.4.7 Additional and complex configurations

1.3.2.4.7.1 Tachyon Switch and Background Channel servers (DMZ)

In some customer environments, with network segmentation, it may be beneficial to separate the Switch infrastructure servers from other Tachyon component servers so that clients connect to a more network local server, whilst the platform and SQL Servers reside in a more central datacenter subnet.

This same model is true for a DMZ environment, where remote clients only connect to **Switch** and **Background Channel** components in an intentionally separated DMZ environment and subnet.

Tachyon Setup (DMZ installation) can be used to install Tachyon components for required for client connectivity only, that is, the **Switch** and **Background Channel** (BGC).

Servers with only Switch and BGC components will have lesser memory, CPU core and storage requirements than a full Tachyon server, but the following requirements should be noted:

- As stated above, a new instance of the Switch is required for every 50k clients with a dedicated NIC of at least 1GBps speed. This network IP may be shared with the BGC.
- To support additional client connection count numbers, for every 50k clients, a separate dedicated NIC and additional instance of the Switch and separate IP address will be required.
- An additional internal facing interface is required for outgoing response traffic from Switch(s) on the Switch/DMZ Server to the internal Response Stack. This also should have a minimum speed of 1Gbps, or higher if hosting multiple switch instances.

On-premises and cloud specifications for a Switch and BGC (DMZ) server

Platform	On-premises	Microsoft Azure	Amazon AWS
CPU Cores	4	4	4
RAM	16 GB	16 GB	16 GB

Platform	On-premises	Microsoft Azure	Amazon AWS
Switches	1	1	1
NICs	2	2	2
Devices	**Up to 100,000**	**Up to 100,000**	**Up to 100,000**
Server Type	Physical or Virtual	Std_D8s_v4	M5.2xlarge
CPU Cores	8	8	8
RAM	32 GB	32 GB	32 GB
Switches	2	2	2
NICs	3	3	3
Devices	**Up to 200,000**	**Up to 200,000**	**Up to 200,000**
Server Type	Physical or Virtual	Std_D16s_v4	M5.4xlarge
CPU Cores	16	16	16
RAM	64 GB	64 GB	64 GB
Tachyon Switches	4	4	4
NICs	5	5	5

1.3.2.4.7.2 Separate Master and Response Stacks

The standard Tachyon installation assumes all components are installed on a single server, with databases hosted on a remote dedicated SQL Server.

However, it is also supported to split some of Tachyon components between multiple servers - in this configuration creating a **Tachyon Master Stack** server (Coordinator Service, Consumer API, Experience and SLA Inventory components) and one or more **Tachyon Response Stack** servers (Switch, Background Channel and Core components).

Tachyon Setup has different configuration options, to support these installation types, installing first a **Master Stack** and then separate **Response Stack** servers.

A split-server configuration would only really be practical in large scale environments, but does have a couple of advantages over installing all components on a single server:

- **Spread the H/W requirements into multiple, smaller servers:** If the required VM sizes (CPU and Memory or of NICs) is greater than the capabilities of the virtual host, then multiple smaller sized VMs may be more practical in some environments.
- **Provide some Resilience and fault-tolerance for the Platform:** Multiple and redundant Response Stack servers, would allow for the failure of a single Response Server VM, where all clients fall over to the remaining server and it's Switch instances in single VM failure.

Multiple Response Stacks can provide higher performance throughput than a single server, but at the cost of increased total vCPU and Ram for the platform, across multiple VMs.

To achieve resilience, it would assume the number of Switches configured and total capacity of a single Response server, is matched to the total load of all required client connections. This may mean at least three response server installations are required, so that two remaining response servers can handle all the required number of active connections, if one VM fails.

In terms of resilience, it should be noted that multiple redundant Response Servers only provide resilience in the failure of one of the redundant Response server VMs – if the separate and single Master Stack VM (or SQL Server) fails, then the entire Tachyon solution would be unavailable.

Overall resilience and high-availability would best be enabled using the standard high-availability features built-in to the chosen virtualization platform and at the storage system level (on-premises), or if in the cloud, through their specific high-availability and disaster recovery options.

The rule that for every 50,000 clients, Tachyon requires a separate instance of the Switch component, which requires a dedicated Network Interface (NIC), still applies for Response Servers, as they will host switch instance(s) alongside the Tachyon Core component.

If deploying separate Response and Master Stack servers, it is still recommended installing all Tachyon databases on a separate and dedicated SQL Server, so as not to mix a SQL Server installation with IIS other and web server components, as per Microsoft best practice. Therefore, the VM sizing guidelines, disk throughput and storage requirements for SQL Server VM will be identical, if either a single or split platform server configuration. Please refer to the above sections for SQL Server sizing, using specific total client counts required for the environment.

1.3.2.4.7.2.1 Response Stack server design patterns

With Response Stack servers, there are various configuration sizes that could be used to support the required maximum number of active clients, depending on required resilience or redundancy.

The basic formula for sizing a separate Response server is to allocate at least 8x vCPU cores and 16GB of memory for a maximum of 50,000 active clients reporting to that server.

Response Stack server sizing for different customer sizes

Response Servers				
CPU Cores	4	8	16	32
RAM	12 GB	24 GB	48 GB	96 GB
Switches	1	1	2	4

Response Servers				
NICs	2	2	3	5

Note

When planning for resiliency, there should be enough capacity in the individual Response Stack servers to allow for at least 1 VM server to fail, but the remaining VMs to have the capacity to support the total number of required connections.

1.3.2.4.7.2.2 Master Stack server design patterns

The basic formula for sizing a separate Master Stack server is to allocate at least 2x vCPU cores and 16GB of memory for every 50,000 active clients in the environment.

The following table details the VM CPU, Memory and NIC requirements for example individual Response servers, supporting a max total number of active clients in the environment.

Master Stack server sizing for different customer sizes

Master Stack Servers				
CPU Cores	2	4	8	16
RAM	16 GB	32 GB	64 GB	128 GB
NICs	1	1	1	1

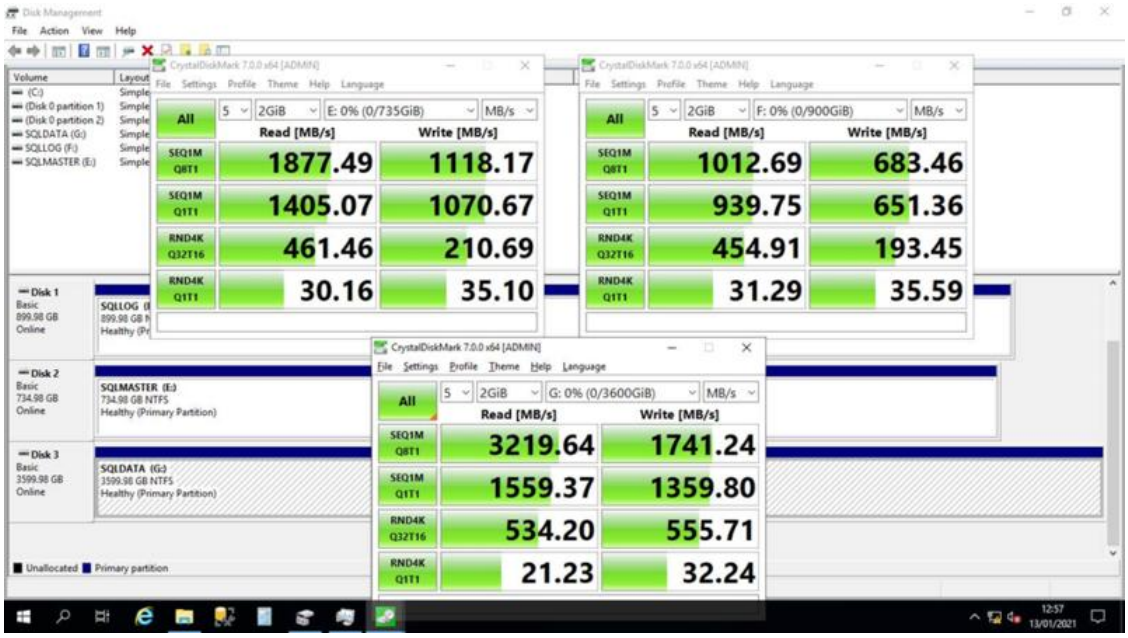
Note

Although the multiple (and potentially redundant) Response Stack servers can support more clients, the total number of active clients across all the Response Stack servers will always stay the same.

1.3.2.4.8 How we measure disk performance

There are a number of third party tools to measure disk and storage performance but the most commonly used and referenced by various hardware providers, is CrystalDiskMark (https://crystalmark.info/en/software/crystaldiskmark).

An example of the output from CrystalDiskMark is shown below, where the drives consist of an array of Samsung Pro 850, 6 Gb/s SATA SSDs.

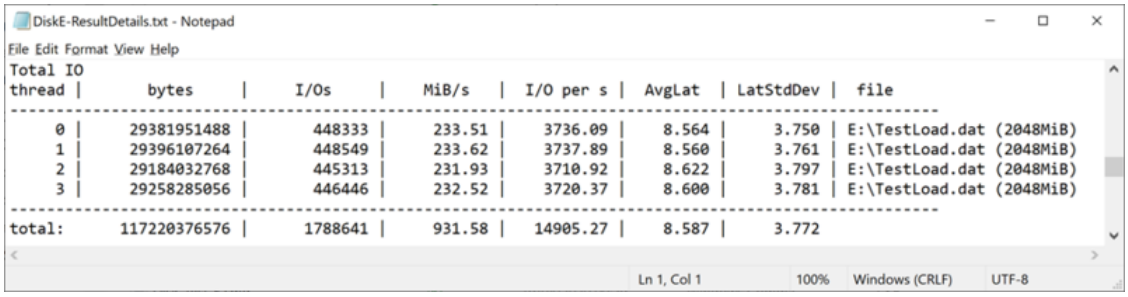


Under the hood, CrystalDiskMark uses the Microsoft tool **Diskspd** (https://github.com/microsoft/diskspd/releases) which can be useful to run on its own to get a simple and reproducible way to measure different server and VM disk subsystem performance.

Use the following command line to test each of the relevant SQL volumes, by drive letter, in turn.

Diskspd -b64k –d120 –o32 –t4 –h –r –w25 –L –c2G G:\TestLoad.dat > GDisk_resultdetails.txt

Once complete, review the output in the created results file **GDisk_resultdetails.txt** for the Total IO thread section. In the following example, the total throughput in MiB/s is measured at **931.58.**



Tachyon is more akin to a Data Warehouse type SQL Application (large sequential Writes and Reads) and not an OLTP type system (millions of small random IO requests). Therefore, overall throughput (MB/s) is more important than just IO alone. Also, when comparing IOPS in the sizing tables above (16k), and Diskspd at 64K block size, x4 to equate the values.

1.3.2.4.9 Table of references

External reference documents (mentioned in the above sections)

Section	Topic	Reference
General	SQL Server Performance	https://docs.microsoft.com/en-us/sql/relational-databases/performance/performance-center-for-

Section	Topic	Reference
		sql-server-database-engine-and-azure-sql-database?view=sql-server-ver15
SSAS performance guide	http://download.microsoft.com/download/d/2/0/d20e1c5f-72ea-4505-9f26-fef9550efd44/analysis%20services%20molap%20performance%20guide%20for%20sql%20server%202012%20and%202014.docx	
Network performance (RSS)	https://docs.microsoft.com/en-us/windows-hardware/drivers/network/introduction-to-receive-side-scaling	
What is an Always On availability group?	https://docs.microsoft.com/en-us/sql/database-engine/availability-groups/windows/overview-of-always-on-availability-groups-sql-server	
Crystal DiskMark and Diskspd	https://crystalmark.info/en/software/crystaldiskmark and https://github.com/microsoft/diskspd/releases	
Azure	What is Azure SQL?	https://docs.microsoft.com/en-us/azure/azure-sql/azure-sql-iaas-vs-paas-what-is-overview
Best practices for SQL Server on Azure VMs	https://docs.microsoft.com/en-us/azure/azure-sql/virtual-machines/windows/performance-guidelines-best-practices	

Section	Topic	Reference
Increasing Azure SQL Server Performance	https://azure.microsoft.com/en-us/blog/increase-remote-storage-performance-with-azure-ebsv5-vms-now-generally-available/ https://learn.microsoft.com/en-us/azure/virtual-machines/disk-bursting https://learn.microsoft.com/en-us/azure/virtual-machines/disks-enable-bursting	
Azure Storage for SQL VMs	https://docs.microsoft.com/en-us/azure/virtual-machines/premium-storage-performance#optimize-IOPS-throughput-and-latency-at-a-glance	
Azure Constrained Core VMs	https://docs.microsoft.com/en-us/azure/virtual-machines/constrained-vcpu	
Azure managed disk types	https://learn.microsoft.com/en-us/azure/virtual-machines/disks-types	
Azure Premium Storage	https://docs.microsoft.com/en-us/azure/azure-sql/azure-sql-iaas-vs-paas-what-is-overview	
Windows Storage Spaces	https://docs.microsoft.com/en-us/azure/azure-sql/virtual-machines/windows/performance-guidelines-best-practices-storage	
Azure Accelerated Networking	https://docs.microsoft.com/en-us/azure/virtual-network/create-vm-accelerated-networking-powershell	

Section	Topic	Reference
Azure Load Balancer	https://azure.microsoft.com/en-us/blog/new-configurable-idle-timeout-for-azure-load-balancer	
AWS	AWS SQL Server Best Practices	https://aws.amazon.com/blogs/storage/maximizing-microsoft-sql-server-performance-with-amazon-ebs
AWS Nitro Systems	https://aws.amazon.com/ec2/nitro	
AWS Storage optimized instances	https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-optimized.html and https://d1.awsstatic.com/whitepapers/maximizing-microsoft-sql-using-ec2-nvme-instance-store.pdf	
Increasing AWS SQL Server Performance	https://aws.amazon.com/blogs/compute/sql-server-runs-better-on-aws/ https://aws.amazon.com/ebs/provisioned-iops/	
AWS Constrained core Instances	https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/instance-optimize-cpu.html	
AWS EBS volume types	https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-volume-types.html	

Section	Topic	Reference
AWS Accelerated Networking	https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/sriov-networking.html	

1.3.2.5 SQL Server requirements

1.3.2.5.1 Local or remote SQL Server

You will need to decide if Tachyon databases are installed locally or on remote SQL Server instance(s).

Databases that are remote from their Tachyon Servers increase the complexity of design and installation in the following ways:

- Tachyon Server installation depends on the server installation account having appropriate rights on the SQL Server instance. Remote SQL Servers are typically run on farms managed by other teams who may not want to grant permissions to your installation account.
- If a Response Stack serves over 500 devices then you will require an additional network interface, which requires network routing as described in Network interfacesbelow.

Microsoft SQL Server Express is not supported for either Master or Responses databases, due to its limitations.

You will also require **SQL Server Analysis Services** if you are using Business Intelligence (as required by the Patch Success application).

Below is a list of SQL Server requirements covered in other sections on this page:

- SQL Server editions and configuration - see Server software section:
  - SQL Server database instance is required for databases
  - SQL Server Analysis Server (SSAS) instance for the SLA-BI cube (required by Patch Success).
- Network interface for remote SQL Server - see Network interfaces section
- Directory requirements: SQL Login for the Network Service account
- Directory requirements: SQL Logins for the server installation account
- Microsoft Bulk Copy Program (BCP) s installed on the Response Stack server(s) where the Tachyon Core component is installed, as described in Export all feature below.

Please refer to the /document/preview/791302#UUID-aa1c2691-97ed-e134-ac7d-62b2ea04fe4a page for details of SQL Server hardware and database sizing.

Please refer to High Availability options for SQL Server for HA options and their requirements.

1.3.2.5.2 Backup and recovery

You will need to regularly backup the following databases. The Tachyon server can be re-installed from scratch using the existing databases or a restored backup.

- 1E Catalog
- ContentDistribution (optional, required by Nomad)
- SLA-Data
- SLA-Shared
- SLA-Integrate
- SLA-BI (optional, required for Patch Success)
- TachyonMaster
- TachyonExperience (optional, required for Experience).

There is no requirement to backup the Tachyon Responses database because it only contains transient data. You can backup and restore the Responses database if that is your organization's preference for recovery.

There are no requirements to backup the ActiveEfficiency database, which you can delete. ActiveEfficiency is no longer supported.

For more detail about upgrading, please refer to Upgrading Tachyon Platform.

1.3.2.5.3 Export all feature

The **Export all** feature is available on the Explorer responses page, when an instruction has finished retrieving all its responses. To enable Tachyon users with the appropriate permissions to use this feature, you must ensure that the **Microsoft Bulk Copy Program** (BCP) is installed on the same Response Stack server(s) where the Tachyon Core component has been installed.

Please refer to Configure Tachyon to support the Export all responses feature for more details on configuring SQL BCP and setting up a suitable share.

1.3.2.6 High Availability options for SQL Server

1.3.2.6.1 High Availability options

Overview of High Availability (HA) options for SQL Server databases used by Tachyon and its applications. Includes steps before upgrading Tachyon, and post-installation steps required when using certain HA options.

The options described here provide resilience, they are not for increasing load and performance.

Tachyon supports the following High Availability (HA) options for SQL Server:

- AlwaysOn Availability Group (AG) using an AG Listener
- Failover Cluster Instance (FCI)

Tachyon does not support the following HA options for SQL Server:

- AlwaysOn Availability Group without an AG Listener
- AlwaysOn Availability Group on FCI
- AlwaysOn Basic Availability Group (provided by SQL Server Standard Edition)
- Older HA methods such as Log Shipping and Transactional Replication
- SQL Server Analysis Server (SSAS) databases.

This page does not describe HA options for application servers, that is servers with Tachyon Master and Response stack components, including DMZ Servers. SQL Server(s) must be remote from application servers, that is, not local. HA for Response stack components (Switches and Background Channel) is possible using multiple response servers and Network Load Balancing (NLB) as discussed in Network requirements.

> **Note**
>
> Please contact your 1E Account Team if you need help with HA for Tachyon Master stack components.

1.3.2.6.2 Failover Cluster Instance (FCI)

Installation, upgrade, and patching of Tachyon on a Failover Cluster Instance, are all supported by using Tachyon Setup.

The FCI Cluster has a **Virtual Network Name** (VNN). When you run Tachyon Setup, you must specify the **VNN** for each database in the Database servers screen.

When patching, you must use Tachyon Setup and 1E Hotfix bundles, as described in Tachyon Server post-installation tasks.

1.3.2.6.3 AlwaysOn Availability Group (AG)

Installation, upgrade, and patching of Tachyon servers in a AlwaysOn Availability Group, are all supported by using Tachyon Setup, provided your AG has an **AG Listener**.

This page does not support converting an existing installation without an AG, to one using an AG, because the re-configuration is too complex. However, you can convert as part of an upgrade, or re-installation, because Tachyon Setup will handle the configuration changes.

When installing Tachyon, you must specify the **AG Listener** name in Tachyon Setup. After installation, you can then add the databases to the AG, and manually copy SQL Logins and linked servers to secondary nodes.

When upgrading, you must temporarily remove Tachyon databases from the AG, and add them back after upgrading your Tachyon system.

> **Note**
>
> This page does not cover Basic Availability Groups (provided SQL Server Standard Edition). They are created and managed much like normal Availability Groups, but each AG only supports one database.

1.3.2.6.3.1 Prerequisites

In addition to all the requirements listed in SQL Server requirements, your AlwaysOn Availability Group (AG) must have an **AG Listener**.

> **Note**
>
> If the AG Listener is using a non-default port, then this must be included in the steps below. The Browser service does not help.

> **Note**
>
> The AG Listener name must have a **Service Principle Name (SPN)** registered for the SQL Server service account used by each SQL instance in the AG. Typically, all instances in an AG will use the same service account.

```
setspn -L domain\sqlserviceaccount

setspn -S MSSQLSvc/AGListenerName:port domain\sqlserviceaccount
setspn -S MSSQLSvc/AGListenerName.FQDN:port domain\sqlserviceaccount
```

The requirements include an **installation account** that must have a SQL Login with sysadmin or relevant rights on the primary node. If you have previously installed Tachyon, then you may already have this. Please refer to SQL Logins in Directory requirements.

You also require a user account that has sysadmin or relevant rights on all AG node instances, in order to manage the AG, replicate databases, create SQL Logins and linked servers. This can be the **installation account**.

1.3.2.6.3.2 Installing Tachyon

This scenario is for a new installation of Tachyon, and you have already prepared the Availability Group with an AG Listener.

> **Note**
>
> If you want to pre-create databases before a new installation, do *not* put them in the AG. SQL Server will find the empty databases in the primary node when you specify the AG Listener name in Tachyon Setup.

1. When you run Tachyon Setup to do the installation
   - you must specify the **AG Listener** name for each database in the **Database servers** screen
   - do not specify the **AG Listener** name in the **SSAS servers** screen
2. After installation, you can verify Tachyon functions
3. Manually add databases to the Availability Group
4. Manually copy SQL Logins to each secondary node
5. Manually copy linked servers to each secondary node
6. Verify the failover.

1.3.2.6.3.3 Upgrade Tachyon with an existing Availability Group

This scenario is for an existing installation that is already running in an AlwaysOn Availability Group.

You must use the following steps:

1. Remove all the Tachyon databases from their AG - keep the databases as full recovery model, do not change the AG, its replica(s), or the AG listener
2. Use Tachyon Setup to do the upgrade
   - you must specify the **AG Listener** name for each database in the **Database servers** screen
   - do not specify the **AG Listener** name in the **SSAS servers** screen
3. Manually add databases to the Availability Group.

You must use these steps to temporarily remove databases from the AG, because of a known issue with installers switching databases into single-user mode, which is not supported within an AG.

1.3.2.6.3.4 Upgrade Tachyon with a new Availability Group

This scenario is for an existing installation that you want to add to a new AlwaysOn Availability Group. The process is similar to a new installation.

You must use the following steps:

1. When you create the new Availability Group, ensure its primary node is the same as the SQL instance that hosts the existing Tachyon databases. Do not add the databases to the Availability Group yet.
2. When you run Tachyon Setup to do the upgrade
   - you must specify the **AG Listener** name for each database in the **Database servers** screen
   - do not specify the **AG Listener** name in the **SSAS servers** screen

   Note

   The Database servers screen will show the name of the original SQL instance (the primary node) but you must change these to the name of the AG Listener.
3. After the upgrade, you can verify Tachyon functions
4. Manually add databases to the Availability Group
5. Manually copy SQL Logins to each secondary node
6. Manually copy linked servers to each secondary node
7. Verify the failover.

1.3.2.6.3.5 Patching Tachyon

You must use Tachyon Setup and 1E Hotfix bundles, as described in Tachyon Server post-installation tasks.

1.3.2.6.3.6 Manually add databases to the Availability Group

You must manually add all databases to the AG after installing or upgrading Tachyon.

1.3.2.6.3.6.1 Tachyon databases

Tachyon uses the following SQL Server databases:

- 1ECatalog
- ContentDistribution (if using Content Distribution)
- SLA-Data
- SLA-Shared
- SLA-Integrate
- TachyonExperience (if using Experience)
- TachyonMaster
- TachyonResponses (if using a Response Stack)

1.3.2.6.3.6.2 Database recovery model

Before you add a Tachyon database to an Availability Group for the first time, you must change its recovery model from simple to full. You must do this for each Tachyon database.

> **Note**
>
> By default, Tachyon Setup installs its SQL databases with simple recovery model on the primary node of the Availability group. You must change each database to full recovery model before adding it to an Availability Group.
>
> With full recovery model, you must ensure you have a SQL maintenance plan to truncate logs, otherwise transaction logs will grow and cause performance and other issues.

1.3.2.6.3.6.3 Replicating databases to secondary nodes

When you add a database to an Availability Group, the SQL Server wizard provides two options for replicating the databases to the other AG nodes. Your choice depends on how quickly you need to complete the replication. You must do this for each Tachyon database.

- **Copy** - use this for new or small installations
- **Backup and restore** - use this for existing large installations - you can use the steps below, or whatever process your organization prefers

  1. Make a full backup of each database on the primary replica
  2. Make a tlog backup of each database on the primary replica
  3. Copy the database backups to the secondary replica

4. Restore the full backup (with no recovery) of each database on the secondary replica

5. Restore the tlog backup (with no recovery) of each database on the secondary replica.

1.3.2.6.3.7 Manually copy SQL Logins to each secondary node

When you install Tachyon, with application and SQL server in separate servers, Tachyon Setup creates a SQL Login on the primary node for the Tachyon application server's computer$ account. This is the remote representation of its **Network Service** account. For more information about this account, please refer to Directory requirements.

If you are installing SLA Business Intelligence (required by Patch Success) then Tachyon Setup will create a SQL Login for the **BI SSAS User** account.

The above SQL Logins must be manually copied to each secondary node. You can use the following steps to copy each SQL Login, or use whatever process your organization prefers. In summary, you will create a script for the SQL Login, which you then run on each of the secondary nodes.

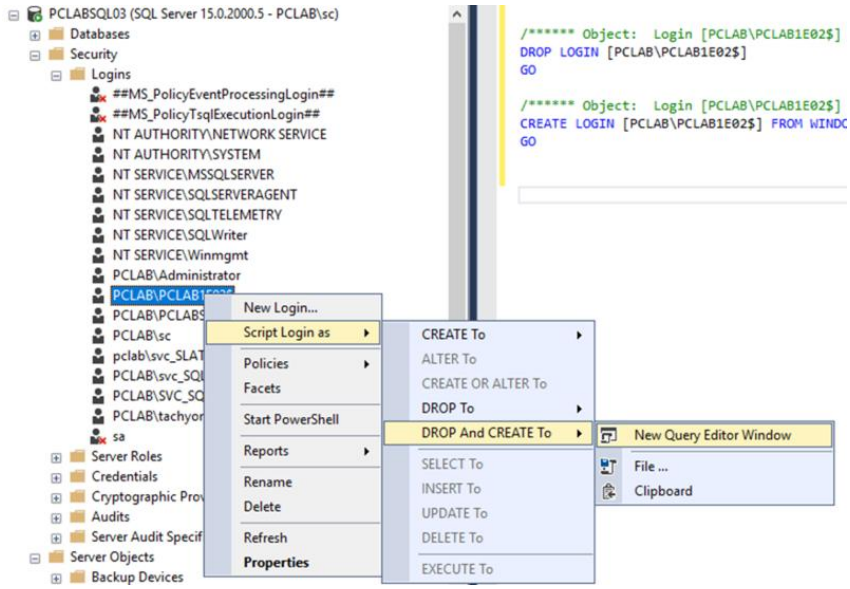
1. Using SQL Server Management Studio, connect to the primary node (the SQL instance where you originally installed Tachyon)

2. For each SQL Login

    a. Right-click on SQL Login, and select **Script Login as** → DROP And CREATE To → New Query Editor Window

    b. Save the new script

3. Connect to each secondary node, open the saved script as a new query, and execute it.



1.3.2.6.3.8 Manually copy linked servers to each secondary node

When you install Tachyon, it will create the following linked servers on the primary node. These must be manually copied to all the other nodes in the AG.

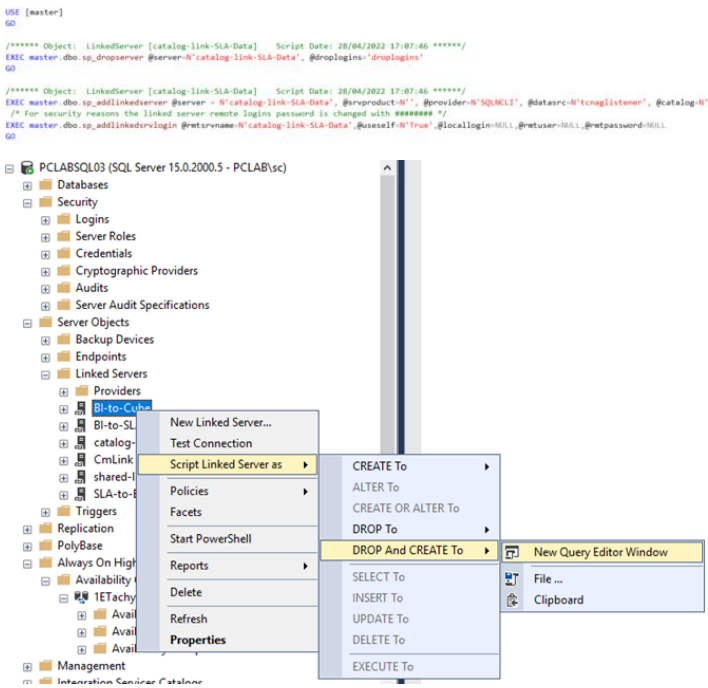
- catalog-link-SLA-Data

- shared-link-SLA-Data

You can use the following steps to manually copy each linked server, or use whatever process your organization prefers. In summary, you will create a script for each linked server, which you then run on each of the secondary nodes.

1. Using SQL Server Management Studio, connect to the primary node (the SQL instance where you originally installed Tachyon)
2. For each linked server
    a. Right-click on the linked server, and select **Script Linked Server as** → DROP And CREATE To → New Query Editor Window
    b. Save the new script
3. Connect to each secondary node, and for each linked server, open the saved script as a new query, and execute it
4. Repeat for each linked server on each of other nodes.

Below is an extract of an example script used to create the linked server **catalog-link-SLA-Data**. Note its **@datasrc** is the **AG Listener**, which you do not need to edit.



1.3.3 Windows Server requirements

You will need to provision one or more servers using the guidance provided here as the minimum specification.

For comprehensive guidance for CPU, RAM, disk volumes, and network connections, please refer to the /document/preview/791302#UUID-aa1c2691-97ed-e134-ac7d-62b2ea04fe4a page.

You will install each Tachyon Server using a wizard called Tachyon Setup. To make the process easier for installing Tachyon platform and its applications, the Tachyon Setup wizard aims to help you:

- Prepare for a successful deployment of Tachyon platform and applications
- Find online resources for Tachyon platform and applications
- Check and configure prerequisites
- Create the Tachyon Server certificate for use with the Tachyon Server website and the Tachyon Switch
- Deploy selected components
- Perform post-installation tasks, including configuring the components for interaction with each other
- Running validation tests on the completed installation.

The correct choice of DNS Name(s) for your Tachyon Servers is perhaps the most fundamental decision you will make.

1.3.3.1 Server software

Category	Product	Notes
Server OS	• Windows Server 2022 • Windows Server 2019 • Windows Server 2016	For more detail about configuration of servers, please refer to Windows Server requirements. Only 64-bit server OS are supported. The server must be domain-joined. This version of Tachyon requires the server OS to be **English** because of a Known issues with certain regional settings. If TLS 1.0 is disabled, then please ensure you follow the steps in If TLS1.0 is disabled to add registry entries, for the 1E Catalog Update Service to successfully connect to the 1E Cloud Catalog. **Note** This list shows only those OS versions in mainstream support by Microsoft, and therefore

Category	Product	Notes
		supported by Tachyon, and by 1E Client 8.1. Please refer to Constraints of Legacy OS regarding the end of mainstream support. For Microsoft product lifecycle details, please refer to https://support.microsoft.com/en-us/lifecycle/search. Refer to Support for Microsoft Rapid-Release Cycle on https://support.1e.com/ for details of which Current Branch versions are supported by 1E products, and known issues regarding specific versions.
SQL Server and SQL Server Analysis Services (SSAS)	• SQL Server 2019 • SQL Server 2017 • SQL Server 2016 SP3	For more detail, please refer to SQL Server requirements. Standard and Enterprise editions of these versions of SQL Server and SQL Server Analysis Services (SSAS) are supported. SQL Server 2016 RTM is not supported due to some issues, which are resolved by SP3. **Note** Tachyon only supports AlwaysOn Availability Groups on **SQL Server Enterprise Edition**. Please refer to High Availability options for SQL

Category	Product	Notes
		Server for HA options and their requirements. **Note** If you intend to integrate with third-party business intelligence products such as Power BI, you must install the **Enterprise edition of SSAS** as per their requirements. A SQL Server database instance is required for the following databases: • **1ECatalog** • **ContentDistribution** (optional - required for Nomad) • **SLA-BI** (optional - required for Patch Success) • **SLA-Data** • **SLA-Integrate** • **SLA-Shared** • **TachyonExperience** (optional - required for Tachyon Experience) • **TachyonMaster** • **TachyonResponses** **SLA Inventory databases** Tachyon Setup can install the above databases on separate SQL Server instances, however SLA-Data, SLA-Integrate, and

Category	Product	Notes
		SLA-Shared must exist on the same instance. A SQL Server Analysis Services (SSAS) instance installed in **Multidimensional** mode is required for SLA Business Intelligence. **SLA Business Intelligence** SLA Business Intelligence (BI) is only required for the Patch Success application. Together, the SLA Platform and BI installers create the following: • A database called **SLA-BI** on the SQL Server database instance. • A MOLAP cube called **SLA-BI** on the SSAS instance. • A linked server for the SLA databases to get data from the SLA-BI database and then from the SLA-BI cube. • A linked server for the SLA-BI database to get data from the SLA databases. • A datasource definition used by the SLA-BI cube to connect to the BI database. If the SLA databases, BI database, or SSAS instance for BI, are on *different* SQL Servers then the BI installer enforces

Category	Product	Notes
		the use of a SQL login on each instance. If they are on the *same* SQL Server then the installer gives you a choice of using integrated security (domain user account) or a SQL login. However, if you are installing all the components using Tachyon Setup instead of their individual installers, then you are not given the choice. Tachyon Setup always uses integrated security. Contact your 1E Account Team if your scenario requires the above-mentioned databases to be on *different* SQL Servers. This affects different servers, not different instances. All SQL Server instances *must* be configured with the following: • A case-insensitive, accent-sensitive collation which is **SQL_Latin1_General_CP1_CI_AS** by default, • **Allow remote connections to this server** enabled. All SQL Servers should be configured with the **SQL Server Browser service** running in order for the BI installer to select from a list of instances. **SQL Server Management Studio** is required to review the

Category	Product	Notes
		configuration and edit settings in 1E database tables. If installing SQL Server locally, note: • SQL Server 2016 and 2017 require .NET Framework 4.6 or later • SQL Server setup requires PowerShell 2.0. For the latest information about SQL Server prerequisites, please refer to http://go.microsoft.com/fwlink/?LinkId=622999.
Microsoft Endpoint Configuration Manager	• MECM CB 2303 • MECM CB 2211 • MECM CB 2207 • MECM CB 2203 • MECM CB 2111 • MECM CB 2107	Tachyon uses Configuration Manager for the following optional apps and features: • Reclaiming a product using SCCM Uninstall • Introducing Application Migration • Introducing Inventory captures data using the System Center Configuration Manager connector • Tachyon extensions for the Configuration Manager Console. - installed on Configuration Manager consoles using the 1E Tachyon Toolkit installer • Introducing Nomad requires 1E Client with Nomad client features enabled.

Category	Product	Notes
		Nomad provides the following Content Distribution features for Configuration Manager: • Nomad app overview provides visibility of content distribution activity • Single Site Download (SSD) (SSD). • Task sequence actions to augment OS Deployment: – Peer Backup Assistant - PBA – High Availability PBA (HAPBA) – Get Migration Settings to manage computer associations. • Nomad Pre-caching • Nomad Download Pause. Nomad requires the Content Distribution web service to synchronize with the Configuration Manager database. For standalone primary site environments, permissions are automatically assigned to the service account of Content Distribution's web application pool service (by default Network Service) using the **ConfigMgr_DViewAccess** localgroup native to Configuration Manager. For a CAS, this group is not created natively therefore additional steps are required to allow access. Please refer to Preparation: Microsoft

Category	Product	Notes
		Endpoint Configuration Manager preparation.
Web Server	• IIS 10	See Windows Server roles and features for details about required Web Server roles and features.
Runtime libraries	• Visual C++ 2013 Redistributable • Visual C++ 2015-2019 Redistributable • ASP.NET Core Framework 3.1 • .NET Framework 4.8	See Windows Server roles and features for details about required .NET Framework roles and features. To know supported combinations of OS and .NET Framework, please refer to: https://docs.microsoft.com/en-us/dotnet/framework/migration-guide/versions-and-dependencies. • Windows Server 2022 has .NET Framework 4.8 installed by default. • Windows Server 2019 has .NET Framework 4.7.2 installed by default. • Windows Server 2016 has .NET Framework 4.6.2 installed by default. **ASP.NET Core Hosting Bundle** is required only for the Nomad. It is not included with the Operating System, and must be downloaded and installed separately. If it not already installed, Tachyon Setup will attempt to automatically download version **3.1.11** and install it. Alternatively you can download it, or a later version, and install it yourself. For more detail please refer to ASP.NET Core Hosting Bundle. Installers include and automatically installs the redistributable packages

Category	Product	Notes
		for **Visual C++ 2013** and **Visual C++ 2015-2019**. The Coordinator (licensing module on the Master Stack), and Switch (on Response Stack) are written in C++ using Visual Studio 2013 and 2019, therefore require the **runtime (x64)** versions of these packages. Other server components use .NET Framework. **SQL BCP** is required by the **Export All** feature described in Exporting data from Explorer, and must be installed on each Tachyon Response Stack server (specifically the servers which have the Tachyon Core installed). BCP uses ODBC, which requires **Microsoft ODBC Driver versions 13.1 and 17** and **Visual C++ 2017 Redistributable** to be installed first. Please refer toP SQL BCP for more detail.
Other software	• PowerShell	PowerShell is required by Tachyon installer during installation.
Browsers	Latest version of: • Google Chrome • Microsoft Edge (Chromium) • Mozilla Firefox	A browser is not a prerequisite for installation of Tachyon servers but is required to use and administer the Tachyon platform. The administration is performed via the Tachyon portal and can be on a remote computer. These browsers are supported on all OS platforms which the browser vendor supports. The Portal and any API should be added as a trusted site. This is especially important when running

Category	Product	Notes
		scripts that may produce unexpected errors. Please review Known Issues Using Tachyon. **Note** **Microsoft legacy browsers** Support has been withdrawn for **Internet Explorer 11** and **legacy Microsoft Edge** (non-Chromium version) because Microsoft no longer supported them since 2021. We recommend you use Google Chrome, Firefox, or Microsoft Edge Chromium browser.

1.3.3.2 Naming

1.3.3.2.1 Computername

The computername of a Tachyon Server must comply with Microsoft NetBIOS naming standards, which includes having a length of 15 characters or less.

Microsoft's guidance can be found here: https://docs.microsoft.com/en-us/windows/desktop/SysInfo/computer-names.

1.3.3.2.2 DNS Names and SPNs

Please refer to the following sections on the Network requirements page:

- Network interfaces
- DNS Names
- Service Principal Names

1.3.3.3 Windows Server roles and features

Items in **bold** are included in the PowerShell script available for download from Windows Server roles and features.

Note

Tachyon Setup will create a website with the necessary bindings, therefore please do not pre-create a website of the same name.

The following roles, role services and features must be **installed/enabled** as a minimum. The **Name** column is the reference used in PowerShell commands.

In the case of .NET Framework features we refer to 4.X in the **Display Name**, as X may be different depending on the server OS. The PowerShell **Name** always uses 45 instead of the actual version.

Role or Feature	Display Name	Name	Notes
Web Server	**Web Server (IIS)**	**Web-Server**	
Web Server Common HTTP Features	Default Document	Web-Default-Doc	Included in Web-Server.
Directory Browsing	Web-Dir-Browsing	Included in Web-Server.	
HTTP Errors	Web-Http-Errors	Included in Web-Server.	
Static Content	Web-Static-Content	Included in Web-Server.	
HTTP Redirection	**Web-Http-Redirect**	Only required to support **legacy Nomad clients** after upgrading ActiveEfficiency.	
Web Server Health and Diagnostics	HTTP Logging	Web-Http-Logging	Included in Web-Server.
Web Server Performance	Static Content Compression	Web-Stat-Compression	Included in Web-Server.

Role or Feature	Display Name	Name	Notes
Dynamic Content Compression	**Web-Dyn-Compression**		
Web Server Security	Request Filtering	Web-Filtering	Included in Web-Server.
Basic Authentication	**Web-Basic-Auth**	Only required if using 1E ITSM Connect or 1E Core for integrating ServiceNow and Tachyon.	
IP Address and Domain Restrictions	**Web-IP-Security**	See note below.	
Windows Authentication	**Web-Windows-Auth**		
Web Server Application Development	.NET Extensibility 4.X	Web-Net-Ext45	Included in Web-Asp-Net45.
ASP.NET 4.X	**Web-Asp-Net45**		
ISAPI Extensions	Web-ISAPI-Ext	Included in Web-Asp-Net45.	
ISAPI Filters	Web-ISAPI-Filter	Included in Web-Asp-Net45.	
Web Server Management Tools	**IIS Management Console**	**Web-Mgmt-Console**	
.NET Framework 4.X Features	**.NET Framework 4.X**	**Net-Framework-45-Core**	

Role or Feature	Display Name	Name	Notes
ASP.NET 4.X	**Net-Framework-45-ASPNET**		

The following roles, role services and features must be removed/disabled.

Parent	Display Name	Name
Web Server Common HTTP Features	WebDAV Publishing	Web-DAV-Publishing

IIS Features Configuration

Core web applications use **IP and Domain Restrictions** so that only specific servers can access it. Other web applications cannot be accessed using HTTP because their **SSL Settings** are configured with **Require SSL**.

The web applications for the Consumer API and Explorer use Tachyon role-based security and therefore have **Windows Authentication** enabled. The other web applications have **Anonymous Authentication** enabled.

HTTP Redirection (Web-Http-Redirect) is only required to support legacy Nomad clients after an In-place upgrade of ActiveEfficiency Server for Nomad

Basic Authentication (Web-Basic-Auth) is required only if you will be installing 1E ITSM Connect or 1E Core for integrating ServiceNow and Tachyon.

Note

Web-Http-Redirect is only required to support legacy Nomad clients after an In-place upgrade of ActiveEfficiency Server for Nomad.

Web-Basic-Auth is only required if you will be installing 1E ITSM Connect or 1E Core for integrating ServiceNow and Tachyon.

1.3.3.4 Anti-Virus and Malware

The following should be excluded from scans to prevent file locking and resource deletion.

- 1E log files. See Log files for details of Tachyon Server and 1E Client logs
- The Background channel virtual directories (Agent, Content, Installers, PolicyDocuments, and Updates, which by default are in **%programdata%\1E\Tachyon**)

1.3.3.5 Constraints of Legacy OS

In this documentation, the following are referred to as legacy OS. Below are described some known issues for these OS.

1E does not provide support for 1E products on the following OS unless the OS is explicitly listed as being supported for a specific 1E product or product feature. This is because Microsoft has ended mainstream support for these OS or they are not significantly used by business organizations.

- **Windows XP ***
- **Windows Vista**
- **Windows 7**
- **Windows 8.0**
- **Windows 8.1**
- **Windows Server 2003 ***
- **Windows Server 2008**
- **Windows Server 2008 R2**
- **Windows Server 2012**
- **Windows Server 2012 R2**

Note

1E Client 8.1 and later will not install on Windows XP and Windows Server 2003. Please contact 1E if you intend to continue using any of the other legacy OS. If you experience an issue, then please try replicating the issue on a supported OS.

For Microsoft product lifecycle details, please refer to https://support.microsoft.com/en-us/lifecycle/search.

1.3.3.5.1 Microsoft legacy browsers

Support has been withdrawn for **Internet Explorer 11** and **legacy Microsoft Edge** (non-Chromium version). 1E has taken this decision for new releases that are expected to remain in support by 1E beyond March 2021 when **Microsoft Edge** goes end of life and August 2021 when **Internet Explorer 11** goes end of life. We recommend you use Google Chrome, Firefox or Microsoft Edge Chromium browser.

1.3.3.5.2 Certificate limitations - SHA2

Like most software vendors, 1E software requires the OS to support SHA2. If your organization has a PKI configured to use SHA2 256 or higher encryption, then your legacy OS may have already been updated to support it.

- Windows XP and Server 2003 require an update as described in **KB968730.** Microsoft no longer provides this hotfix as a download. You must contact Microsoft Support if you need it
- Windows 7 and Server 2008 R2 require an update as described in **KB3033929**. This update is not available for Vista and Server 2008
- Windows 8, 8.1, Server 2012, Server 2012 R2 and later OS already support SHA2.

1.3.3.5.3 Certificate limitations - encrypted certificate requests

Windows XP and Server 2003 are unable to encrypt certificate requests, whereas later OS are able to support higher more secure RPC authentication levels. If you are using a Microsoft CA and expect these clients to request (enrol) certificates then the CA must have its IF_ENFORCEENCRYPTICERTREQUEST flag disabled. It is disabled by default on Windows 2003 and 2008 CA, but is enabled by default on Windows 2012 CA.

To determine which InterfaceFlags are set, execute the following command on the CA server:

```
certutil -getreg CA\InterfaceFlags
```

If the following is specified then it means the flag is enabled.

```
IF_ENFORCEENCRYPTICERTREQUEST -- 200 (512)
```

To disable the encrypt certificate requests flag, execute the following commands on the CA server:

```
certutil -setreg CA\InterfaceFlags -IF_ENFORCEENCRYPTICERTREQUEST
sc stop certsvc
  sc start certsvc
```

1.3.3.5.4 Certificate limitations - signing certificates missing

On Windows computers, the installation MSI files, and binary executable and DLL files of 1E software are digitally signed. The 1E code signing certificate uses a timestamping certificate as its countersignature. 1E occasionally changes its code signing certificate, and uses it for new releases and patches for older versions, as shown in the table(s) below.

Root Certificate Authorities are implicitly trusted to validate certificates, and their certificates must be correctly installed to do this. Your computers should already have the necessary **root CA** certificates installed, however this may have been prevented by your organization's security policies, or inability to connect to the Internet, or they are legacy OS. In general this is not an issue because by default Windows allows software to be installed and run without validation, although you may see a warning or experience a delay. However, you *must* have relevant CA certificates installed if you are using 1E Client (which self-validates its own files), or your organization has applied more secure polices (for example UAC, AppLocker or SmartScreen).

Typical reasons for issues with signing certificate are:

- If your organization has disabled **Automatic Root Certificates Update** then you must ensure the relevant **root CA** certificates are correctly installed on each computer
- If computers do not have access to the Internet then you must ensure the relevant **root and issuing CA** certificates are correctly installed on each computer, numbered in the table(s) below.

The signature algorithm of the 1E code signing certificate is SHA256RSA. In most cases, the file digest algorithm of an authenticode signature is SHA256, and the countersignature is a RFC3161 compliant timestamp. The exception is on legacy OS (Windows XP, Vista, Server 2003 and Server 2008) which require the file digest algorithm of an authenticode signature to be SHA1, and a legacy countersignature.

The table below applies to software and hotfixes released in 2020.

2020	Signing certificate	Timestamping certificates
Certificate	1E Limited	TIMESTAMP-SHA256-2019-10-15 ***and*** DigiCert Timestamp Responder

2020	Signing certificate	Timestamping certificates
Issuing CA	**DigiCert EV Code Signing CA (SHA2)** Thumbprint: 60ee3fc53d4bdfd1697ae5beae1cab1c0f3ad4e3	**DigiCert SHA2 Assured ID Timestamping CA** Thumbprint: 3ba63a6e4841355772debef9cdcf4d5af353a297 ***and*** **DigiCert Assured ID CA-1** Thumbprint: 19a09b5a36f4dd99727df783c17a51231a56c117
Root CA	**DigiCert High Assurance EV Root CA** Thumbprint: 5fb7ee0633e259dbad0c4c9ae6d38f1a61c7dc25	**DigiCert Assured ID Root CA** Thumbprint: 0563b8630d62d75abbc8ab1e4bdfb5a899b24d43

1.3.3.5.5 Certificate limitations - expired root certificates

Ensure that your Root CA Certificates are up-to-date on clients and servers. The **Automatic Root Certificates Update** feature is enabled by default, but its configuration may have been changed or restricted by Group Policy **Turn off Automatic Root Certificates Update**.

If this GPO is enabled, then you will see *DisableRootAutoUpdate = 1 (dword)* in *HKLM\Software\Policies\Microsoft\SystemCertificates\AuthRoot.*

1.3.3.5.6 PowerShell limitations

PowerShell version 3.0 (required by some Tachyon instructions) is not supported on Windows XP, Vista and Server 2003. However, PowerShell 2.0 is supported on the following OS versions:

- Windows XP SP3
- Vista SP1 & SP2
- Windows Server 2003 R2 & SP2.

1.3.4 Certificate requirements

You need to have a PKI in your environment with at least one Issuing CA. Each server that has Tachyon Server components installed requires its own Web Server certificate (except for a remote SQL Server). By default, every client requires a client authentication certificate.

Client-Switch communication uses **WebSocket Secure** protocol, whereby each client establishes a secure link to the Switch, which is then used by the Switch to send instructions to the client. This is shown as a dotted line in the pictures on the Communication Ports page.

All other communications from external devices use **HTTPS**, including client connecting to the Background Channel in order to download resources that may be required by instructions, and using the Tachyon Portal to administer and use the system.

All communication is encrypted, which requires a **Public Key Infrastructure** (PKI).

1.3.4.1 PKI certificates

PKI is required for:

- **Web Server certificate** - prerequisite for each Tachyon server website, must contain all the DNS Names used for the server
- **Tachyon server's client authentication certificate** - only on Tachyon servers hosting a Background Channel, and only if using Content Distribution
- **Client authentication certificates** - each 1E Client uses the device's client certificate to authenticate itself to Tachyon Switches
- **Certificate Revocation Lists (CRLs)** - 1E Clients and Switches use HTTP-based CRL Distribution Points to validate certificates
- **Code signing certificates** - used for signing custom and modified instructions, so they can be imported into Tachyon and then run
- **Digital signing certificates** - used for signing 1E software.

1.3.4.2 Public Key Infrastructure

You need to have a PKI in your environment with at least one Issuing CA.

Tachyon requires each Issuing CA has:

- A **Certificate Revocation List** (CRL) **Distribution Point** (CDP) that uses HTTP/S.
- This HTTP/S CDP information included in certificates issued to Tachyon Server and client devices.

PKI notes

If you have an existing PKI and have just added a new CDP to support HTTP/S then you will need to re-issue certificates to your servers and devices.

Tachyon web server deliberately does not work with self-signed certificates for security reasons. Therefore, Tachyonservers cannot be installed on the same server as a Root CA, because its certificate is self-signed. For the same reason, 1E Client cannot be installed on a DC unless the client's Switch is configured to not require client certificates.

Tachyon supports TLSv1.2 and TLSv1.3. If your PKI is using SHA512, then please ensure that your environment has relevant updates applied, as described in KB2973337. See Enabling SHA-512 to work with TLSv1.2.

If you want Tachyon to manage legacy OSs that Microsoft no longer supports, there may be issues with encrypted certificates described in Constraints of Legacy OS.

Note

1E Client and Tachyon Switches use OpenSSL and its validation process to verify certificates. Websites use Microsoft IIS validation methods.

1.3.4.3 Web Server certificate

Each server that has Tachyon server components installed requires its own Web Server certificate (except for a remote SQL Server). This certificate is also used by the Switch and the Coordinator. Therefore, a single-server installation requires only one Web Server certificate. This certificate must be provided on the server prior to installation of Tachyon.

The Web Server certificate requires the minimum of the following:

1. Issued by a trusted Certificate Authority (CA)
   - The certificate for the Root CA in the Certification Path must exist in the Trusted Root CA store of the server
   - If the issuing CA is not the Root CA then the certificate for the issuing CA and any intermediate CA in the Certification Path must exist in the Intermediate CA store of the server
   - The above CA certificates must exist on the Tachyon Web Server and Windows client devices
   - Most organizations have automated distribution of these CA certificates to servers and clients, using Group Policy for example.
2. Has at least the following Key Usage:
   - Digital signature
   - Key encipherment.
3. Has at least the following Enhanced Key Usages:
   - Server Authentication.
4. Revocation information is included
   - References at least one CRL Distribution point that uses HTTP - see DMZ Server note below.
5. Must have a private key available.

Tip

The default template **Web Server** available with a Microsoft PKI is suitable for requesting a Tachyon Web Server certificate.

DMZ Server

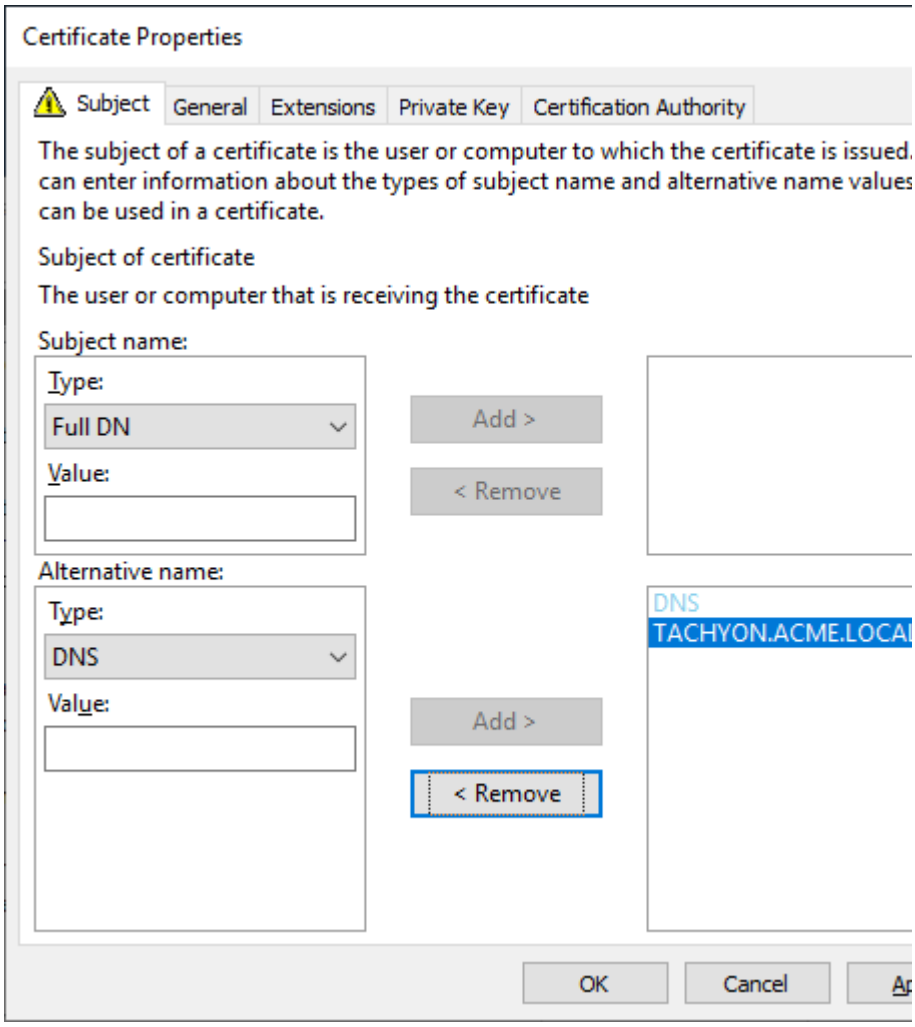
Please ensure you note the additional certificate requirements described below, when installing any server in a system that also contains a DMZ Server. Internal Master and

Response Stack servers, and DMZ Server, each require **two** HTTPS bindings, as described in DNS Names. For even more detail, please refer Implementing a Tachyon DMZ Server.

Also note the requirement for server certificates to reference at least one CRL Distribution point that uses HTTP. These CRL DPs are likely to be in the internal network, and the firewall will need to allow the DMZ server to access these internal servers.

Web Server certificates used by a Tachyon servers must be issued with their fields set as follows. Example **DNS Names** are discussed in DNS Names.

Fields	Example Option 3 type certificate
Subject Common Name Field (subject:commonName)	Subject (CN) can be any valid name, and is no longer mandatory as required by previous versions of Tachyon.
Subject Alternative Name Extension (extensions:subjectAltName), type dnsName	The **Tachyon server DNS Name FQDN** (DNS Alias) of the server. This is mandatory, same as required by previous versions of Tachyon. On a Master Stack - example: **DNS Name=TACHYON.ACME.LOCAL** On a Response Stack - example: **DNS Name=TACHYONRS.ACME.LOCAL** On a DMZ Server - example: **DNS Name=TACHYONEXT.ACME.COM**
Subject Alternative Name Extension (extensions:subjectAltName), type dnsName	An **Alternate DNS Name FQDN** (DNS Alias) of the server. This is usually mandatory, for example if there is more than one server in your Tachyon system, as discussed in DNS Names. On a Master Stack, example: **DNS Name=TACHYONALT.ACME.LOCAL**or**DNS Name=TACHYON.ACME.LOCAL** On a Response Stack - example: **DNS Name=TACHYONALT.ACME.LOCAL** On a DMZ Server - example: **DNS Name=TACHYONDMZ.ACME.LOCAL**

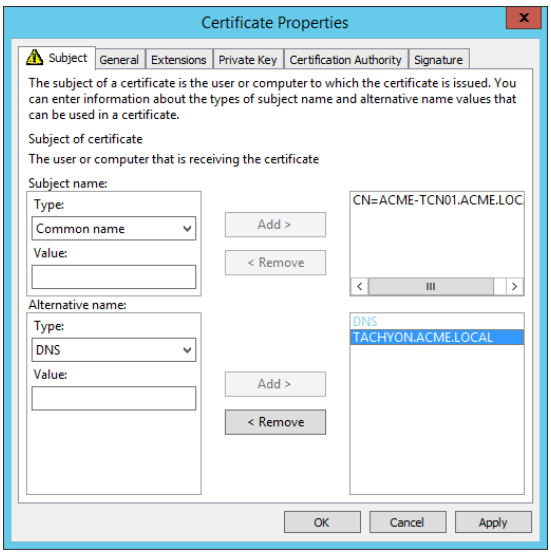
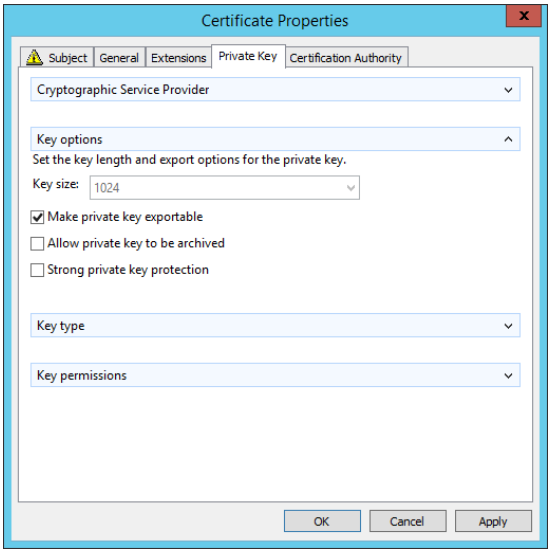
Fields	Example Option 3 type certificate
Example	

Note

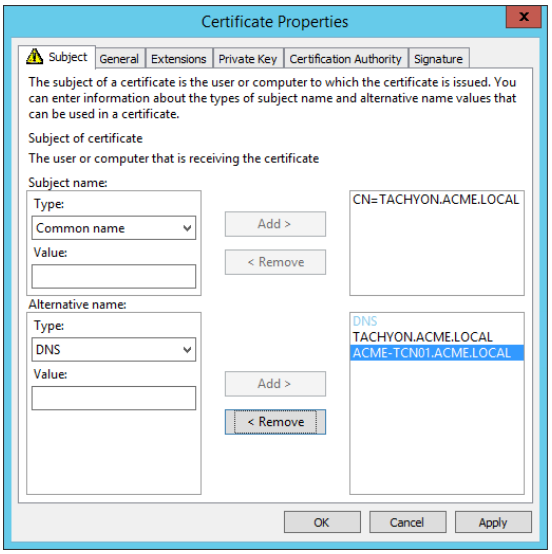
Earlier versions of Tachyon required the certificate to have a CN and used SAN fields differently. If you are upgrading your Tachyon server from an earlier version, it may still be using this type of certificate. When upgrading Tachyon, you can issue a replacement certificate, or continue using the old style certificate (because the new-style certificate requires only a SAN DNS Name that matches the DNS Alias, which are provided by the old style certificates).

Examples of old-style certificates:

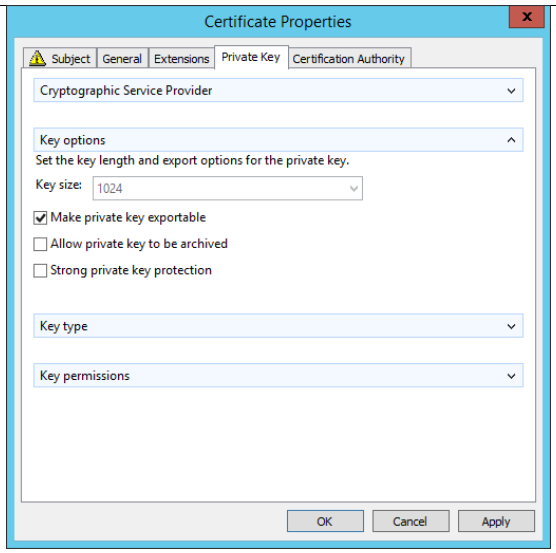
Fields	Example old Option 2 type certificate
Subject Common Name Field (subject:commonName)	The computername FQDN of the server

Fields	Example old Option 2 type certificate
	Example: **CN=ACME-TCN01.ACME.LOCAL**
Subject Alternative Name Extension (extensions:subjectAltName), type dnsName	The DNS Alias FQDN of the server Example: **DNS Name=TACHYON.ACME.LOCAL** **Tip** Add any additional DNS Names here.
Example certificate request	  **Note** Option 2 type certificates required the CN to be the computername FQDN, and the list of

Fields	Example old Option 2 type certificate
	Subject Alternate Names (SAN) to contain the DNS Alias. Also, prior to Tachyon 5.0 the certificate required its private key to be exportable. Tachyon 5.0 and later is able to use this type of certificate when upgrading from an earlier version of Tachyon.

Fields	Example of old Option 1 type certificate
Subject Common Name Field (subject:commonName)	The DNS Alias FQDN of the server Example: **CN=TACHYON.ACME.LOCAL**
Subject Alternative Name Extension (extensions:subjectAltName), type dnsName	The DNS Alias FQDN of the server Example: **DNS Name=TACHYON.ACME.LOCAL** The computername FQDN of the server Example: **DNS Name=ACME-TCN01.ACME.LOCAL**
Example certificate request	

Fields	Example of old Option 1 type certificate



Note

Option 1 type certificates required the CN to be the DNS Alias, and the list of Subject Alternate Names (SAN) to contain the computername FQDN.

Also, prior to Tachyon 5.0 the certificate required its private key to be exportable.

Tachyon 5.0 and later is able to use this type of certificate when upgrading from an earlier version of Tachyon.

The following need to be considered when requesting this type of certificate.

- The certificate can be used only on the server it was intended, that has the correct computername FQDN and DNS Alias FQDN.
- It is not possible to use the **Create Certificate Request** method in IIS Manager Server Certificates, because it does not support all the above requirements.
- If you have a Microsoft CA, and a suitable **Web Server** template has been issued and enabled in the **Directory Enrollment Policy**, then it is possible to **Request New Certificate** in the **Certificates (Local Computer)** mmc snap-in and use the **Certificate Enrollment wizard**.
- Many organizations have their own process for submitting a Certificate Signing Request (CSR). Please ensure all the above requirements are specified. Security administrators sometimes have difficulty providing a certificate with one or more Subject Alternative Names (SAN), and it helps to explain these are type DNS.

If you have a Microsoft CA then it is simplest to use the Certificate Enrollment wizard available in the mmc certificates snap-in, to request a Web Server certificate and fill in the details.

1.3.4.4 Tachyon server's client authentication certificate

When Content Distribution is installed, any server hosting a Background Channel must have a Client Authentication certificate. This can be the same certificate as a Client authentication certificates if you have 1E Client installed, or it can be the same certificate as the Web Server certificate if your organization security policy allows your Web Server certificates to be used for both **Server Authentication** and **Client Authentication**.

The Background Channel proxy uses this certificate to be authenticated by the Content Distribution Web API, and must be available on the server so that it can be selected on the Tachyon Setup Nomad screen during installation.

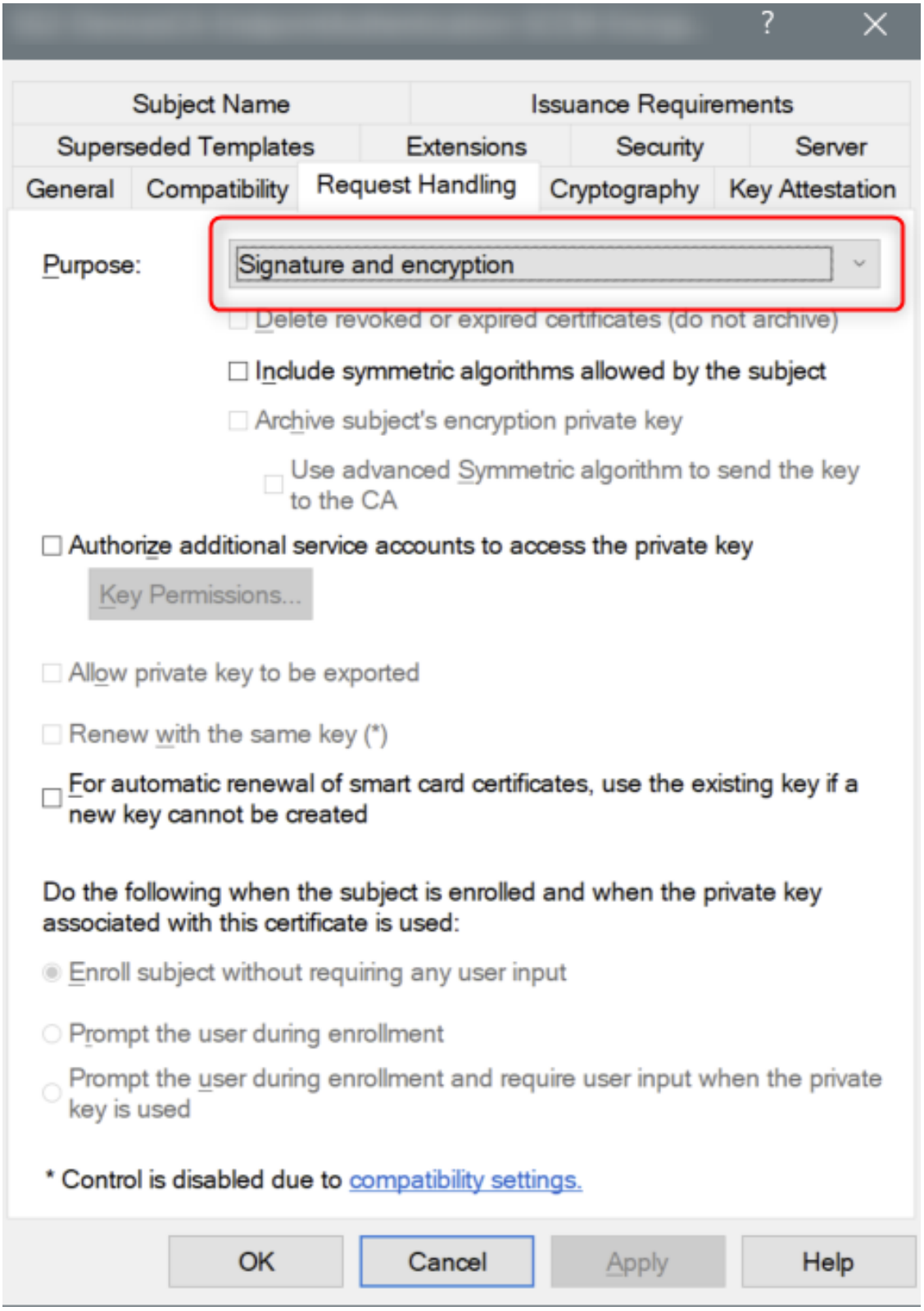
1.3.4.5 Client authentication certificates

Note

You can use Tachyon Setup to install Tachyon so it does not require 1E Clients to present certificates to the Tachyon Switch. Tachyon can be reconfigured later to re-enable use of client certificates when your environment is ready. Each Tachyon server requires a Web Server certificate. Please contact your 1E Account Team if you need help with this.

Note

The 1E Client requires that the client certificate it presents to the platform has both the **Signature** and **Encryption** request handling options. These options are the defaults if provisioning using a Computer Certificate template from a Microsoft Windows Certificate Authority. If you are using a custom template, or an alternative certificate authority, you should confirm that both these options are enabled.



If you have configured Tachyon to require client certificates (Client certificates) then each device requires a certificate with the following properties, so the 1E Client can be authenticated by the Tachyon Switch.

1. Issued by a trusted Certificate Authority (CA):
    - The certificate for the Root CA in the Certification Path must exist in the Trusted Root CA store of the client.
    - If the issuing CA is not the Root CA then the certificate for the issuing CA and any intermediate CA in the Certification Path must exist in the Intermediate CA store of the client.
    - If either of these CA certificates are different to those used by the Tachyon Web Server, they will need to be exported and imported on the TachyonTachyon Web Server.
    - Most organizations have automated distribution of these CA certificates to clients and servers, using Group Policy for example.
2. Has at least the following Enhanced Key Usage:
    - Client Authentication.
3. Has at least the following Key Usage:
    - Digital Signature.
    - Key encipherment.
4. Has a private key:
    - For workgroup and non-Windows devices, the **private key must be exportable**.
5. Revocation information is included:
    - References at least one CRL Distribution point that uses HTTP.
6. Has a Subject Name of type Common Name (**CN=<computername>**) or Subject Alternative Name (**DNS Name=<computername>**) where <computername> depends on the type of device:
    - On domain-joined Windows PCs this must be the **computername FQDN** of the computer, for example **W701.ACME.LOCAL**.
    - On workgroup Windows PCs and non-Windows devices, this must be the computername of the computer - as returned by the **hostname** command, for example on Windows PC this could be **W701**, and on a Mac this could be **MAC01.local**.

Note

Tachyon clients and Switches use OpenSSL and its validation process to verify certificates.

The client device's certificate is stored differently depending on the type of OS:

- For Windows devices, the certificate is stored in the Windows Local Computer personal certificates store.
- For non-Windows devices, except for the Mac, the Tachyon client does not use proprietary certificate stores. Instead, the client requires the certificate exists as a **.pfx** file in the client installation folder structure. For more information, please refer to Client certificates.

- For macOS, you have a choice of storing the client certificate in the macOS Key Store or using the **.pfx** file approach required by other non-Windows devices. Please refer to Client certificates.

If using a Microsoft Enterprise CA then the following should be considered.

- For domain joined Windows computers:
  - Use the Computer template or a duplicate.
  - Enable auto-enrollment - so that devices enroll automatically.
- For workgroup Windows and non-Windows devices:
  - Use a duplicate or equivalent of the Computer or Workstation template.
  - The template's Subject Name uses **supply in the request** - so the hostname can be entered when requesting a certificate.
  - The template must **Allow private key to be exported** - so a certificate can be requested on a domain joined Windows computer, exported as a **.pfx** file and then imported on the target device (see non-Windows Device Certificate).

If using a standalone CA, then certificates must be deployed by other means.

1.3.4.6 Code signing certificates

You will need your own code signing certificate, and have it registered in your Tachyon license, if you want to develop your own custom Tachyon instructions, or modify those of other authors. Instructions that are provided in the Tachyon Platform zip or downloaded from the 1E Exchange have already been code signed using the Platform and 1E Exchange certificates from 1E. Your Tachyon license controls whether you can use these instructions.

Ideally, all of your Tachyon instruction developers should share a single **code signing certificate** between them. Each code signing certificate must be registered in your Tachyon license and associated with your organization's **instruction name prefix**. When you have chosen your prefix and have your code signing certificate(s) you then need to send details of these to 1E, who will update your Tachyon license. This will then automatically activate on your Tachyon server (assuming it has connection to the Internet).

The following applies to the importing and running of custom Tachyon instructions:

- Tachyon platform will only allow instructions to be imported if they have been signed and the code-signing certificate exists in the Tachyon server's Trusted Publishers certificate store.
- Tachyon platform will only allow instructions to be run if their prefix and code-signing certificate have been registered in the Tachyon server's license file (even if the instruction has been successfully imported, it will be flagged as unlicensed if the license information is not there).

Custom Instructions must be signed by TIMS using a code-signing certificate present in the Personal certificate store where TIMS is installed (either local user or machine store). The TIMS user signing the Instruction also needs to have access to the certificate's private key.

For a getting started guide to configuring and verifying your Tachyon system so that you can run customized Tachyon instructions, refer to /document/preview/736871#UUID-66857689-bfb0-8dbc-ae8d-1de40c66fad9.

1.3.4.7 Digital signing certificates

On Windows computers, the installation MSI files, and binary executable and DLL files of 1E software are digitally signed. The 1E code signing certificate uses a timestamping certificate as its countersignature. 1E occasionally changes its code signing certificate, as shown in the table below, and uses it for new releases and hotfixes for older versions, as shown in the table below.

The signature algorithm of the 1E code signing certificate is SHA256RSA. In most cases, the file digest algorithm of an authenticode signature is SHA256, and the countersignature is a RFC3161 compliant timestamp. The exception is on legacy OS (Windows XP, Vista, Server 2003 and Server 2008) which require the file digest algorithm of an authenticode signature to be SHA1, and a legacy countersignature.

The root CA certificates (for signing and countersigning) must exist in the **Third-Party Root Certification Authorities** store (which is replicated in the Trusted Root Certification Authorities store). These root CA certificates are normally automatically provided by Microsoft's Update Root Certificates feature, however, this may not be true for legacy OS computers in a lab environment that are not connected to the Internet.

The table below applies to software and hotfixes released in 2020.

2020	Signing certificate	Timestamping certificates
Certificate	1E Limited	TIMESTAMP-SHA256-2019-10-15 ***and*** DigiCert Timestamp Responder
Issuing CA	**DigiCert EV Code Signing CA (SHA2)** Thumbprint: 60ee3fc53d4bdfd1697ae5beae1cab1c0f3ad4e3	**DigiCert SHA2 Assured ID Timestamping CA** Thumbprint: 3ba63a6e4841355772debef9cdcf4d5af353a297 ***and*** **DigiCert Assured ID CA-1** Thumbprint: 19a09b5a36f4dd99727df783c17a51231a56c117
Root CA	**DigiCert High Assurance EV Root CA** Thumbprint: 5fb7ee0633e259dbad0c4c9ae6d38f1a61c7dc25	**DigiCert Assured ID Root CA** Thumbprint: 0563b8630d62d75abbc8ab1e4bdfb5a899b24d43

1.3.4.8 PKI in the cloud

Tachyon relies on both client (device) and server side certificates to ensure secure communication. In order for these certificates to work the computers need to trust the PKI implementation (issuing

Certification Authority and chain of trust). In a standard on-premises environment, devices can be enrolled with certificates using Directory Group Policy.

It is possible to use a non-Windows based PKI, but it is then left as an exercise for the user as to how to distribute and enrol device certificates to all end-points.

Given the supported Directory configuration above, the PKI requirements described above still apply to a cloud based implementation.

1.3.4.8.1 Tachyon Web Server certificate

Since clients must be able to access the Tachyon Switch and Background Channel from both the internal corporate network and the Internet, there are some additional considerations when creating the Tachyon web server certificate.

1. The server must have a consistent external FQDN.

   In AWS, a standard EC2 instance has an external FQDN based upon its externally accessible IP address. However, this IP address will change each time the server restarts, and since the Tachyon Switch relies on an HTTPS certificate that utilizes the FQDN to authenticate the server, this would cause the Switch to stop working. In order to work around this, any AWS implementation MUST use an Elastic IP address associated with the network interface of the Switch to ensure that the IP address never changes, and therefore the external FQDN is always the same. Alternatively, you can create a CNAME entry in your external DNS to point to the external FQDN of the AWS instance and use the CNAME as the subject name of the server certificate.

2. The web server certificate must incorporate all DNS Names that will be used to access the server in the certificate SAN.

   Clients can be configured to connect to multiple Switches for resilience and geographic load balancing. In many cases a cloud based virtual machine may be able to be accessed through both an internal VPN network, and an external Internet connection. These connections can be made using the same DNS name (via a CNAME entry as specified in the main documentation) or by different DNS names (where there are separate internal and external DNS domains in use).

   The certificate crafted for the Tachyon Switch ***must contain all*** DNS Names that will be used to contact the server in the Subject Alternate Name (SAN) entry within the certificate.

1.3.4.8.2 Client certificates

Any devices that will connect to the Tachyon implementation must have a client certificate from a PKI infrastructure trusted by the Tachyon server. In a Windows domain environment, this is usually provided through an Enterprise Certificate Authority and the use of Group Policy. It is also possible to provide certificates through SCEP, which 1E has tested and support the use of the Microsoft Device Enrollment Service (MDES) for this purpose. Use of other SCEP solutions will be supported on a best-efforts basis.

1.3.5 Directory requirements

Please note the following considerations:

- Tachyon Servers must be domain-joined. The exception is a Tachyon DMZ Server where domain-joined is optional.

- Tachyon is supported in multi-domain, multi-forest environments.
- Each Tachyon user requires an account in Azure Active Directory. Azure Active Directory accounts must have their userPrincipalName (UPN) attribute populated, which is normal but may be missing if user accounts have been created using scripts.
- Users and approvers should have email addresses to support approval workflow and notifications. Email addresses are mandatory if Two-Factor Authentication (2FA) is enabled.
- Azure Active Directory groups are recommended for role-based access control (RBAC) but are not mandatory. Azure Active Directory groups can be assigned to Tachyon roles after installation, they are not required during installation. Groups are not mandatory because users can be assigned to roles and managed within Tachyon instead of Azure Active Directory.
- Tachyon Setup assigns a limited set of permissions to the Setup user account (specified during installation/updates), as described on the Roles page which cannot be edited. It is possible to increase this user account to have Full Administrator access during installation/upgrade, 1E recommends that this user account is viewed as a service account and kept with the minimum permission.
- An Azure Active Directory group is useful to configure access to the CatalogWeb Admin page, as described in Rebuilding the 1E Catalog .

Note

AD *distribution* groups are not supported.

If AD *security* groups are nested (groups within groups), they can slow down the performance of the Tachyon Portal for administrators. Therefore, we recommend nesting is not used, and each administrator and approver account is a member of a group used in Tachyon . You can improve performance further by disabling the recursive search used by Tachyon , bearing in mind this will not support nested groups. Please refer to the Post Installation page.

Domain Local security groups are not supported.

1.3.5.1 Server installation account

This is the account used to run Tachyon Setup (and the MSI installer) when installing or upgrading a Tachyon Server. The account is automatically defined as a Tachyon admin user with limited rights which cannot be edited (called a system principal).

1.3.5.1.1 Local admin rights

The server installation account has the following requirements on the server.

- **Local admin rights on the Tachyon Server**. It must be an Azure Active Directory domain user account that is a direct or indirect member of the Administrators local group on the server where Tachyon Server will be installed.
- Can be disabled (not deleted) in Azure Active Directory after additional admin users have been created in Tachyon, and installation has been verified.

1.3.5.1.2 Tachyon user permissions

The installation account only has sufficient rights to add other Tachyon users, assign them to Tachyon roles, and install Tachyon applications. The users and roles created by the installation account are then used for ongoing use and management of Tachyon.

If you need the installation account to have additional roles or be a **Full Administrator**, then the recommended approach is:

- First create a role-based AD Security group, and add the installation and other accounts to this group
- Then, the installation account:
  - Logs into Tachyon and navigates to Settings→Permissions→Users and Groups
  - Creates a new Tachyon user for the role-based AD Security Group
  - Assigns the relevant system role(s) to the new Tachyon user - this can be Full Administrator.

Tip

You can disable the installation account in AD after the system is operational and other Tachyon users have been set up. You can then re-enable it whenever required for ongoing configuration changes and upgrades.

Note

Do not delete the server installation account from Tachyon after installation.

The server installation account is granted the following permissions as a Tachyon user, configured during installation of the Tachyon Server.

- It is the first Tachyon user account and is a **System Principal**, which means it cannot be deleted or assigned any other rights
- It is assigned to the Tachyon system role of Installer
- It should be used to add additional Tachyon users and administrators, assign them to Tachyon roles, which should then be used for ongoing use and management of Tachyon.
- It may be included in any AD security group assigned to a Tachyon system or custom role.

Refer to Roles and Securables for a complete reference of Tachyon system roles, custom roles, securables and operations.

1.3.5.1.3 SQL Logins for the server installation account

The server installation account requires SQL permissions during installation and upgrade, which can be temporary or permanent. The level of SQL permissions required by the installation account depends on which Tachyon components it is installing.

1.3.5.1.3.1 Master Stacks

For master stacks **sysadmin** is required as follows, to:

- Install **1E Catalog**
- Create Linked Servers for **SLA,** which requires **sysadmin** for the SQL database instances for both SLA and 1E Catalog databases
- Create Linked Servers for **BI**, which requires **sysadmin** for the SQL database instances for both SLA and BI databases, and the SSAS instance for the BI cube (required only by Patch Success).

1.3.5.1.3.2 Response Stacks

<table>
<tr><th>Sysadmin availability on SQL instance(s)</th><th>SQL Login permissions</th></tr>
<tr><td>sysadmin SQL Server role is permitted</td><td>The server installation account requires the sysadmin SQL Server role on the SQL Server instance(s) that host the TachyonMaster and/or TachyonResponses database(s).

This can be used for a new installation, or for an upgrade.</td></tr>
<tr><td>sysadmin SQL Server role is not permitted</td><td>The SQL Login permissions required by the server installation account vary depending on which choice is implemented, as described in the following table:

<table>
<tr><th>Choice implemented</th><th>Role required for the installation account's SQL Login</th></tr>
<tr><td>Database(s) created by the Tachyon Server installer during installation.</td><td>dbcreator SQL Server role on the SQL instance</td></tr>
<tr><td>Database(s) created before installation - a common scenario if you want to select database location and size.

Also required when upgrading Tachyon.</td><td>db_owner database role on the pre-created databases:

• TachyonResponses</td></tr>
</table>

Note
In addition to the permissions given in the table above, the server installation account also needs to ALTER ANY LOGIN Securables permission in order to allow the creation of the Example SQL scripts for creating a SQL Login and granting roles, used by the Tachyon Server web applications and services.

Example scripts are provided below to create a SQL Login and grant roles.</td></tr>
</table>

Sysadmin availability on SQL instance(s)	SQL Login permissions
	During installation, the Tachyon Server installer will **always** attempt to grant **db_owner** permission to the server installation account on each of the Tachyon databases. **Note** Databases must be configured in multi-user mode.

Please refer to Preparation for example SQL scripts.

1.3.5.2 Service accounts

All Tachyon web applications and services use network service account, **NT AUTHORITY\NETWORK SERVICE**, except for the **BI SSAS User** account which must be a domain user account.

The **BI SSAS User** account has the following requirements:

- The account name and its password will be specified in the Tachyon Setup screen.
- Must be a **domain user account**
  - Configured with **Password never expires**
  - Although this user might be referred to as a service account, it does not require **Logon as a service** on the server.
- During installation, the SLA BI installer (used by Tachyon Setup) does the following with the user account:
  - Stores its credentials encrypted in the following places:
    - A linked server connection for the BI database to access the BI cube
    - In the configuration file used by the MDX API to query the BI cube.
  - Creates a SQL Login, with rights on the SLA-BI database.

1.3.5.2.1 SQL Login for the Network Service account

The SQL Login that is used by the Tachyon Server web applications and services depends on whether the SQL Server is remote from the Tachyon Server or is local, as described in the following table:

Installation scenario	Service account SQL Login
Tachyon Server is remote from SQL	The computer account of the remote Tachyon Server. For example **ACME\ACME-TCN01$**
Tachyon Server and SQL are local	The local network service account, **NT AUTHORITY\NETWORK SERVICE**

Note

Before upgrading Tachyon, or installing or upgrading Consumer applications like Application Migration or AppClarity, the SQL Login must be granted the following rights to support Database Snapshot of the 1E Catalog and SLA databases, to restore them if an error occurs:

- **dbcreator** rights on the SQL database instance hosting the 1E Catalog database.
- **dbcreator** rights on the SQL database instance hosting the SLA databases.

During installation, the Tachyon Setup will **always**:

- Attempt to create the SQL Login
- Grant it **db_owner** permission on each of the Tachyon databases
- Remove the **db_owner** permissions when installation is completed.

1.3.5.3 User accounts

Please note the following:

- Each Tachyon user requires an account in Azure Active Directory. AAD accounts must have their userPrincipalName (UPN) attribute populated, which is normal, but may be missing if users accounts have been created using scripts.
- Tachyon users and approvers should have email addresses to support approval workflow and notifications. Email addresses are mandatory if Two-factor Authentication is enabled.
- Users are added to the Tachyon system and assigned roles by any Tachyon user assigned to the **Full Administrator** system role. A Full administrator manages Tachyon users and roles using the Permissions Menu in the Tachyon Portal Settings application.
- Tachyon is supported in multi-domain, multi-forest environments. You have a choice of how Tachyon queries Azure Active Directory, specified during installation.
- Tachyon services locate users and computers and membership of security groups by querying a semi-colon delimited list of Azure Active Directory GC and/or LDAP URLs.

GC URL	This is the quickest and simplest method of resolving users and group membership. A single GC URL will normally resolve all users and groups within a single **forest**.

	Supports only Universal security groups.
LDAP URL	A single LDAP URL will normally resolve all users and groups within a single **domain**. Supports Universal and Global security groups. Required if a Global Catalog (GC) server does not exist in a trusted forest, or if Global security groups must be used.

Any domain which contains Tachyon servers, users or groups must:

- Be resolvable from the Tachyon Server using DNS - that is, the server must be able to resolve domain names using DNS
- Have a two-way trust with the domain in which the Tachyon (Master Stack) Server exists - so that users trust the server, and the server trusts users
- Allow the Tachyon Server to read computer, user and security group objects in each domain.

The default **GC://** is sufficient for a Tachyon Server in a simple Active Directory environment of one forest which has a Global Catalog. You can include, but it is not required, the name of the server's local domain or root domain, for example: **GC://acme.local**

To add support for a remote forest which has its own GC, you would for example have **GC://acme.local;GC://nadir.local** and so forth adding the root domain of any other forests to the list of GC URLs.

If you prefer to use LDAP, or there are difficulties with trusts between forest domains, then you would create a list of LDAP URLs including *all* domains that have Tachyon users and groups, as well as domains in which a Tachyon server resides. For example:

LDAP://acme.local;LDAP://pop.acme.local;LDAP://rock.acme.local;LDAP://country.acme.local;LDAP://nadir.local;LDAP://disco.nadir.local

You can mix GC and LDAP URLs, but you should avoid mixing LDAP URLs that are also resolved by a GC URL. For example: **GC://;LDAP://nadir.local;LDAP://disco.nadir.local**

1.3.5.3.1 Active Directory Security Groups

Active Directory security groups are strongly recommended for role-based access control (RBAC) but are not mandatory. AD security groups can be assigned to Tachyon roles after installation, they are not required during installation. They are added as Tachyon users and configured in the same way as AD user accounts. A Tachyon user can therefore be a domain user account or a security group. Groups are not mandatory because users can be assigned to roles and managed within Tachyon instead of AD, or a combination.

Tachyon Setup assigns a limited set of permissions to the server installation account, as described in Tachyon user permissions, which cannot be edited. However, the installation account's permissions can be extended if the account is a member of one or more AD Groups configured as Tachyon users.

An AD security group is also useful to configure access to the CatalogWeb Admin page, as described in Rebuilding the 1E Catalog.

Note

AD *distribution* groups are not supported.

If AD *security* groups are nested (groups within groups), they can slow down the performance of the Tachyon Portal for administrators. Therefore, we recommend nesting is not used, and each administrator and approver account is a member of a group used in Tachyon . You can improve performance further by disabling the recursive search used by Tachyon , bearing in mind this will not support nested groups. Please refer to the Post Installation page.

Domain Local security groups are not supported.

Tachyon sends emails to users and approvers of Tachyon instructions, which requires user AD accounts to be email-enabled. However, Tachyon allows you to permission instruction sets with AD users or groups, roles that Permissions are assigned to instruction sets, and AD security groups can be assigned permissions. Tachyon will use the email address of an AD security group if it has been configured, and relies on the Mail system to forward emails to the members of the AD security group. If the AD security group is not configured with an email address, then Tachyon sends an email to each member that has an email address. AD distribution groups are not supported.

1.3.5.4 Active Directory in the cloud

The Tachyon software must be installed on a Windows Server that is part of an Active Directory domain. Companies do not always have their on-premises Active Directory extended into their cloud environment - there are security concerns that must be taken into account and there must be some mechanism for either a secure network connection between the customer's on-premises systems and the cloud environment (usually via VPN connection) or a way of synchronizing the cloud based Active Directory implementation with the on-premises one (through a directory synchronization of some sort).

Both AWS and Azure provide the following 'cloud' based versions of Active Directory:

1. **AWS Directory Service for Microsoft Active Directory (Enterprise Edition)** - This is a full implementation of Active Directory, but it requires a VPN and a trust relationship set up with any existing on-premises Active Directory to be able to use on-premises based accounts. This makes it quite a complex solution to implement and maintain.

   Note

   1E have not yet tested any Tachyon platform implementation using this solution, and as such it is only supported by 1E on a best-efforts basis.

   Also known as AWS Managed Microsoft Active Directory (AD).

2. **AWS AD Connector** - This is a mechanism for redirecting domain queries from the local network to an on-premises Domain Controller using a VPN instead of needing a domain controller in the cloud.

   Note

   1E have not yet tested any Tachyon platform implementation using this solution, and as such it is only supported by 1E on a best-efforts basis.

3. **AWS Simple AD** - This is an implementation of Active Directory based upon Samba 4 and provides a limited subset of a full Active Directory.

   Warning

   1E do not support the Tachyon platform running in this environment.

4. **Azure Active Directory** - Although this provides cloud based identity, it cannot be used for direct directory connectivity from an Azure virtual machine, for that you need Azure Active Directory Services (see next).

5. **Azure Active Directory Services** - This provides the ability to domain join Azure Virtual Machines to your Azure Active Directory, however, it is not a full AD as you cannot have domain admin or enterprise admin privileges.

   Warning

   1E do not support the Tachyon platform running in this environment.

The following is the only cloud solution that is fully supported by 1E, and is what we call **Extended AD**. It doesn't use any of the above, but has the following requirements, which provide an Active Directory presence in the cloud and brings the full capabilities of Active Directory to bear.

- Virtual machines located in the customer's cloud network installed with Windows Server as hosts for:
  - Domain Controller(s) in the existing enterprise domain, which can be Read-Only domain controllers (RODC).
  - Other member server(s) which host the Tachyon Server components, including Microsoft SQL Server, must be joined to the same enterprise domain.
- A permanent site-to-site VPN connection from cloud to the corporate on-premises network.

Note

1E fully support the **Extended AD** solution for AWS and Azure, which do not change any of the Active Directory requirements described above.

1.3.6 Email and 2FA requirements

You will need to decide if you want to use the Email and two-factor authentication features.

1.3.6.1 SMTP server

The Tachyon SMTP feature can optionally be enabled to send the following types of emails to Tachyon users.

- Approval request emails to approvers about pending action requests
- Notification emails to users about responses that will expire shortly
- One-time authentication code emails if the two-factor authentication feature is enabled.

Emails are HTML format, without any attachments, and have a typical size of approximately 70KBytes. You can choose to modify the email banner header.

Emails are sent by the Coordinator service (workflow module) which by default uses the built-in Network Service (NT AUTHORITY\NETWORK SERVICE).

If the Tachyon SMTP feature is enabled, your SMTP relay/gateway may require the following to be configured.

- Add the Tachyon Server name or IP address to a new or existing white-list policy
- Disable require SMTP authentication (allow anonymous) - see note below
- Assign the "mail-from" address to an AD account - see Mail-From address below - if it has a **SPF (Sender Policy Framework)** or **Sender ID** policy.

Note

In this version of Tachyon, **SMTP Authentication** is not configurable using the Server installer. The default is anonymous authentication. However, it can be changed post-installation. For details of changing the SMTP configuration and disabling email notifications, please refer to Tachyon Server post-installation tasks.

1.3.6.2 Mail-From address

If the Tachyon SMTP feature is enabled, then a Mail-From address is required as the Sender of Tachyon emails.

Tachyon does not require the Mail-From address to belong to a real AD account or have a real mailbox, however, your SMTP relay/gateway might have these requirements, therefore you may need to create an additional AD account.

Choose a suitable email address, especially if there is no mailbox, for example no_reply@acme.local.

1.3.6.3 Email for Users and Approvers

Each Tachyon user and approver should have an email address, otherwise they will not receive emails when actions require authentication or approval. Email addresses are mandatory if two-factor authentication is enabled.

If a Group is assigned rights in Tachyon to approve actions, and the Group has an email address, then Tachyon will use that. However, a group member will receive emails only if your organization's mail system supports group emails and the member has an email address. If the Group does not have an email address, then Tachyon will look up group members and send emails to any member that has an email address. Irrespective of whether the Group has an email address, members must have emails addresses in order to receive emails.

Note

If your organization uses separate accounts for user and administration tasks, then you should consider the impact of using admin accounts for Tachyon if they do not have associated email addresses.

1.3.6.4 Two-factor Authentication requirements

If the 2FA feature is enabled, Tachyon users are prompted to enter a one-time authentication code in addition to their password in order to confirm they want to submit an **action** instruction.

The one-time authentication code is sent to the user by email. The two-factor authentication feature requires email.

Please refer to Tachyon Server post-installation tasks.

1.3.7 Product integration requirements

An overview of how Tachyon connects to third-party systems, and how it integrates with its companion 1E products.

More detailed information about how to configure Tachyon is provided in Using Settings.

1.3.7.1 1E companion products

The following tables show the 1E products that combine to support particular features.

Supported versions of 1E companion products with features that depend on Tachyon 8.1.

(For products that depend on the 1E Client, please refer to urn:resource:component:647597)

Products and features that depend on Tachyon platform	Supported versions of companion products	
AppClarity	AppClarity is a consumer application of the Tachyon platform and requires a full Tachyon infrastructure.	• AppClarity 8.1
Application Migration	Application Migration is a consumer application of the Tachyon platform and requires a full Tachyon infrastructure.	• Application Migration 8.1
Guaranteed State	Guaranteed State is a consumer application of the Tachyon platform and requires a full Tachyon infrastructure.	• Guaranteed State 8.1
NightWatchman	Console live status of NightWatchman clients is an optional feature of NightWatchman and requires a full Tachyon infrastructure. NightWatchman is not a Tachyon platform application and requires its own server(s).	• NightWatchman Enterprise 7.3

Products and features that depend on Tachyon platform	Supported versions of companion products	
Nomad	Nomad is a consumer application of the Tachyon platform and requires a full Tachyon infrastructure. It includes the Content Distribution feature that replaces the legacy ActiveEfficiency Server and its features.	• Nomad 8.1 (app) and Nomad 8.1 (tools)
Patch Success	Patch Success is a consumer application of the Tachyon platform and requires a full Tachyon infrastructure. It also requires 1E SLA Platform Business Intelligence to be installed and a SQL Server Analysis Server (SSAS) instance.	• Patch Success 8.1
Shopping	Shopping uses Tachyon platform and 1E Client for its client-side order notifications, and to allow end-users to shop for Tachyon instructions. Shopping is not a Tachyon platform application, and requires its own server(s).	• Shopping 6.1
Experience	Experience is a consumer application of the Tachyon platform and requires a full Tachyon infrastructure.	• Experience 8.1
Explorer	Explorer is a consumer application of the Tachyon platform and requires a full Tachyon infrastructure.	• Explorer 8.1

Note

In addition to the consumer applications listed above, Tachyon Setup is also used to install the Inventory and Settings applications.

Supported versions of 1E companion products that Tachyon 8.1 platform features depend on.

Products and features that Tachyon platform depends on	Supported versions of companion products	

1E Client	Tachyon requires the 1E Client to be installed on all client computers.
	
	Client features:
	
	• Real-time response to instructions, which supports the retrieval of information using questions, and running actions
	• Tags (freeform and device/coverage)
	• Criticality and Location
	• 1E Client UI to support the Real-Time Control Center, Announcements, Surveys, and Sentiment features of Experience #
	• Inventory, including process usage, to support the:
	  – Tachyon Activity Record feature
	  – Inventory and other consumer applications.
	• Performance metrics features to support the Experience application #
	• Policy feature to support consumer applications: Guaranteed State ##, Experience #, and Nomad #
	• Modules to support:
	  – Patch Success #
	  – Command and script execution
	  – Content distribution
	  – Device criticality
	  – Manipulation of files and processes
		• 1E Client 8.1
		• 1E Client 8.0
		• 1E Client 5.2
		• 1E Client 5.1

Products and features that Tachyon platform depends on	Supported versions of companion products	
	– Manipulation of registry and WMI # – Security # – Software uninstallation – User sessions, including Primary User. # not supported on non-Windows, ## partially supported on non-Windows Platform clients can optionally use the Nomad client module of 1E Client to more efficiently download content.	
Nomad	Clients can optionally use Nomad (1E Client with Nomad client features enabled) to provide more efficient downloading of content.	• 1E Client 8.1 (with Nomad enabled) • 1E Client 8.0 (with Nomad enabled) • 1E Client 5.2 (with Nomad enabled) • 1E Client 5.1 (with Nomad enabled).

1.3.7.2 Connectors

Connectors are used to connect to other 1E and third party systems, retrieve their data and populate repositories. Tachyon provides the following inventory connectors to populate the Inventory repositories, for details refer to Repositories page:

- BigFix connector — Connects to a BigFix Inventory database server.
- BigFixInv connector — Connects to a BigFix Inventory database.

- File Upload connector — Uploads inventory data from a folder containing tab (TSV) and comma (CSV) separated value file(s).
- Intune connector — Connects to an Intune application and collects inventory and usage data.
- Microsoft Office 365 connector — Connects to an Office 365 application in InTune and pulls in inventory and usage data.
- OpenLM connector — Connects to an OpenLM database server.
- Oracle LMS connector — Connects to Oracle LMS and queries it for inventory information.
- ServiceNow connector — Connects to a ServiceNow instance to import basic inventory data into SLA Platform.
- System Center Configuration Manager connector — Connects to a Configuration Manager database and pulls in inventory and usage data.
- Tachyon connector — Connects the Tachyon and SLA components to support Management group and Tachyon Powered Inventory features. The Tachyon Powered Inventory feature uses instructions to fetch inventory data from clients, and is a prerequisite for 1E Patch Success.
- vCenter connector — Connects to a vCenter server and pulls in inventory data.
- Windows Server Update Services connector — Connects to a WSUS database and pulls in patch data.

Use the links above to find more information about each type of connector. Please refer to Introducing Inventory for more information about viewing and exporting inventory repositories.

Additional connectors may exist for add-on Consumer applications that have been installed. For example, Connectors page has the following connectors to populate its entitlement repository:

- AppClarity v5.2 connector — Exports entitlements from an AppClarity 5.2 database into a TSV file, which can then be reviewed and imported into.
- Entitlement .tsv connector — Uploads entitlements from a folder containing one or more tab or comma-separated value file(s).

Please refer to the relevant connector page to identify security and other requirements for a specific connector.

Patch Success needs to get meta-data for patches. Ensure you add a connector for whichever one of the following sources that you use to approve patches:

- Configuration Manager (SCCM) if it is configured to manage WSUS
- Windows Server Update Services (WSUS).

If you are using Configuration Manager then you must add a System Center Configuration Manager connector.

If you are using WSUS then you must add a Windows Server Update Services connector.

Patch Success also requires a Tachyon connector.

The following table shows the supported versions of software used by the Tachyon out-of-box connectors.

Connector	Product	Notes
BigFix	• BigFix	Please refer to the BigFix connector for prerequisites.
Intune	• Intune	Please refer to the Intune connector page for prerequisites.
Microsoft Office 365	• Azure	Please refer to the Microsoft Office 365 connector page for prerequisites.
OpenLM	• OpenLM Server version 21.12	Please refer to the OpenLM connector page for prerequisites.
Oracle LMS	• Oracle LMS	Please refer to the Oracle LMS connector page for prerequisites.
ServiceNow	• ServiceNow Jakarta release	Please refer to the ServiceNow connector page for prerequisites.
System Center Configuration Manager (SCCM)	• SCCM CB 2203 • SCCM CB 2111 • SCCM	Please refer to the System Center Configuration Manager connector page for prerequisites.

Connector	Product	Notes
	CB 2107 • SCCM CB 2103 • SCCM CB 2010	
Tachyon	• Tachyon 8.1	Please refer to the Tachyon connector page for prerequisites.
vCenter	• VMware PowerCLI 11.1.0	VMware PowerCLI 11.1.0 (code.vmware.com/web/dp/tool/vmware-powercli/11.1.0) must be installed on the Tachyon Master server (where the SLA Integrate Services Agent service is hosted) before you can configure and use the vCenter connector. Earlier or later versions of PowerCLI are not supported and may cause errors. VMware PowerCLI is freeware and was previously known as vSphere PowerCLI. VMware PowerCLI supports multiple versions of VMware vCenter Server. For details, please refer to the VMware compatibility matrix using the following link: https://www.vmware.com/resources/compatibility/sim/interop_matrix.php#interop&2=&106= Please refer to the vCenter connector page for configuration details.
WSUS (Windows Server Update Services)	• WSUS	Please refer to the Windows Server Update Services connector page for configuration details.

1.3.7.3 Product Pack and Security Roles

Classic Product Packs:

- Include instructions
- Are uploaded using either of the following methods:
  - Tachyon Product Pack Deployment Tool as described in Tachyon Product Pack Deployment Tool
  - **Upload** button on the **Settings - Instructions sets** page, as described in Instruction sets page
- Once the instructions are uploaded you must organize them manually into Instruction Sets, although the Tool will use the name of the zip file as the basis for the Instruction set name
- Instruction Sets are the basis for assigning custom roles that determine who can do what with the instructions in each Set.

Integrated Product Packs:

- Include policies and/or instructions
- Are uploaded using the Tachyon Product Pack Deployment Tool as described in Uploading Integrated Product Packs
- If the pack contains instructions, each one is automatically uploaded into an Instruction Set using the folder name as the basis for the Instruction set name
- Policies are uploaded into Guaranteed State.

The Integrated Product Packs provided by 1E include ready-made Policies, and any instructions included in the packs are intended to augment the policies, but can be used independently.

You may want to create AD security groups to use custom roles to control access to:

- **Instructions Sets** - you should think about groups of people who will need to view, question, action, and approve instructions
- **Policies** - you must decide who needs access to Guaranteed State - in this version, you cannot grant access to individual Policies.

1.3.7.4 Nomad integration

Nomad integration is available on Windows PC devices and is enabled by default (NomadContentDownloadEnabled=true), and can be disabled during or after installation of the 1E Client.

With the integration feature enabled, Tachyon will detect if the Nomad client module of the 1E Client is enabled, or if Nomad v6.0.100 or later version is running on the device. Nomad then automatically downloads content from Tachyon Background Channel servers, and any other HTTP/S content source that the client may use.

Tachyon use of Nomad works irrespective of whether Nomad is integrated with Configuration Manager or using advanced Nomad features that use ContentDistribution.

Configuration Manager is not a prerequisite for Nomad integration with Tachyon, but you will need to consider the following:

1.3.7.4.1 Configuration Manager present

You do not need to make any configuration changes to Nomad for it to integrate with Tachyon. Please refer Introducing Nomad for guidance on designing and deploying Nomad.

1.3.7.4.2 Configuration Manager not present

You can deploy Nomad to Windows devices where the Configuration Manager client is not present. You will need to enable the following bits in relevant installer properties:

- CompatibilityFlags bit 1 - enable long hashes
- SpecialNetShare bit 13 - enable HTTP(S)

These are enabled by default in the Nomad client module of the 1E Client.

1.3.7.5 Configuration Manager integration

Tachyon is able to integrate into the Configuration Manager console to provide a right-click context menu that can be invoked from Configuration Manager computer collections. Tachyon can then use the members of the computer collections as the coverage for any instruction selected from the menu. The Configuration Manager extensions are part of the 1E PowerShell Toolkit. For more details, please refer to Preparing for the Tachyon extensions for the Configuration Manager Console..

1.3.8 Network requirements

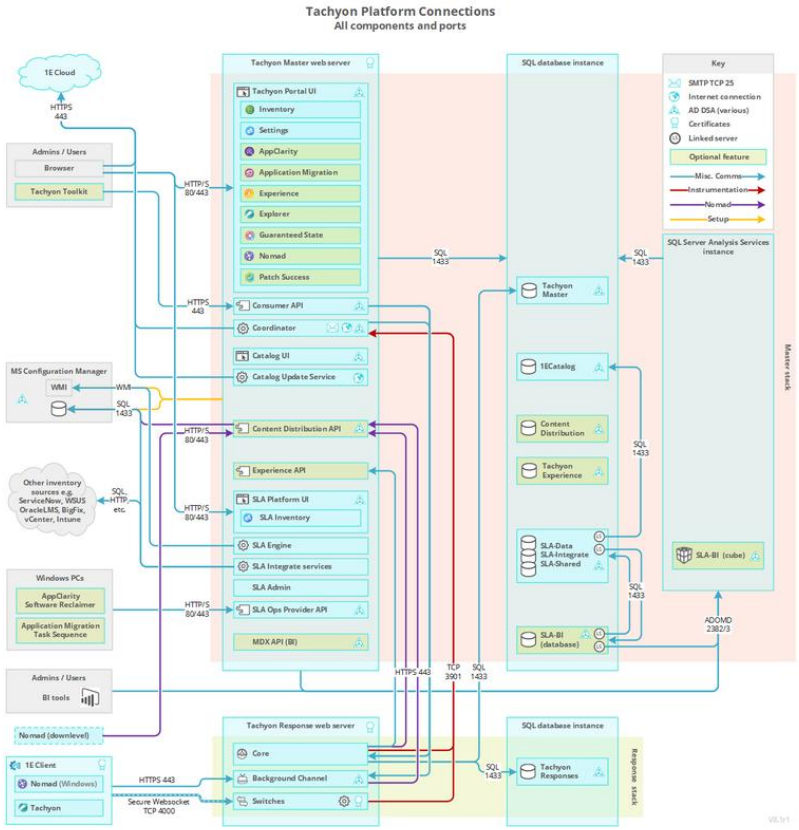
The correct choice of DNS Names for your Tachyon Servers is perhaps the most fundamental decision you will make.

You must ensure the firewalls on your client, servers, and network are configured correctly, and your Internet connections to the 1E Cloud are whitelisted.

For a remote SQL Server, please refer to Configuring a persistent route for SQL traffic. However, please ensure you also consult your server, firewall and networking teams.

1.3.8.1 Firewall Ports

The following are extracts from the Communication Ports reference page.



The following table lists firewall requirements for a **single-server** where **Tachyon Master Stack** and **Response Stack** are installed on the same server. The table assumes a remote SQL Server hosting TachyonMaster and TachyonResponses databases. Each Tachyon component described in the table has at least one output and/or input. For each Tachyon component with an output, there is a matching input.

Firewalls normally protect against incoming traffic from remote devices, however, the table below also includes outgoing connections. The table does not include internal communications within the Server.

In addition to but not included in the table are various ports that Tachyon uses to communicate with Microsoft services, including Certificate Services and Active Directory. The Coordinator **Workflow service** queries AD for email details; the **Consumer API** queries AD for security details.

Port requirements are not provided here for the Content Distribution, Shopping, and WakeUp modules of the **1E Client**. Only the ports used by the 1E Client feature of the **1E Client** are listed.

If the 1E Nomad module is being used by the 1E Client on Windows computers, it has additional port requirements of its own, which are not changed by Tachyon.

Additional ports may be required if Tachyon instructions need to connect to non-Tachyon content sources.

Additional requirements may exist if the environment has changed default security settings.

1.3.8.2 Tachyon Servers

Device	Port	Protocol	Direction	Usage	Configurable
Tachyon Server (Master Stack)	TCP 443	HTTPS	Incoming	• Console browser connections to **Tachyon Portal UI** • Console browser connections to **SLA Platform UI** • Console browser connections to **1E Catalog UI** • Consumer connections to**Catalog API**	Yes, during installation. In the **Website Configuration** panel in Tachyon Setup. See #UUID44187c3f8a182c06d4353770a23bb3e4_id_TachyonServerinstallerpropertiesHTTPSIISPORTHTTPSIISPORT. Setup installs other components using the same settings as Tachyon Server.

Device	Port	Protocol	Direction	Usage	Configurable
				• Consumer connections to **Consumer API** • Consumer connections to **SLA Operations Provider API**	
Tachyon Server (Master Stack)	TCP 80	HTTP	Incoming	• Console browser connections to **SLA Platform UI** • Console browser connections to **1E Catalog UI**	Yes, during installation. In the **Website Configuration** panel in Tachyon Setup. See #UUID44187c3f8a182c06d4353770a23bb3e4_id_TachyonServerinstallerpropertiesHTTPSIISPORTHTTPSIISPORT. Tachyon Setup installs other components using the same settings as Tachyon Server.

Device	Port	Protocol	Direction	Usage	Configurable
				• Consumer connections to **Catalog API**	
				• Consumer connections to **SLA Operations Provider API**	
Tachyon Server (Response Stack)	TCP 443	HTTPS	Incoming	• Client retrieving content from the **Background Channel**.	Yes, during installation. In the **Website Configuration** panel in Tachyon Setup. See #UUID44187c3f8a182c06d4353770a23bb3e4_id_TachyonServerinstallerpropertiesHTTPSIISPORTHTTPSIISPORT.
Tachyon Server (Master Stack)	TCP 443	HTTPS	Outgoing	• Tachyon **Coordinator service** contacting the **1E Cloud License Se**	The port used to connect to the **1E Cloud Services** is not configurable.

Device	Port	Protocol	Direction	Usage	Configurable
				rvice via an Internet connection. • **1E Catalog Update service** contacting the **1E Cloud Catalog Service** via an Internet connection.	
Tachyon Server (Master Stack)	TCP 6002	WebSocket (ws)	Incoming Outgoing	• **Integrate Agent** service connecting to the **Integrate Manager Web API** to get connector jobs	Yes, configurable after installation. **Note** **Integrate Agent** component is not shown on the diagram, and installation on remote systems is not supported.

Device	Port	Protocol	Direction	Usage	Configurable
Tachyon Server (Response Stack)	TCP 4000	WebSocketSecure (wss)	Incoming	• Client receiving instructions from and sending compressed responses to the Tachyon Switch.	Switch ports are not configurable using the Server installer. A Switch port can be changed post-installation, by configuring the value in the **Port** column for the relevant Switch in the **SwitchConfiguration** table in the Tachyon Master database. If the Switch port is changed after deploying 1E Client (with Tachyon features enabled) then the corresponding Switch port must be updated in each Client's configuration file. Clients initiate and maintain a WebSocket Secure connection to a Switch, which the Switch uses to communicate back to the clients.
Tachyon Server (Master Stack)	TCP 25	SMTP	Outgoing	• Tachyon **Coordinator service** sending two-factor authentication emails. • Tachyon **Coordinator service** sending workfl	Yes. In this version of Tachyon, **SMTP Authentication** is not configurable using the Server installer. The default is anonymous authentication. However, it can be changed post-installation. For details of changing the SMTP configuration and disabling email notifications, please refer to Changing the SMTP Host configuration.

Device	Port	Protocol	Direction	Usage	Configurable
				ow emails.	
Tachyon Server (Master Stack)	TCP 1433	TDS	Outgoing	• Tachyon Web Site application pools (**Portal**, **Consumer API**) communicating with SQL Server. • SLA Platform Web Site application pools (**Admin**, **CoreExternal**, **Platform**) communicating with SQL Server.	Not configurable from Setup. In the **Database Servers** panel in Tachyon Setup you can select a SQL Server instance. The instance can be installed using a non-standard port. However, selecting an instance that uses a non-standard port will not change the port used by the Tachyon Installer, and installation will fail. If you require the use of a non-standard port on a Default SQL Server instance, contact 1E for guidance on a manual workaround. If using a Named Instance that is set to its default configuration where the server automatically chooses a random port (or if you manually configured the instance to use a fixed port), then the **SQL Browser** service needs to be enabled to let the Tachyon Server determine the port in use. You will need to open UDP port 1434 used by the SQL Browser. See #UUID44187c3f8a182c06d4353770a23bb3e4_id_TachyonServerinstallerpropertiesSQLSERVER_MASTERSQLSERVER_MASTER.

Device	Port	Protocol	Direction	Usage	Configurable
				• Tachyon **Coordinator service** communicating with SQL Server. • Catalog services and application pool communicating with SQL Server. • **1E Catalog Update service** communicating with SQL Server.	

Device	Port	Protocol	Direction	Usage	Configurable
Tachyon Server (Master Stack)	TCP 1433	TDS	Outgoing	• Inventory connectors fetching data from sources that use SQL Server.	Configurable in various Connectors, please refer to Connectors page.
Tachyon Server (Master Stack)	TCP 135 and 445 (initially)	WMI (DCOM)	Outgoing	• SCCM WMI Server provider connection to Configuration Manager. • Nomad connection to Configuration Manager used by the Nomad Sync	Not configurable. Please refer to Provider configuration page and Nomad.

Device	Port	Protocol	Direction	Usage	Configurable
				feature.	
Tachyon Server (Response Stack)	TCP 1433	TDS	Outgoing	• Tachyon Web Site application pools (**Core** and **Core Internal**) communicating with SQL Server (mainly uncompressed responses).	Not configurable from Setup. See the comments above for the Tachyon Server (Master Stack). See #UUID44187c3f8a182c06d4353770a23bb3e4_id_TachyonServerinstallerpropertiesSQLSERVER_RESPONSESSQLSERVER_RESPONSES.
SQL Server (TachyonMaster database)	TCP 1433	TDS	Incoming	• Tachyon Web Site application pools (**Consumer API**, **Portal**) communicating	Not configurable from Setup. See the comments above for the Tachyon Server (Master Stack). See #UUID44187c3f8a182c06d4353770a23bb3e4_id_TachyonServerinstallerpropertiesSQLSERVER_MASTERSQLSERVER_MASTER.

Device	Port	Protocol	Direction	Usage	Configurable
				with SQL Server. • Tachyon **Coordinator service** communicating with SQL Server. • Tachyon Web Site application pools (**Core**) communicating with SQL Server.	
SQL Server (TachyonResponses database)	TCP 1433	TDS	Incoming	• Tachyon Web Site application pools (**Core** and **Core Internal**)	Not configurable from Setup. See the comments above for the Tachyon Server (Master Stack). See #UUID44187c3f8a182c06d4353770a23bb3e4_id_TachyonServerinstallerpropertiesSQLSERVER_RESPONSESSQLSERVER_RESPONSES.

Device	Port	Protocol	Direction	Usage	Configurable
				communicating with SQL Server (mainly uncompressed responses).	

1.3.8.3 Whitelisting connections to 1E Cloud

The simplest method is to whitelist ***.1e.com**

The following sections briefly describe Tachyon features which connect to the 1E Cloud.

For guidance on whitelisting and configuring Internet Explorer proxy settings, please refer to Preparation.

1.3.8.3.1 1E license service URL

Ensure the following URL is whitelisted:

- https://license-v1.1e.com

This URL must be accessible from the Tachyon server during setup and running of Tachyon.

The Tachyon license must be validated on a regular basis via internet contact with the 1E license service. The regular validation period is set when the license is requested.

For whitelisting purposes, the Tachyon server (specifically the Coordinator Workflow module in the Master Stack) requires an Internet connection to the 1E license service, as defined in the license file itself. If activation fails, then the system will install but not be usable until activation is completed.

Upgrading

When upgrading, you are recommended to get a new license file and update your whitelist with the new URL. The old URL (https://license.1e.com) is suitable only for 8.0 and earlier. However, if you are upgrading and your license file has the old URL then you should also whitelist the old URL.

Tachyon setup will report a warning in the Tachyon Setup screen if it is unable to connect to the 1E license service. This is important only on the Tachyon Master Stack Server, not on other types of Tachyon server. You can test the connection using Tachyon setup or using Internet Explorer.

> **Tip**
>
> If you are whitelisting an IP address and your server has multiple network interfaces, then you can configure a persistent route using a similar process described in Configuring a persistent route for SQL traffic.

Your Tachyon server may not be able to connect to the 1E license service if your environment is using web proxy servers. Contact your 1E Account Team for advice in case you have this type of setup.

1.3.8.3.2 1E Catalog service URL

Ensure the following URL is whitelisted:

- https://catalog.1e.com

This URL must be accessible from the Tachyon Server during setup and running of 1E Catalog. This enables the Catalog Update service to connect to the 1E Cloud Catalog and download the latest catalog entries.

> **Note**
>
> 1E Catalog may need additional configuration to support proxy servers, but this depends on the configuration you have in your current environment. Please contact 1E Support if you need help doing this.

1.3.8.3.3 1E Analytics URL

Ensure the following URL are whitelisted for clients and Tachyon servers:

- https://analytics.1e.com
- https://data.analytics.1e.com
- https://content.analytics.1e.com
- https://_460897a4cf2c02443c6af6aed8761f7b.content.analytics.1e.com

Or simply ***.analytics.1e.com** or ***.1e.com**

User Interface telemetry reports how the user interface is used, and data is sent directly from administrator browsers to the 1E Cloud.

Telemetry features are configurable using Tachyon Setup during installation or upgrade, and can be enabled or disabled as a post-installation task. 1E encourages customers to enable sending telemetry.

For more information, please refer to Telemetry.

1.3.8.4 Network interfaces

The following conditions apply to network interfaces, which must be configured before installing Tachyon on a server. Each network interface must be assigned a static IP Address.

Switches	Each Switch supports up to 50,000 devices and requires its own network interface, with a minimum speed of 1Gbps. Switch interfaces can be on the same or different subnets. Each interface can have its own DNS Name or share the same DNS Name as explained in DNS Names below. If necessary, these interfaces can be shared with a Background Channel or other Tachyon services, which may share the same DNS Name or have their own names.
Response Stack with a Core component using a remote SQL Server instance and more than 500 devices	In addition to the Switch interfaces, another interface is required for outgoing response traffic from the Response Stack Core to its remote SQL Server. This should have a minimum speed of 1Gbps, or 10Gbps if the Response Stack has 3 or more Switches. This is required to ensure optimum performance when SQL Server is remote. Network routing on the Response Stack server must be configured so that SQL traffic is routed over this interface. The simplest method is to route all outgoing traffic. The interface used for SQL traffic should not register its IP Address in DNS to avoid unnecessary incoming traffic and accidentally becoming part of a round-robin DNS Name used for Switches.
DMZ Server	An additional internal facing interface is required for outgoing response traffic from Switches on the DMZ Server to the Core on the internal Tachyon Response Stack. This should have a minimum speed of 1Gbps. As stated above, each Switch must have it own external facing interface, used for incoming response traffic from clients to Switches. The external facing interface(s) can also be used for clients to the Background Channel. The simplest way to ensure the internal interface is used for outgoing traffic is for it to be on a different subnet to the external interface(s) with no routing between them - this is normal in a DMZ.

Administration traffic for a Tachyon Master Stack does not have any additional network requirements.

> **Tip**
>
> Tachyon Setup supports installation using IPv4. If you have a working IPv6 environment, then please contact 1E for advice on using that.

For the remote SQL Server requirement, please refer to Configuring a persistent route for SQL traffic. However, please ensure you also consult your server, firewall and networking teams.

1.3.8.4.1 Network impact

Most of the network traffic experienced by a Tachyon system is compressed responses from clients to Switches. Responses to Tachyon instructions are returned by online clients in a matter of a few seconds. Tachyon is designed for speed without impacting your network.

The Response Stack's Core then processes and stores uncompressed responses in the Tachyon Responses database. If the database is remote then this will create significant network traffic when saving responses, but normally this will be within a datacenter. Even so, a dedicated interface is recommended on each Response Stack for connection to a remote SQL Server in order to prevent network contention between incoming and outgoing response traffic.

Other network traffic generated by Tachyon is low by comparison. Explorer is a single page application which uses paging to view responses.

Tachyon clients also download content from a Background Channel, which is a website hosted on the same server as Switches. They deliberately stagger the delay of their download for up to 5 minutes (configurable). By using Nomad, you can avoid the staggered delay on Windows PCs without impacting your network. For further information about Nomad please refer to Downloading client content and Nomad integration below.

1.3.8.4.2 WAN caching

Communications between Tachyon platform clients and Switches should not be cached or delayed, which can be prevented by excluding the Switch port(s) or the IP Addresses of Switch interfaces on caching devices.

Communications between clients and the Background Channel can be cached, however, please refer to Downloading client content and Nomad integration as an alternative to WAN caching.

1.3.8.4.3 Isolated Networks

Tachyon can operate in a multi-domain, multi-forest environment with client devices on internal and external networks, supporting internal and external Certificate Authorities.

Each client device must have a network connection to a Switch and Background Channel, with the necessary network firewall ports open. If clients are unable to connect to the Tachyon server on the corporate network, then it is necessary to install additional Tachyon servers.

1.3.8.5 DNS Names

Each server that has Tachyon platform components installed requires its own DNS Name. A DNS Name can be a DNS alias, CNAME or Host (A) record.

Master Stack	The Master Stack is used by the following, therefore it helps users if it has a recognizable and convenient DNS Name such as **tachyon** - this is specified during installation of the Tachyon server using Tachyon Setup. • Tachyon users, approvers and administrators connecting to the Tachyon Portal and Consumer API • Remote tools and Consumer applications connecting to the Consumer API • Remote Response Stacks and DMZ Server connecting to the Coordinator service. Platform services also reside on the Master Stack, which non-Tachyon clients connect to, for example: • Application Migration, used by Windows Self-Service task sequences • AppClarity, used by AppClarity Software Reclaimer.
DMZ Server	The DMZ Server is a type of Response Stack used to provide Tachyon Real-time and Inventory services to Internet-based clients. It requires an external DNS Name - for example **tachyonext** - this is specified during installation of the DMZ Server using Tachyon Setup. The DNS Name is shared between the Switch network interfaces and Background Channel on the DMZ Server, and specified during installation of Tachyon platform clients, and stored in their configuration file.
Response Stack	A Response Stack is used to provide Tachyon Real-time and Inventory services to clients on the internal (corporate) network. The choice of DNS Name is discussed in the table below. The DNS Name is shared between the Switch network interfaces and Background Channel on the Response Stack, and specified during installation of Tachyon platform clients, and stored in their configuration file.

The number of DNS Names used by a system depend on the location of Tachyon and other Platform services. The table below describes options.

Single DNS Name	A Tachyon system can have a single DNS Name if all components are installed on the same server, for example **tachyon** - this is specified during installation of the Tachyon server using Tachyon Setup. If the server has multiple Switches, and therefore multiple network interfaces, then the same DNS Name can be shared by all Switches, the Background Channel and Master Stack.

Multiple client-facing DNS Names

The following client-facing components can each have their own DNS Name:

- Tachyon Switch and Background Channel on Response Stack servers, including DMZ Server
- Tachyon platform services on the Master Stack, used by clients of Application Migration and/or AppClarity software reclaim
- Tachyon Portal, and Consumer API, on the Master Stack, used by administrators.

Note

Master and Response Stacks must have different DNS Names if they exist on different servers:

- The Master Stack has its own DNS Name, for example, **tachyon**
- Each Response Stack can have its own client-facing DNS Name, or they can share a common client-facing DNS Name, for example **tachyonrs**.

When a Response Stack is installed on the same server as Master Stack, it will normally share the same DNS Name as Master Stack as described under #UUIDba4ce843708df87c3577ca1f7920f3d8_id_PreparationSingleDNSName. However, if you have multiple Response Stacks and want them to share the *same* DNS Name, then the Master Stack must use a *different* DNS Name. This approach of all Response Stacks sharing the same DNS Name simplifies adding further Response Stacks at a later date.

During installation - using Tachyon Setup - you need to consider the following:

HTTP binding	Required for installation, but can be manually removed later - please refer to Tachyon Server post-installation tasks. This binding is not used by Tachyon platform clients or administrators, but can optionally be used for Application Migration and/or AppClarity reclaim clients. Example name **acme-tcn01**.
HTTPS binding	Required. This is the main binding. On a Master Stack server (that has no Response Stack components) it is used by administrators to connect to the Tachyon Portal. It can optionally be used for Application Migration and/or AppClarity reclaim clients. Example name **tachyon** .

On a Response Stack server, it is used by clients to connect to Switches and/or Background Channel. Example name **tachyon** or **tachyonrs**. See panel above about making the right choice.

On a DMZ Server, it is used by Internet-based clients to connect to Switches and/or Background Channel. Example name **tachyonext**. See below.

Alternate HTTPS binding

Required, except in the simplest (single server) configurations, described above.

It is typically used by other Tachyon platform servers to connect to each other, but there are other scenarios.

- Required on a Response Stack server if it will have a DMZ Server connected to it. Example name **tachyonalt**.
- Required on a DMZ Server - used by internal servers to connect to the DMZ Server - see below. Example name **tachyondmz**. See below.
- Required on a Master Stack if you have local and remote Response Stack(s) - used for inter-server communications. Example name **tachyonalt**.
- Required on a Master Stack if the main HTTPS binding is used by client-facing components, and you want a different name for the Portal. Used by administrators to connect to the Tachyon Portal. Example name **tachyon**.
- Required on a Master Stack if you need a different **HTTPS port** for Application Migration and/or AppClarity reclaim clients. This can be by choice, or if you have upgraded from an original SLA Platform installation that used different ports.

Manual bindings

You can manually add further HTTP and HTTPS bindings after installation, to help differentiate the services which client devices and administrators connect to.

If you are upgrading ActiveEfficiency to Tachyon platform then you might have had a HTTPS binding described as **aeserver** in previous documentation.

If Master and Response Stacks are on the same server and you want them to have different DNS Names, then use the main binding for client connections to the Response Stack (because it is client-facing) and use the Alternate binding for other connections to the Master Stack. A simpler option is to put the Response Stack on its own server. Remote Response Stacks are recommended if the Master Stack is also hosting services AppClarity Software Reclaimer or Application Migration.

If you want to configure Switches on the same server to use multiple DNS Names, you will need to seek guidance from 1E. In most cases this is not required or recommended.

Internal DNS Names

A DMZ Server is a special example of a Response Stack. The DMZ Server itself requires two DNS Names:

- A client (external) facing DNS Name - for example **tachyonext** - which is shared between the Switch network interfaces and Background Channel on the DMZ Server - this is specified during Tachyon Setup as the main HTTPS binding
- An internal facing DNS Name for the internal network - for example **tachyondmz** - this is specified during Tachyon Setup as the alternate main HTTPS binding.

Note

Both DNS Names must be included in the web server certificate. You can manually replace the external/client facing certificate after installation, to comply with best practice not to expose internal names in an external facing certificate.

The internal Response Stack also requires an additional DNS Name - for example **tachyonalt** - for internal communications with the DMZ Server.

Please refer to Implementing a Tachyon DMZ Server for more detail about DMZ Servers.

Note

Note

Tachyon Setup supports installation of one HTTP and up to two HTTPS bindings, but you can manually add more bindings after installation.

Tachyon Setup currently supports only one Web server certificate, which must contain all the DNS Names used by the HTTPS bindings on that server. Each DNS Name must be

included as a DNS Name in the **Subject Alternate Name (SAN)** entry of the web server certificate.

You can manually add more certificates, and change bindings. Please refer to Certificate requirements . Please note that Tachyon Setup helps maintain the main and alternate HTTPS bindings using one certificate.

1.3.8.6 Service Principal Names

Tachyon platform and applications use underlying IIS and SQL Server technology, and only require HTTP or MSSQLSvc class SPNs if your company security policy has configured IIS or SQL Server to use Kerberos authentication.

If your IIS server is using Kerberos, then each DNS Name used to access a Tachyon Web Server requires an HTTP class **Service Principal Name (SPN)** to be registered against the relevant service account in Directory, which is **computer$** by default. This allows Tachyon web applications to authenticate clients using Windows Authentication where Kerberos is an authentication provider (primary, fallback or negotiated).

Note

If your IIS server is using Kerberos then HTTP SPNs are required for web applications that use Windows Authentication, and are created using:

- The web application pool's service account, which is Network Service for all Tachyon application pools, and therefore is the computer$ account
- Each (A) Host record used to access the web application. If the server is accessed using a CNAME record, then you need to register an SPN for each (A) Host record used by the CNAME. A CNAME will have multiple (A) Host records when using round-robin or NLB to access the web server.

SPNs are not required for DNS Names used to connect to Switches or Background Channel, because they do not use Windows Authentication. However, bear in mind the same DNS Name might be used to access other web applications.

1.3.8.7 Downloading client content and Nomad integration

1E Client downloads content from the Tachyon Background Channel. Content is mainly scripts and other files required by instructions. It also includes client resources such as extensible modules, providers, and other dependencies to maintain the 1E Client. In most cases, client resources are version controlled to prevent repeated downloads. Tachyon instructions always request a download even if they have run an instruction before, unless the content for that instruction has been cached in memory.

You may need to consider the impact on the network if there is a large amount of content included in an instruction. This is more of an operational consideration instead of a design consideration.

Nomad is an optionally licensed component of the 1E Client. It makes software deployment, patching and downloading content more efficient and reduces the impact on the network. It removes the need for remote Distribution Point servers in Microsoft System Center Configuration Manager systems. When Nomad is installed on computers, it automatically elects a peer to download content from a server over the WAN and

then peer-shares the content with other PCs at the same location. The downloaded content is cached locally on each PC in case it is needed again.

Tachyon can optionally use Nomad to download content from servers irrespective of whether Nomad is integrated with Configuration Manager or not, and also uses advanced Nomad features.

1.3.8.7.1 Tachyon client integration with Nomad disabled

If Nomad integration is not used, the following apply:

- Tachyon platform client waits a randomized stagger period defined by its DefaultStaggerRangeSeconds setting, and then downloads content from the specified **Background Channel**.
- Tachyon platform client retains modules and extensibles that it has downloaded, but does not retain instruction scripts after they have been run. Any instruction that requires a script or other file will download the latest version each time the instruction is run.

1.3.8.7.2 1E Client integration with Content Distributionenabled

Content Distribution integration is available on Windows PC devices and is enabled by default, but can be disabled during installation of the 1E Client.

With the Content Distribution integration feature enabled, 1E Client will detect if a supported version of Content Distribution is running on the device.

- 1E Client immediately requests Content Distribution to download content from the specified HTTP source, such as the **Background Channel**. Content Distribution behaves in the same way as it does with Configuration Manager by ensuring the latest version of content is obtained and electing a master to perform the actual download.
- Content Distribution maintains its own cache of downloaded content which avoids the need for repeat downloads over the WAN, and provides content to peers that require the same resources which avoids peer devices having to download over the WAN.
- If the Content Distribution integration feature is enabled, and requested content is not provided within the timeout period, the 1E Client will fall back to downloading directly from the HTTP source. The most likely reason for a timeout is if Content Distribution is busy downloading other content.

To use Content Distribution, there is no special configuration of Tachyon Servers unless you want to use server-based features provided by the Content Distribution and Content Distribution, which requires the reverse proxy feature to be configured on Background Channels.

The Background Channel is a web application on the Tachyon Server which uses HTTPS and default port is 443. The URL for the Background Channel is defined in the 1E Client configuration file and is specified during installation of the 1E Client if Tachyon features are enabled. The 1E Client passes this URL to Content Distribution when it requests content to be downloaded. Instructions can also specify other HTTP sources.

Content Distribution does not need to be configured to use certificates in order to communicate with the Background Channel (the Content Distribution CertIssuer and CertSubject settings are used only with Configuration Manager Distribution Points that are configured to validate device certificates).

The **Nomad Single-Site Download (SSD)** feature, which uses **Content Distribution**, further reduces the impact of downloading content over the WAN.

1.3.9 1E Client requirements

You will need to plan the deployment of 1E Client using whichever software deployment tools you have.

The 1E Client Deployment Assistant provides a wizard that simplifies deployment of 1E Client for Windows. It also integrates with Configuration Manager to create deployments, for more details refer to Introducing 1E Client Deployment Assistant.

1.3.9.1 Deployment

You must decide how you will configure the 1E Client and deploy to devices.

> **Note**
>
> For more information about configuring the 1E Client properties during and after installation, please refer to 1E Client configuration settings and installer properties.

For details of interactive and command-line installation, please refer to Deploying 1E Client.

Tachyon, Nomad, and Shopping require client certificates. For more detail, please refer to Certificate requirements.

1.3.9.2 Installation accounts

1.3.9.2.1 1E Client Windows installation account

The 1E Client installer installs a service as local system, therefore the installation account for Windows clients must be capable of being elevated in order to run the installer. The simplest way of achieving this is for the account to have full local administrator rights (as a member of the localgroup administrators, either directly or indirectly).

1.3.9.2.2 1E Client non-Windows installation account

To install the 1E Client on a non-Windows client the installation account must have privileges to run the **sudo** command.

1.3.9.3 Supported device platforms

Below are lists of supported OS Platforms. Please also refer to Constraints of Legacy OS, which applies to server and client OS.

1.3.9.3.1 Windows client

Category	Product	Notes
Operating System	• Windows Server 2022 • Windows Server 2019	The zip for 1E Client for Windows is available for download from the support.1e.com/. Professional and Enterprise editions are supported for Windows 10 and Windows 11.

Category	Product	Notes
	• Windows Server 2016 • Windows 11 CB 22H2 • Windows 11 CB 21H2 • Windows 10 CB 22H2 • Windows 10 CB 21H2	All versions are provided with 32-bit & 64-installers, and can be installed on physical and virtual computers. **Note** This list shows only those OS versions in mainstream support by Microsoft, and therefore supported by Tachyon, and by 1E Client 8.1. Please refer to Constraints of Legacy OS regarding the end of mainstream support. For Microsoft product lifecycle details, please refer to https://support.microsoft.com/en-us/lifecycle/search. Refer to Support for Microsoft Rapid-Release Cycle on https://support.1e.com/ for details of which Current Branch versions are supported by 1E products, and known issues regarding specific versions. For installation guidance on Windows, please refer to Deploying 1E Client on Windows. The following 1E Client features and modules are supported on Windows OS: • Real-time features (for example instructions, experience, interaction) • Nomad client • PXE Everywhere Agent client • Shopping client • Windows Servicing Assistant (WSA) client (workstation OS only, not server OS) • WakeUp client
Runtime libraries	• .NET Framework 4.8	.NET Framework is required only for the following features of 1E Client:

Category	Product	Notes
	• Visual C++ 2015-2019 Redistributable	• The Real-Time Control Center feature of the 1E Client (also known as 1E Client UI and Interaction module) supports Experience Engagements (Announcements and Surveys), and ITSM Support Tickets • Windows Servicing Assistant (WSA) is a feature of the Shopping/WSA client module, which supports OS deployment, upgrades and migrations. **Note** This list shows only those .NET Framework versions in mainstream support by Microsoft, and therefore supported by 1E, and by 1E Client 8.1. For Microsoft product lifecycle details, please refer to https://support.microsoft.com/en-us/lifecycle/search. 1E Client installer includes the Visual C++ 2015-2019 Redistributable package.
Other Windows Software	• Nomad 8.0 (or later) • PowerShell 3.0 (or later)	1E Client provides real-time client features. It also includes the Nomad client module. Real-time client features can optionally use Nomad to download content (feature enabled by default) if the Nomad client module in 1E Client is enabled (module disabled by default) or Nomad 7.0 or later is running. For more details please refer to Nomad client requirements. PowerShell is not a prerequisite for installation of the 1E Client. PowerShell is used by some Tachyon instructions (that have PowerShell commands embedded or scripts that are downloaded) and some of these require PowerShell 3.0 or later.

Category	Product	Notes
Microsoft Endpoint Configuration Manager Client	• MECM CB 2211 • MECM CB 2207 • MECM CB 2203 • MECM CB 2111 • MECM CB 2107	The following client features work with these versions of Configuration Manager on Windows computers: • Real-time client - instructions used by Tachyon Configuration Manager Console extensions • Nomad client • PXE Everywhere Agent • Shopping/WSA client • WakeUp client - including Policy Refresh and REFRESHONSUBNETCHANGE features Configuration Manager is not a prerequisite for installation of the 1E Client, and except for above features, the 1E Client, its features and modules, have no dependency on Configuration Manager. Tachyon, Nomad, WakeUp, and Application Migration have Configuration Manager Console extensions which are available separately. **Note** This list shows only those Configuration Manager versions in mainstream support by Microsoft, and therefore supported by 1E, and by 1E Client 8.1. For Microsoft product lifecycle details, please refer to https://support.microsoft.com/en-us/lifecycle/search. Please refer to the Support for the Microsoft Rapid-Release Cycle on https://support.1e.com/ for details of which Current Branch versions are supported by 1E products, and known issues regarding specific versions. (Microsoft Endpoint Configuration Manager - MECM - is also known as Configuration Manager,

Category	Product	Notes
		ConfigMgr, Config Man, CM, and SCCM among other names. Version names include 2012 and Current Branch or CB.)

1.3.9.3.2 macOS clients

Category	Product	Notes

Operating System	• macOS Monterey 12.0
	• macOS Big Sur 11.6
	• macOS Big Sur 11.0
	• macOS Catalina 10.15
	• macOS Mojave 10.14
		Other versions of these non-Windows OS should work but have not been tested by 1E.
		
		1E Client package for macOS is included in the non-Windows zip available for download from the support.1e.com/.
		
		Note
		1E Client for macOS is written for Intel and supported on Apple devices using Intel processors. It is also supported on Apple devices using the M1 chip, provided you have installed Rosetta 2, which is included with Big Sur. 1E Client is a daemon (not an app), therefore, during installation or running it will *not* prompt for Rosetta 2, which does not get installed on-demand.
		You only need to install Rosetta 2 once, using one of the following commands, but repeating the command will safely reinstall it. The second version of the command requires root permission. Attempting to install on an Intel device will issue a harmless "unrecognized option" usage message.
		`/usr/sbin/softwareupdate --install-rosetta`
		`/usr/sbin/softwareupdate --install-rosetta --agree-to-license`
		
		For installation guidance, please refer to Deploying 1E Client on macOS.

Other Software	• Bash • Perl • Rosetta 2 (on non-Intel)	Bash and perl are required for installation of 1E Client on all non-Windows OS. Tachyon instructions support the use of Bash scripts on all supported non-Windows OS.

Category	Product	Notes
		To see if an Instruction requires a Bash script, look in its Instruction Definition XML file for Bash script resources defined under the <Resources> tag. Bash is the preferred choice when developing custom instructions for non-Windows OS. There are slight differences between OS implementations of Bash, particularly on the Mac. Therefore, 1E recommends testing custom Bash scripts on each supported OS. Rosetta 2 must be installed before installing 1E Client for macOS on an Apple device using a non-Intel processor such as M1 chip. Please see note above about installing Rosetta 2.

1.3.9.3.3 Linux clients

Category	Product	Notes
Operating System	• CentOS Stream 8 • Debian 10.4 • Fedora 34 • openSUSE Leap 15.2 • Red Hat Enterprise Linux 7.9 • Red Hat Enterprise Linux 8.5 • SUSE Linux Enterprise 15.2 • Ubuntu 18.04	Other versions of these non-Windows OS should work but have not been tested by 1E. • 1E Client packages for other Linux distributions can be requested, including Raspberry Pi. • 1E Client for Linux supports Linux variations on Intel 64-bit platforms. • 1E Client packages for Linux are included in the non-Windows zip available for download from support.1e.com/. • 1E Client supports features on non-Windows devices. For installation guidance on the following OS, please refer to Deploying 1E Client on Linux.
Other Software	• Bash • Perl	Bash and perl are required for installation of 1E Client on all non-Windows OS.

Category	Product	Notes
		Tachyon instructions support the use of Bash scripts on all supported non-Windows OS. To see if an Instruction requires a Bash script, look in its Instruction Definition XML file for Bash script resources defined under the <Resources> tag. Bash is the preferred choice when developing custom instructions for non-Windows OS. There are slight differences between OS implementations of Bash, particularly on the Mac. Therefore, 1E recommends testing custom Bash scripts on each supported OS.

1.3.9.3.4 Solaris clients

Category	Product	Notes
Operating System	• Withdrawn	**Note** 1E Client is no longer available for Solaris, but 1E may reintroduce it, if there is sufficient demand.

1.3.9.4 Tachyon scripting requirements

You must ensure the appropriate scripting environment is present on client devices. SCALE supports running native **PowerShell** on Windows and **bash** on non-Windows devices, which can be script files downloaded when an instruction runs, or command text.

- Windows Tachyon clients can use **PowerShell** scripts. Ensure your client devices have an appropriate version of PowerShell installed to support any custom scripts you may develop. PowerShell on Windows OS.
- Non-Windows clients use **bash** as their scripting medium. This should be present on all non-Windows 1E Client devices. See Bash on non-Windows OS.

1.3.9.4.1 PowerShell on Windows OS

PowerShell is used by some Tachyon instructions (that have PowerShell commands embedded or scripts that are downloaded) and some of these require PowerShell 3.0 or later, although some scripts will support PowerShell 2.0. PowerShell scripts are supported only on Windows OS.

If installing or upgrading PowerShell, it is best to install the latest version available. However, do not expect full forward or backward compatibility between PowerShell versions.

Tip

To determine the version of PowerShell on a computer, start PowerShell (command prompt or ISE) and enter one of the following commands: **$PSVersionTable.PSVersion** or **$PSVersionTable** for more detail.

The table below shows which versions of PowerShell are supported on each OS version and Service Pack, and if it is built-in or needs to be installed.

OS Version	PowerShell Version	Notes					
Windows Server 2022						RTM (Notes 12, 13)	Note 4
Windows 11						RTM (built-in)	
Windows Server 2016, 2019, 2022					RTM (Note 9)	RTM (Notes 12, 13)	Note 4
Windows 10					RTM (built-in)	Anniversary Update (built-in)	
Windows Server 2012 R2 *				RTM (built-in)	RTM (Note 9)	RTM (Note 12)	Note 4
Windows 8.1 *				RTM (built-in)	RTM (Note 9)	RTM (Note 12)	
Windows Server 2012 *			RTM (built-in)	RTM (Note 7)	RTM (Note 9)	RTM (Note 12)	Note 4
Windows 8 *			RTM (built-in)				
Windows Server 2008 R2 *		RTM (built-in)	SP1 (Note 6)	SP1 (Note 7)	SP1 (Note 8)	SP1 (Note 10)	Note 4

OS Version	PowerShell Version	Notes					
Windows 7		RTM (built-in)	SP1 (Note 6)	SP1 (Note 7)	SP1 (Note 8)	SP1 (Note 10)	
Windows Server 2008 *	RTM (built-in)		SP1 & SP2 (Note 2)				
Windows Server 2003 *	RTM & SP1	R2 & SP2					Notes 1, 2
Windows Vista *	RTM	SP1 & SP2					Notes 1, 2
Windows XP *	RTM, SP1 & SP2	SP3					Notes 1, 2

* These OS are regarded as legacy OS:

1. PowerShell is not built-in for these OS. These OS do not support 3.0 or later. See Constraints of Legacy OS
2. If PowerShell 1.0 is installed it must be removed in order to install a later version.
3. Support for PowerShell 2.0 is included in PowerShell 3.0 and later.
4. PowerShell is not installed by default on these OS but is an optional feature that should be enabled using Server Manager.
5. PowerShell 2.0 is part of WMF Core package (KB968930) with prerequisite of .NET Framework 3.51 (which includes .NET 2.0 SP1).
6. PowerShell 3.0 is part of WMF 3.0 with prerequisite of .NET Framework 4.0 or later. Refer https://www.microsoft.com/en-us/download/details.aspx?id=34595
7. PowerShell 4.0 is part of WMF 4.0 with prerequisite of .NET Framework 4.5 or later. Refer https://www.microsoft.com/en-us/download/details.aspx?id=40855
8. PowerShell 5.0 is part of WMF 5.0 with prerequisites of .NET Framework 4.5 or later and WMF 4.0. Refer https://www.microsoft.com/en-us/download/details.aspx?id=50395
9. PowerShell 5.0 is part of WMF 5.0 without any other prerequisites. Refer https://www.microsoft.com/en-us/download/details.aspx?id=50395
10. PowerShell 5.1 is part of WMF 5.1 with prerequisites of .NET Framework 4.6 or later, WMF 4.0 and SHA-2 Code Signing. Refer https://msdn.microsoft.com/en-us/powershell/wmf/5.1/install-configure

11. PowerShell 5.1 is part of WMF 5.1 with prerequisites of .NET Framework 4.6 or later and WMF 4.0. Refer https://msdn.microsoft.com/en-us/powershell/wmf/5.1/install-configure

12. PowerShell 5.1 is part of WMF 5.1 with prerequisite of .NET Framework 4.6 or later. Refer https://msdn.microsoft.com/en-us/powershell/wmf/5.1/install-configure

13. In these Server OS, PowerShell 5.1 is referred to as the Desktop Experience. You can use the PowerShell Core version if you prefer.

Please refer tohttps://support.microsoft.com/en-gb/help/17455/lifecycle-faq-net-framework for details of Microsoft support for .NET Framework.

- Support for 4, 4.5, and 4.5.1 ended on January 12, 2016
- Support for 4.5.2, 4.6 and 4.6.1 ended on April 26, 2022

1.3.9.4.2 Bash on non-Windows OS

Bash and perl are required for installation of all non-Windows 1E Client.

Tachyon instructions support the use of Bash scripts on all supported non-Windows OS.

To see if an Instruction requires a Bash script, look in its Instruction Definition XML file for the Scripting.Run method. Bash is the preferred choice when developing custom Instructions for non-Windows OS.

There are slight differences between OS implementations of Bash, particularly on the Mac. Therefore, 1E recommends testing custom Bash scripts on each supported OS.

1.4 Installing Tachyon

How to set up Tachyon servers.

Once you have reviewed relevant requirements, you will know how many Tachyon servers you will need, and where they will be installed. After Preparation of each server, you will use this documentation section to help you install each server.

1.4.1 Preparation

What you will need to prepare in advance of implementing a Tachyon server in your network. Typically, these are tasks that may take some time to organize, depending on how your organization works.

1.4.1.1 Implementation Overview

Please review all tasks to decide how you wish to proceed, and record all configuration details.

Implementation of Tachyon can be extremely quick if all necessary preparations have taken place, and is typically performed in this order:

1. Obtain the Tachyon License file - ensure it includes entries for the consumer applications you have purchased.

2. Provision the Tachyon Web and SQL server hardware refer to Server Provisioning.

- Install the Windows Server OS
- Configure Network interfaces
- Create the server's DNS Names (see note) and Service Principal Names
- Obtain and install the server's Web Server Certificate, for which you will need to know the server's DNS Name
- Install IIS roles, role services and features, refer to Windows Server roles and features.

3. Optionally pre-create the Tachyon databases, refer to Tachyon databases (you can allow the Tachyon server installer to create the databases using default settings).
4. Prepare the Mail Server.
5. Identify and create AD Accounts and Groups, refer to Active Directory.
6. Review each of the requirements pages under Planning for Tachyon.
7. Run Tachyon Setup.
8. Manually install clients on a few test devices, refer to Deploying 1E Client.
9. Use the Tachyon Verification Product Pack to verify the installation, refer to Verifying.
10. To install other Instruction Definitions refer to Instruction sets page - from the Tachyon Platform zip, and from https://exchange.1e.com/
11. Add the Instruction Definitions to Instruction Sets to determine their permissions, refer to the Instruction sets page.
12. Install Tachyon Consumers (documentation not provided here).
13. Package the Tachyon client as required by your software deployment tool (see note).
14. Deploy the client to more pilot devices.
15. Pilot testing.
16. Start rollout of clients.
17. Use the SDK to begin developing your own instructions and testing your use cases.

Note

If your organization requires the client to be packaged, then you can do this once you know the **DNS Name(s)**. Then you can prepare for deploying the client in parallel to preparing and installing the server.

1.4.1.2 Details required when using Tachyon Setup to install a Tachyon server

The table below lists details required on each of the Tachyon Setup screens. You can review screens in the Tachyon Setup page. Items marked * can wait until after installation.

Tachyon Setup	Documentation Reference	All components installed on a single server	Master Stack	Response Stack	DMZ Server
Configuration		Decide which applications you want to install from the following list: • Experience • Nomad • Business Intelligence (required for Patch Success) • AppClarity • Application Migration.	Decide which applications you want to install from the following list: • Experience • Nomad • Business Intelligence (required for Patch Success) • AppClarity • Application Migration	Select Nomad if you are using, or plan to use Nomad.	Select Nomad if you are using, or plan to use Nomad.
Check prerequisites	Web Server Certificate Windows Server roles and features	All prerequisites must be checked, including: • ASP.NET Core Hosting Bundle (if using Nomad) • SQL BCP *	All prerequisites must be checked, including: • ASP.NET Core Hosting Bundle (if using Nomad)	All prerequisites must be checked, including: • SQL BCP *	All prerequisites must be checked.

Tachyon Setup	Documentation Reference	All components installed on a single server	Master Stack	Response Stack	DMZ Server
Server certificate	Web Server Certificate(server)	A web server certificate is required for: • Website (including Explorer, Consumer API, Core and Background Channel) • Switch(es)	A web server certificate is required for: • Website (including Explorer and Consumer API)	A web server certificate is required for: • Website (Core and Background Channel) • Switch(es)	A web server certificate is required for: • Website (Background Channel) • Switch(es)
Client certificates	Web Server Certificate (clients) *	Decide whether you will require certificates to be presented by the clients. Import the certificates of any trust authorities used by devices and remote servers that do not match the trust authority used by the Server certificate.	Decide whether you will require certificates to be presented by the clients. Import the certificates of any trust authorities used by devices and remote servers that do not match the trust authority used by the Server certificate.	Import the certificates of any trust authorities used by devices and remote servers that do not match the trust authority used by the Server certificate.	Import the certificates of any trust authorities used by devices and remote servers that do not match the trust authority used by the Server certificate.
Database servers	SQL Databases	Name of the SQL Server	Name of the SQL Server	Name of the SQL Server	This page is greyed out.

Tachyon Setup	Documentation Reference	All components installed on a single server	Master Stack	Response Stack	DMZ Server
		instance that will host the new TachyonMaster database. Name of the SQL Server instance that will host the new TachyonResponses database. Names of the SQL Server instances that will host the additional databases used by any bundled components that are selected for installation. Keep old DB or not (n/a for new installation). If using a remote SQL Server, please refer to Network interfaces.	instance that will host the new TachyonMaster database. Names of the SQL Server instances that will host the additional databases used by any bundled components that are selected for installation. Keep old DB or not (n/a for new installation).	instance that hosts the existing TachyonMaster database. Name of the SQL Server instance that will host the new TachyonResponses database. Keep old DB or not (n/a for new installation). If using a remote SQL Server, please refer to Network interfaces.	The DMZ Server does not have direct access to SQL Servers. Access to databases is via the Core API on the internal Response Stack. Manual steps are required to configure access to the Core API, as described in Implementing a Tachyon DMZ Server.
SSAS servers	SSAS Databases BI SSAS user - only if the	Name of the SQL Server SSAS instance that will host the	Name of the SQL Server SSAS instance that will host the	n/a	n/a

Tachyon Setup	Documentation Reference	All components installed on a single server	Master Stack	Response Stack	DMZ Server
	BI component is selected for installation	multidimensional data cube for BI (required by Patch Success). Account credentials that will be used for the BI services.	multidimensional data cube for BI (required by Patch Success). Account credentials that will be used for the BI services.		
Number of devices	Architectural requirements	Specify the number of devices supported by this server in order to calculate the number of Switches required, as well as the number of Workers and Slots used by the Switches.	The number is only used to cross-check against the number in the license file.	Specify the number of devices supported by this server in order to calculate the number of Switches required.	Specify the number of devices supported by this server in order to calculate the number of Switches required.
Switch configuration	Network interfaces	Select an IP Address for each Switch. All Switch IP Addresses will typically use the same DNS Name. If the TachyonResponses database is remote from the server, and the number of	This page is greyed out. The Master Stack does not require Switch configuration.	Select an IP Address for each Switch. All Switch IP Addresses will typically use the same DNS Name. If the TachyonResponses database is remote from the server, and the number of	Select an IP Address for each Switch. All Switch IP Addresses will typically use the same DNS Name. Provide an additional interface so that internal traffic uses a different IP

Tachyon Setup	Documentation Reference	All components installed on a single server	Master Stack	Response Stack	DMZ Server
		devices is more than 500, provide an additional interface so that SQL traffic uses a different IP address to the Switch(es), and see and Configuring a persistent route for SQL traffic.		devices is more than 500, provide an additional interface so that SQL traffic uses a different IP address to the Switch(es), and see and Configuring a persistent route for SQL traffic.	address to the Switch(es), and see and Configuring a persistent route for SQL traffic.
Website configuration	Windows Server roles and features	Required for website.	Required for website.	Required for website.	Required for website. Specify names for the internal facing network interface. The HTTPS binding for the external facing network interlace is created manually after installation.
Active Directory and email	Email and 2FA requirements: SMTP server Email and 2FA requirements: Two-	Required for Master Stack components.	Required for Master Stack components.	n/a (Uncheck Enable SMTP)	n/a (Uncheck Enable SMTP)

Tachyon Setup	Documentation Reference	All components installed on a single server	Master Stack	Response Stack	DMZ Server
	factor Authentication requirements				
Telemetry	Telemetry	Optional.	Optional.	n/a	n/a
SLA and 1E Catalog	1E Catalog	Confirm internet access to the 1E Catalog.	Confirm internet access to the 1E Catalog.	n/a	n/a
Nomad	Nomad (Only if installing Nomad)	If Nomad is enabled: • Name of the Configuration Manager site server that will be queried to locate its SQL database • The synchronization interval in minutes • Client authenti	If Nomad is enabled: • Name of the Configuration Manager site server that will be queried to locate its SQL database • The synchronization interval in minutes.	If Nomad is enabled: • Client authentication certificate for the Background Channel to communicate with Content Distribution API.	If Nomad is enabled: • Client authentication certificate for the Background Channel to communicate with Content Distribution API.

Tachyon Setup	Documentation Reference	All components installed on a single server	Master Stack	Response Stack	DMZ Server
		cation certificate for the Background Channel to communicate with Content Distribution API.			

Other requirements:

- Server Installation Account, refer to Installation Accounts
- Server sizing for on-premises, refer to On-premises installation
- Server sizing for AWS and Azure, refer to On-premises installation

Post-installation requirements:

- Tachyon user permissions
- Product integration requirements
- Verifying
- Client devices preparation, refer to License file.

1.4.1.3 License file

You will need to obtain a valid license file from 1E. For more details, please refer to License requirements.

1.4.1.3.1 Whitelisting for license activation and validation

Ensure the following URL is whitelisted:

- https://license-v1.1e.com

This URL must be accessible from the Tachyon Server during the setup and running of Tachyon.

The Tachyon license must be validated on a regular basis via internet contact with the 1E license service. The regular validation period is set when the license is requested.

For whitelisting purposes, the Tachyon Server (specifically the Coordinator Workflow module in Master Stack) requires an Internet connection to the 1E license service, as defined in the license file itself. If activation fails, then the system will install but not be usable until the activation is completed.

Upgrading

When upgrading, you are recommended to get a new license file and update your whitelist with the new URL. The old URL (https://license.1e.com) is suitable only for 8.0 and earlier. However, if you are upgrading and your license file has the old URL then you should also whitelist the old URL.

Note

Other URL must also be whitelisted, please refer to Whitelisting connections to 1E Cloud.

1.4.1.3.2 Code Signing Certificates

You will need your own code signing certificate, and have it registered in your Tachyon license, if you want to develop your own custom Tachyon instructions, or modify those of other authors. Instructions that are provided in the Tachyon Platform or downloaded from the 1E Exchange have already been code signed using the Platform and Exchange certificates from 1E. Your license controls whether you can use these instructions.

Ideally, all of your instruction developers should share a single **code signing certificate** between them. Each code signing certificate must be registered in your license and associated with your organization's **instruction name prefix**. When you have chosen your prefix and have your code signing certificate(s) you then need to send details of these to 1E, who will update your license. This will then automatically activate on your Tachyon Server (assuming it has connection to the Internet).

1.4.1.4 Server Provisioning

An IIS Web Server should be provisioned. SQL Server can be installed on the same server or the databases can be hosted on remote SQL Server instance(s). Please refer to /document/preview/791302#UUID-aa1c2691-97ed-e134-ac7d-62b2ea04fe4a regarding hardware and software specifications for on-premises and cloud servers.

In addition, the Tachyon Server requires the following, which requires more thought and preparation:

- Network interfaces
- DNS Names and their Service Principal Names
- Web Server Certificate
- Install and configure IIS, refer to Windows Server roles and features
- Services and NTFS Security.

1.4.1.4.1 Network interfaces

For the remote SQL Server requirement, please refer to Configuring a persistent route for SQL traffic. However, please ensure you also consult your server, firewall, and networking teams.

Cloud implementations have special configuration requirements for SQL Server and network interfaces described in Server sizing requirements.

1.4.1.4.1.1 Configuring a persistent route for SQL traffic

The following example steps can be used to configure IPv4 network routing so that a specific network interface is used for all traffic going to the specified SQL Server. The example is for a Response Stack and SQL Server on different subnets, but also works if both servers are on the same subnet.

> **Note**
>
> If you add a new interface for SQL traffic after installing Tachyon, then ensure the interface is not registered in DNS using the same DNS Name that devices use to connect to Switches or Background Channel. If you intend to use the new interface to support inbound HTTP traffic from remote Response Stacks then you will also need to configure the Tachyon website to include the IP Address of the new interface as described in Server installation issues.
>
> In our example below we would add **10.0.10.31**. Installation and upgrades will automatically configure IP Address and Domain restrictions.

1. On the Tachyon Server (single-server or Response Stack) open a **PowerShell command prompt**
2. The following command should resolve the name and IP Address of the SQL Server, and show the existing network route. In our example the **10.0.20.20**.

   ```
   pathping ACME-SQL02
   ```

3. If not already installed on the server, add a new interface. Configure its properties as follows:
   - Disable IPv6
   - Configure IPv4 properties and assign a static IP Address and subnet mask. In our example, these are **10.0.10.31** and **255.255.255.0**.
   - You do not need to configure a default gateway. You can if required, but you will receive a warning later about multiple default gateways and redundancy. However, you do need to know the default gateway for the route to the SQL Server, in our example, this is **10.0.10.1**.
   - Click Advanced... and click on the DNS tab. Uncheck **Register this connection's addresses in DNS** so that the interface IP Address is NOT registered in DNS.
   - Click OK twice to save, and then Close
   - You can give the interface a name to help distinguish it from Switch interfaces. In our example, this is **Interface used for SQL**

Warning

This interface must not be registered in DNS if the DNS Name of the server is a CNAME Alias for (A) Host records registered by Switch interfaces because clients need to use the DNS Name to connect to Switches. If you need this interface to be registered in DNS, then do this with a (A) Host record.

4. Enter the following PowerShell command, which provides all the details you need to confirm interfaces have been configured correctly.

```
Get-NetIPConfiguration
```

5. This provides output similar to the following and tells us the interface index for the new interface. In our example, this is **7**.

```
InterfaceAlias       : Interface used for SQL
InterfaceIndex       : 7
InterfaceDescription : Microsoft Hyper-V Network Adapter #4
NetProfile.Name      : ACME.local
IPv4Address          : 10.0.10.31
IPv4DefaultGateway   : 10.0.10.1
DNSServer            : 10.0.1.2
                       10.0.1.3

InterfaceAlias       : Interface used for Switch 1
InterfaceIndex       : 5
InterfaceDescription : Microsoft Hyper-V Network Adapter #3
NetProfile.Name      : ACME.local
IPv4Address          : 10.0.10.32
IPv4DefaultGateway   : 10.0.10.1
DNSServer            : 10.0.1.2
                       10.0.1.3
```

6. Use the **route** command to add a persistent route. The mask must be **255.255.255.255** and NOT the same as the interface mask configured earlier because the persistent route to the SQL Server is for its IP Address and not its subnet.

```
route -p add <SQL Server IP Address> mask 255.255.255.255 <Interface used for SQL IPv4DefaultGateway> metric 1 if <Interface used for SQL Interface Index>
```

In our example:

```
route -p add 10.0.20.20 mask 255.255.255.255 10.0.10.1 metric 1 if 7
```

Note

For networks with no routing, such as a lab, the default gateway is 0.0.0.0. Therefore, <**Interface used for SQL IPv4DefaultGateway**> must be specified as **0.0.0.0**. In our example:

```
route -p add 10.0.20.20 mask 255.255.255.255 0.0.0.0 metric 1 if 7
```

If your lab has no routing then you should ensure other means for your Tachyon Server to connect to the 1E license service via the Internet.

7. Enter the following command to confirm that the **<SQL Server IP Address>** has a persistent route with the details specified. In our example, this is **10.0.20.20**.

   ```
   route print
   ```

8. Enter the following command to verify the route works and uses the correct interface.

   ```
   pathping ACME-SQL02
   ```

   The first line (hop 0) must show the name of the Tachyon Server and the IP Address of the interface. This IP Address will then be selected as **used for SQL** in the Switch configuration screen of Tachyon Setup. In our example this would be:

   ```
   0  ACME-TCN01.ACME.local [10.0.10.31]
   ```

1.4.1.4.2 Computername

The computername of a Tachyon Server must comply with Microsoft NetBIOS naming standards, which includes having a length of 15 characters or less.

Microsoft's guidance can be found here: https://docs.microsoft.com/en-us/windows/desktop/SysInfo/computer-names.

1.4.1.4.3 DNS Names

Each server that has Tachyon platform components installed requires its own DNS Name. A DNS Name can be a DNS alias, CNAME or Host (A) record.

Master Stack

The Master Stack is used by the following, therefore it helps users if it has a recognizable and convenient DNS Name such as **Tachyon** - this is specified during installation of the Tachyon Server using Tachyon Setup.

- Tachyon users, approvers and administrators connecting to the Tachyon portal and Consumer API
- Remote tools and Consumer applications connecting to the Consumer API
- Remote Response Stacks and DMZ Server connecting to the Coordinator service

Platform services also reside on Master Stack, which non-Tachyon platform clients connect to, for example:

- Application Migration, used by Windows Self-Service task sequences
- AppClarity, used by AppClarity Software Reclaimer.

DMZ Server	The DMZ Server is a type of Response Stack used to provide Tachyon Real-time and Inventory services to Internet-based clients. It requires an external DNS Name - for example, **tachyonext** - this is specified during installation of the DMZ Server using Tachyon Setup. The DNS Name is shared between the Switch network interfaces and Background Channel on the DMZ Server, and specified during installation of Tachyon clients, and stored in their configuration file.
Response Stack	A Response Stack is used to provide Tachyon Real-time and Inventory services to clients on the internal (corporate) network. The choice of DNS Name is discussed in the table below. The DNS Name is shared between the Switch network interfaces and Background Channel on the Response Stack, specified during installation of Tachyon platform clients, and stored in their configuration file.

The number of DNS Names used by a system depends on the location of Tachyon and other Platform services. The table below describes the options.

Single DNS Name	A Tachyon system can have a single DNS Name if all components are installed on the same server, for example, **tachyon** - this is specified during installation of the Tachyon Server using Tachyon Setup. If the server has multiple Switches, and therefore multiple network interfaces, then the same DNS Name can be shared by all Switches, the Background Channel, and Master Stack.
Multiple client-facing DNS Names	The following client-facing components can each have their own DNS Name: • Tachyon Switch and Background Channel on Response Stack servers, including DMZ Server • Tachyon platform services on Master Stack, used by clients of Application Migration and/or AppClarity software reclaim • Tachyon, and Consumer API, on the Master Stack, are used by administrators. **Note** Master and Response Stacks must have different DNS Names if they exist on different servers: • The Master Stack has its own DNS Name, for example, **tachyon** • Each Response Stack can have its own client-facing DNS Name, or they can share a common client-facing DNS Name, for example **tachyonrs**.

When a Response Stack is installed on the same server as Master Stack, it will normally share the same DNS Name as Master Stack as described under #UUIDba4ce843708df87c3577ca1f7920f3d8_id_PreparationSingleDNSName. However, if you have multiple Response Stacks and want them to share the *same* DNS Name, then the Master Stack must use a *different* DNS Name. This approach of all Response Stacks sharing the same DNS Name simplifies adding further Response Stacks at a later date.

During installation - using Website configuration - you need to consider the following:

HTTP binding	Required for installation, but can be manually removed later - please refer to Removing the HTTP binding from the Tachyon website. This binding is not used by clients or administrators, but can optionally be used for Application Migration and/or AppClarity reclaim clients. Example name **acme-tcn01**.
HTTPS binding	Required. This is the main binding. On a Master Stack server (that has no Response Stack components) it is used by administrators to connect to the Tachyon portal. It can optionally be used for Application Migration and/or AppClarity reclaim clients. Example name **tachyon** . On a Response Stack server, it is used by clients to connect to Switches and/or Background Channel. Example name **tachyon** or **tachyonrs**. See the panel above about making the right choice. On a DMZ Server, it is used by Internet-based clients to connect to Switches and/or Background Channel. Example name **tachyonext**. See below.
Alternate HTTPS binding	Required, except in the simplest (single server) configurations, described above. It is typically used by other Tachyon platform servers to connect to each other, but there are other scenarios. • Required on a Response Stack server if it will have a DMZ Server connected to it. Example name **tachyonalt**.

- Required on a DMZ Server - used by internal servers to connect to the DMZ Server - see below. Example name **tachyondmz**. See below.
- Required on a Master Stack if you have local and remote Response Stack(s) - used for inter-server communications. Example name **tachyonalt**.
- Required on a Master Stack if the main HTTPS binding is used by client-facing components, and you want a different name for the Portal. Used by administrators to connect to the Tachyon portal. Example name **tachyon**.
- Required on a Master Stack if you need a different **HTTPS port** for Application Migration and/or AppClarity reclaim clients. This can be by choice, or if you have upgraded from an original SLA Platform installation that used different ports.

Manual bindings

You can manually add further HTTP and HTTPS bindings after installation, to help differentiate the services which client devices and administrators connect to.

If you are upgrading ActiveEfficiency to Tachyon platform then you might have had an HTTPS binding described as **aeserver** in previous documentation.

If Master and Response Stacks are on the same server and you want them to have different DNS Names, then use the main binding for client connections to the Response Stack (because it is client-facing) and use the Alternate binding for other connections to Master Stack. A simpler option is to put the Response Stack on its own server. Remote Response Stacks are recommended if Master Stack is also hosting services AppClarity Software Reclaimer or Application Migration.

If you want to configure Switches on the same server to use multiple DNS Names, you will need to seek guidance from 1E. In most cases, this is not required or recommended.

Internal DNS Names

A DMZ Server is a special example of a Response Stack. The DMZ Server itself requires two DNS Names:

- A client (external) facing DNS Name - for example, **tachyonext** - which is shared between the Switch network interfaces and Background Channel on

the DMZ Server - is specified during Tachyon Setup as the main HTTPS binding

- An internal facing DNS Name for the internal network - for example, **tachyondmz** - this is specified during Tachyon Setup as the alternate main HTTPS binding.

Note

Both DNS Names must be included in the web server certificate. You can manually replace the external/client facing certificate after installation, to comply with best practice not to expose internal names in an external facing certificate.

The internal Response Stack also requires an additional DNS Name - for example **tachyonalt** - for internal communications with the DMZ Server.

Please refer to Implementing a Tachyon DMZ Server for more detail about DMZ Servers.

Note

Note

Tachyon Setup supports installation of one HTTP and up to two HTTPS bindings, but you can manually add more bindings after installation.

Tachyon Setup currently supports only one Web server certificate, which must contain all the DNS Names used by the HTTPS bindings on that server. Each DNS Name must be included as a DNS Name in the **Subject Alternate Name (SAN)** entry of the web server certificate.

You can manually add more certificates, and change bindings. Please refer to Certificate requirements . Please note that Tachyon Setup helps maintain the main and alternate HTTPS bindings using one certificate.

Where possible the Tachyon Server DNS Name should be a **CNAME Alias** which references the **(A) Host** records for each of the Switch network interfaces registered in DNS.

Warning

Ensure network interfaces used for anything other than Switches, for example, the SQL interface, are not registered in DNS. If they are registered ensure the DNS Name used by Switches only has Switch IP Addresses assigned.

For multiple Switches to share the same DNS Name, the load balancing options include:

- **DNS round-robin.** Create a CNAME record which references the (A) Host records for each of the Switch network interfaces registered in DNS.
- **Network Load Balance (NLB)** and register the Tachyon Server's DNS Name as the NLB Name, and configure the NLB to forward to each of the Switch IP Addresses.

Note

DNS round-robin provides reasonable load balancing so that devices should be evenly spread across all Switches. Each device will cache the IP Address given to it by DNS and keep using that, even if the Switch using that IP Address is not available until the TTL expires or the DNS cache is flushed.

A Network Load Balancer (NLB) allows all the Switches to share the same DNS Name which is actually the IP Address of the NLB Cluster, which can then intelligently route the connection to a Switch interface.

1.4.1.4.4 Service Principal Names

Tachyon platform and applications use underlying IIS and SQL Server technology, and only require HTTP or MSSQLSvc class SPNs if your company security policy has configured IIS or SQL Server to use Kerberos authentication.

If your IIS server is using Kerberos, then each DNS Name used to access a Tachyon Web Server requires an HTTP class **Service Principal Name (SPN)** to be registered against the relevant service account in Directory, which is **computer$** by default. This allows Tachyon web applications to authenticate clients using Windows Authentication where Kerberos is an authentication provider (primary, fallback, or negotiated).

Note

If your IIS server is using Kerberos then HTTP SPNs are required for web applications that use Windows Authentication, and are created using:

- The web application pool's service account, which is Network Service for all Tachyon application pools, and therefore is the computer$ account
- Each (A) Host record used to access the web application. If the server is accessed using a CNAME record, then you need to register an SPN for each (A) Host record used by the CNAME. A CNAME will have multiple (A) Host records when using round-robin or NLB to access the web server.

SPNs are not required for DNS Names used to connect to Switches or Background Channel, because they do not use Windows Authentication. However, bear in mind the same DNS Name might be used to access other web applications.

If an SPN is not created, then you will see "401 Not authenticated" errors in the browser and/or log files.

Service Principal Names (SPN) are attributes of AD accounts. A domain administrator will need to create an HTTP class SPN for the Tachyon web server service account, by using one of the following methods:

- By editing the ServicePrincipalName attribute of the web server's computer account
- Using the following SETSPN commands, substituting your DNS Name, server and service account:

```
setspn -l ACME\ACME-TCN01$
setspn -s http/acme-tcn01.acme.local ACME\ACME-TCN01$
setspn -s http/tachyon.acme.local ACME\ACME-TCN01$
```

Use each command as follows:

1. List existing SPNs for the service account. Run this to record details before you request for any new SPN(s) to be created. Re-run this after creation, ensuring you wait sufficient time for AD replication to occur.
2. Use this if **tachyon.acme.local** is a CNAME record and its (A) Host record is **acme-tcn01.acme.local**.
3. Use this if **tachyon.acme.local** is a (A) Host record.

The above example assumes:

- The service account for all Tachyon web application pools is Network Service
- The Tachyon server name is **ACME-TCN01** with a computer account in the **ACME** domain, which means the service account is **ACME\ACME-TCN01$**
- The DNS Name for the server is **tachyon.acme.local**.

Tip

If in doubt, it does no harm to create an SPN for each DNS Name used to access the Tachyon Server, including its CNAMEs and (A) Host records using: *setspn -s http/<DNS Name> ACME\ACME-TCN01$*

To determine which type of record a DNS Name is, run the following command:

```
nslookup tachyon.acme.local
```

- If the command returns Name: **acme-tcn01.acme.local** and alias **tachyon.acme.local** then tachyon.acme.local is a CNAME record
- If the command returns Name: **tachyon.acme.local** and no aliases then tachyon.acme.local is a (A) Host record.

More complex scenarios can be configured which requires in-depth knowledge of IIS, SPN and DNS configuration and are beyond the scope of this documentation.

1.4.1.4.5 Web Server Certificate

1.4.1.4.5.1 What do I need to begin?

You will need to have requested a Web Server certificate from your Certificate Authority, using the specification below.

To get the certificate in your organization you will have either:

- Submitted a CSR and received a password protected **.pfx** file
- Used the Certificate Enrollment wizard to request a suitable Web Server certificate.

Note

In earlier versions of Tachyon the private key had to be exportable to create certificate files for Tachyon Switches, but this is no longer required for Tachyon 5.0 onwards.

1.4.1.4.5.2 Import the Web Server certificate

Once the Web Server certificate has been provided it must be imported into the Tachyon Server's local computer Personal Certificates store.

After importing, you should give the certificate a Friendly Name, so that you can easily identify it for the post-installation task Tachyon Server post-installation tasks.

1. On the Tachyon Server, start **certlm.msc** (or start mmc and add the certificates snap-in for the local machine).
2. Navigate to the **Personal Certificates** store.
3. Locate the Web Server certificate you have just imported.
4. Right-click on the certificate and select **Properties**.
5. In the **General** tab enter a Friendly name, for example, **1E platform**.
6. Click **OK** to save.

1.4.1.4.5.3 Web Server certificate specification

Each server that has Tachyon Server components installed requires its own Web Server certificate (except for a remote SQL Server). This certificate is also used by the Tachyon Switch and the Tachyon Coordinator. Therefore, a single-server installation requires only one Web Server certificate. This certificate must be provided on the server prior to the installation of Tachyon.

The Web Server certificate requires the minimum of the following:

1. Issued by a trusted Certificate Authority (CA)
   - The certificate for the Root CA in the Certification Path must exist in the Trusted Root CA store of the server
   - If the issuing CA is not the Root CA then the certificate for the issuing CA and any intermediate CA in the Certification Path must exist in the Intermediate CA store of the server
   - The above CA certificates must exist on the Tachyon Web Server and Windows client devices
   - Most organizations have automated distribution of these CA certificates to servers and clients, using Group Policy for example.
2. Has at least the following Key Usage:
   - Digital signature
   - Key encipherment
3. Has at least the following Enhanced Key Usages:
   - Server Authentication
4. Revocation information is included
   - References at least one CRL Distribution point that uses HTTP - see DMZ Server note below

5. Must have a private key available

Tip

The default template **Web Server** available with a Microsoft PKI is suitable for requesting a Tachyon Web Server certificate.

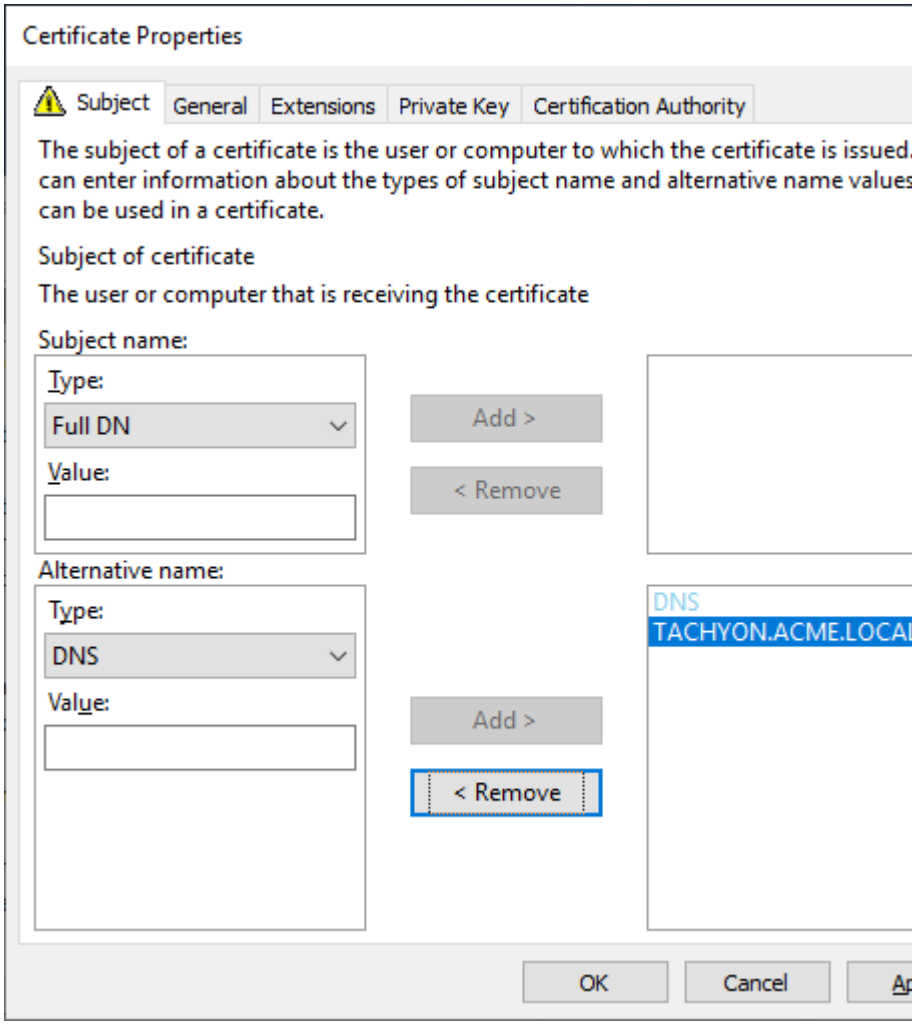
DMZ Server

Please ensure you note the additional certificate requirements described below, when installing any server in a system that also contains a DMZ Server. Internal Master and Response Stack servers, and DMZ Server, each requires **two** HTTPS bindings, as described in DNS Names. For details, please refer Implementing a Tachyon DMZ Server.

Also, note the requirement for server certificates to reference at least one CRL Distribution point that uses HTTP. These CRL DPs are likely to be in the internal network, and the firewall will need to allow the DMZ server to access these internal servers.

Web Server certificates used by Tachyon Servers must be issued with their fields set as follows. Example **DNS Names** are discussed in DNS Names.

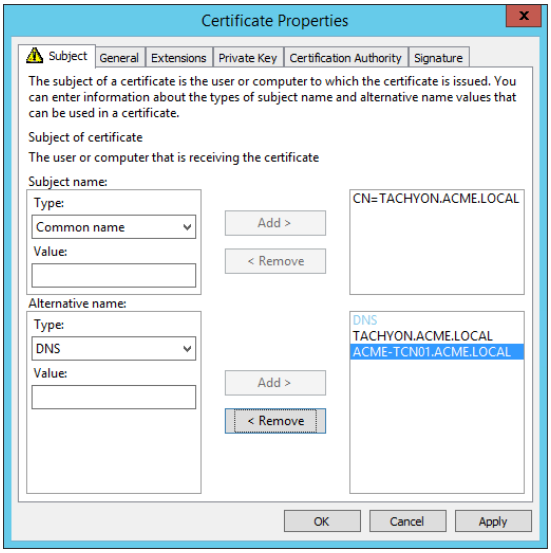
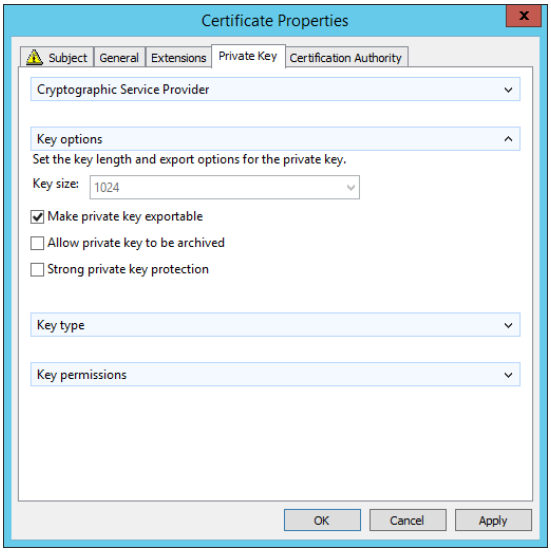
Fields	Example Option 3 type certificate
Subject Common Name Field (subject:commonName)	Subject (CN) can be any valid name and is no longer mandatory as required by previous versions of Tachyon.
Subject Alternative Name Extension (extensions:subjectAltName), type dnsName	The **Tachyon Server DNS Name FQDN** (DNS Alias) of the server. This is mandatory, the same as required by previous versions of Tachyon. On a Master Stack - example: **DNS Name=TACHYON.ACME.LOCAL** On a Response Stack - example: **DNS Name=TACHYONRS.ACME.LOCAL** On a DMZ Server - example: **DNS Name=TACHYONEXT.ACME.COM**
Subject Alternative Name Extension (extensions:subjectAltName), type dnsName	An **Alternate DNS Name FQDN** (DNS Alias) of the server. This is usually mandatory, for example if there is more than one server in your Tachyon system, as discussed in DNS Names. On a Master Stack, example: **DNS Name=TACHYONALT.ACME.LOCAL**or**DNS Name=TACHYON.ACME.LOCAL** On a Response Stack - example: **DNS Name=TACHYONALT.ACME.LOCAL**

Fields	Example Option 3 type certificate
Example	On a DMZ Server - example: **DNS Name=TACHYONDMZ.ACME.LOCAL** 

Note

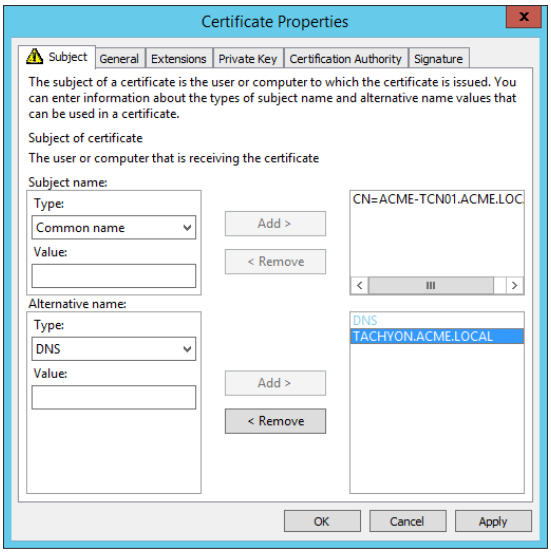
Earlier versions of Tachyon required the certificate to have a CN and used SAN fields differently. If you are upgrading your Tachyon server from an earlier version, it may still be using this type of certificate. When upgrading Tachyon, you can issue a replacement certificate, or continue using the old style certificate (because the new-style certificate requires only a SAN DNS Name that matches the DNS Alias, which are provided by the old style certificates).

Examples of old-style certificates.

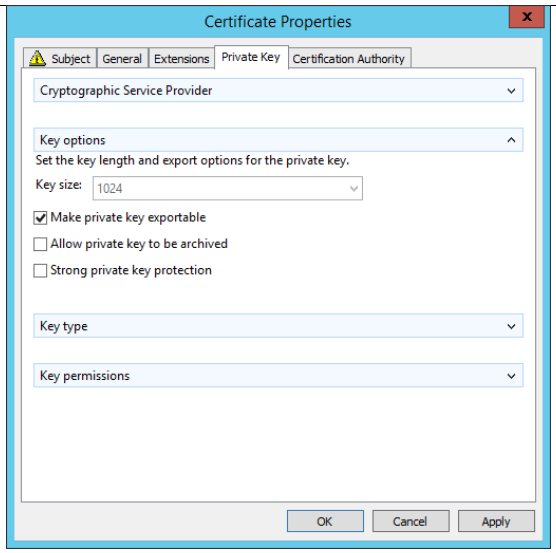
Fields	Example of old Option 1 type certificate
Subject Common Name Field (subject:commonName)	The DNS Alias FQDN of the server Example: **CN=TACHYON.ACME.LOCAL**
Subject Alternative Name Extension (extensions:subjectAltName), type dnsName	The DNS Alias FQDN of the server Example: **DNS Name=TACHYON.ACME.LOCAL** The computername FQDN of the server Example: **DNS Name=ACME-TCN01.ACME.LOCAL**
Example certificate request	 

Note

Fields	Example of old Option 1 type certificate
	Option 1 type certificates required the CN to be the DNS Alias, and the list of Subject Alternate Names (SAN) to contain the computername FQDN. Also, prior to Tachyon 5.0 the certificate required its private key to be exportable. Tachyon 5.0 and later is able to use this type of certificate when upgrading from an earlier version of Tachyon.

Fields	Example old Option 2 type certificate
Subject Common Name Field (subject:commonName)	The computername FQDN of the server Example: **CN=ACME-TCN01.ACME.LOCAL**
Subject Alternative Name Extension (extensions:subjectAltName), type dnsName	The DNS Alias FQDN of the server Example: **DNS Name=TACHYON.ACME.LOCAL** **Tip** Add any additional DNS Names here.
Example certificate request	

Fields	Example old Option 2 type certificate



Note

Option 2 type certificates required the CN to be the computername FQDN, and the list of Subject Alternate Names (SAN) to contain the DNS Alias.

Also, prior to Tachyon 5.0 the certificate required its private key to be exportable.

Tachyon 5.0 and later is able to use this type of certificate when upgrading from an earlier version of Tachyon.

1.4.1.4.5.4 Switch certificate files

Tachyon Switches use certificates in the Windows Certificate Store. From version 5.0 onwards they no longer use Switch Certificate files.

1.4.1.4.6 Windows Server roles and features

Note

Tachyon Setup will create a website with the necessary bindings, therefore please do not pre-create a website of the same name.

The following PowerShell commands can be used to install relevant IIS roles and features and record the server configuration in a file.

Note

When you run Tachyon Setup, you may choose to let the Setup perform this operation for you instead of downloading and running the script manually. Just click on the

Install missing prerequisites button after you have run the checks in the **Check prerequisites** page.

Click here to download - RolesInstall.ps1

RolesInstall.ps1 - Configure IIS using PowerShell

```
Import-Module ServerManager

Get-WindowsFeature | Out-file $PSScriptRoot\ServerManager-1.txt -Append
Install-WindowsFeature Web-Server,
Web-Http-Redirect,
Web-Dyn-Compression,
Web-Basic-Auth,
Web-IP-Security,
Web-Windows-Auth,
Web-Asp-Net45,
Web-Mgmt-Console,
Net-Framework-45-Core,
Net-Framework-45-ASPNET

Uninstall-WindowsFeature Web-DAV-Publishing

Get-WindowsFeature | Out-file $PSScriptRoot\ServerManager-2.txt -Append
```

Note

When running the above command, if you receive an error that contains **The source files could not be downloaded** you will need to supply the source path to your Windows Server OS installation media \Sources\sxs folder.

Append **-source X:\Sources\sxs** or **-source \\Server\Path\Source\sxs** to the command line, adjusted for your drive letter or UNC path.

Note

PowerShell always uses **45** in the names of .NET Framework features, irrespective of the actual version of .NET Framework 4.X installed on the server, like:

- 4.8 in Windows Server 2022 (note: from Tachyon 8.1 onwards, any Tachyon component that requires .NET Framework, requires version 4.8)
- 4.7.2 in Windows Server 2019
- 4.6.2 in Windows Server 2016

For details of .NET Framework versions, please refer to https://docs.microsoft.com/en-us/dotnet/framework/get-started/system-requirements#supported-server-operating-systems.

Tip

If you prefer to use the Add Roles and Features Wizard to manually enable features then you can use the Display Names listed in the table Windows Server roles and features.

Note

Web-Http-Redirect is only required to support legacy Nomad clients after an In-place upgrade of ActiveEfficiency Server for Nomad.

Web-Basic-Auth is only required if you will be installing 1E ITSM Connect or 1E Core for integrating ServiceNow and Tachyon.

1.4.1.4.7 ASP.NET Core Hosting Bundle

This is required on the Tachyon Master Stack server if you are installing Content Distribution features.

If it is not already installed, Tachyon Setup will attempt to automatically download and install version **3.1.1**. However, this supposes your installation account and the server is whitelisted to allow download from https://download.visualstudio.microsoft.com/download/pr/d8b046b7-c812-4200-905d-d2e0242be9d5/53d5698d79013be0232152ae1b43c86b/dotnet-hosting-3.1.11-win.exe.

If you want to download it yourself, or a later version, then go to https://dotnet.microsoft.com/download/dotnet and then install it using a command similar to the following:

dotnet-hosting-3.1.11-win.exe OPT_NO_X86=1 /install

The parameter ***OPT_NO_X86=1*** causes the installer to only install the 64-bit version, which is what Tachyon requires.

You may experience an error if some bundle components are already installed. If this happens, then re-run using ***/repair*** instead of ***/install*** .

Note

You can run the following command to list the installed versions of .NET

%ProgramFiles%\dotnet\dotnet.exe --list-runtimes

1.4.1.4.8 If TLS1.0 is disabled

1.4.1.4.8.1 Web server registry settings

If TLS 1.0 is disabled on the Web server, you must add the following two registry entries, for the 1E Catalog Update Service to successfully connect to the 1E Cloud Catalog.

Import registry entries

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\.NETFramework\v4.0.30319]
"SystemDefaultTlsVersions"=dword:00000001

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319]
"SystemDefaultTlsVersions"=dword:00000001
```

1.4.1.4.9 SQL BCP

The **Export all** feature is described in Exporting data from Explorer. To enable Tachyon users with the appropriate permissions to use the **Export all** feature you must ensure that **Microsoft Bulk Copy Program (BCP)** is installed on each **Tachyon Response Stack**, specifically the Response server where the Core component is hosted.

- If Microsoft SQL Server is installed on the same server as the Tachyon Response Stack, then BCP will normally be present.
- If the TachyonResponses database is remote to the Tachyon Response Stack and there is no local copy of Microsoft SQL Server, then you will need to install BCP.

You can confirm BCP is installed by starting a command prompt and typing **bcp** and usage information is displayed. The command **bcp -v** displays the version.

> **Note**
>
> The information here applies regardless of which version of SQL Server is being used. This does not imply that Tachyon itself is supported under every possible version of SQL Server that falls within those ranges. See Windows Server requirements for the supported versions and required Service Packs.

Install the following components to get BCP working:

Installer file name	Product Name	Where to get it from
vc_redist.x64.exe	Visual C++ 2017 Redistributable	https://support.microsoft.com/en-gb/help/2977003/the-latest-supported-visual-c-downloads
msodbcsql.msi	Microsoft® ODBC Driver 13.1 for SQL Server®	https://www.microsoft.com/en-us/download/details.aspx?id=53339 This needs to be installed because of a known issue in the Microsoft Command Line Utilities 15 for SQL Server.
msodbcsql.msi	Microsoft® ODBC Driver 17 for SQL Server®	https://docs.microsoft.com/en-us/sql/connect/odbc/download-odbc-driver-for-sql-server Use version 17 (x64).
MsSqlCmdLnUtils.msi	Microsoft Command Line Utilities 15 for SQL Server	https://docs.microsoft.com/en-us/sql/tools/bcp-utility The msi includes **BCP** and **SQLCMD**.

To verify the components have been installed, you can use **AppWiz.cpl** and check for the **Product Name**.

1.4.1.4.10 Services and NTFS Security

Tachyon and SLA Platform services, including web application pools, use built-in accounts Local System (SYSTEM) and Network Service (NETWORK SERVICE) by default, and 1E recommends this configuration.

You must ensure these built-in accounts have the necessary NTFS security permissions on the Tachyon and SLA Platform installation and log folders.

If you are using default installation settings for the Tachyon server on a default configuration of Windows Server, then **Local System** has the necessary permissions by default, but **Network Service** requires some additional steps. The simplest method is to add **Network Service** to the **Administrators** localgroup, which allows the default installation and logs folders to be created during installation.

However, adding Network Service to the **Administrators** localgroup is not considered best practice, therefore alternative methods are described below.

The table below lists the Tachyon services and their default service accounts.

Tachyon service	Service account name	Description	SID
Tachyon Switch Host service	NT AUTHORITY\SYSTEM	Local System	S-1-5-18
1E Catalog Update Service 1E SLA Platform services (3) 1E Tachyon Coordinator service Web application pools: • Catalog (1) • SLAPlatform (3) • Tachyon (5)	NT AUTHORITY\NETWORK SERVICE	Network Service	S-1-5-20

The table below lists the default folder locations which must have NTFS security permissions configured for all service accounts.

The Tachyon installation process does not modify permissions, except for the %ProgramData%\1E\Licensing\ folder which *does* receive full permissions for Network Service.

Folder	Default location	Service account	NTFS security
Installation folders	%ProgramFiles%\1E\Catalog\ %ProgramFiles%\1E\SLA Platform\ %ProgramFiles%\1E\Tachyon\	Network Service SYSTEM	Minimum of **read & execute** permission (**folder, subfolders and files**).

Folder	Default location	Service account	NTFS security
Logs folders	%ProgramData%\1E\Catalog\ %ProgramData%\1E\DatabaseUpgrade\ %ProgramData%\1E\Licensing\ %ProgramData%\1E\Platform Consumer\ %ProgramData%\1E\SLA Platform\ %ProgramData%\1E\Tachyon\	Network Service SYSTEM	Minimum of **Full Control** permission (**folder, subfolders and files**).

For a default installation of Tachyon on a default configuration of Windows Server, **Local System (SYSTEM)** has the necessary permissions by default, but **Network Service** requires some additional steps.

You have a choice of how to configure NTFS security for **Network Service**, using one of the following options, according to your organization's policies.

You can pre-create the Tachyon installation and logs folders prior to installation and apply NTFS permissions on these instead of their parent folders.

Choice	Method
Administrators localgroup	Add NETWORK SERVICE to the **Administrators** localgroup (this is the simplest method but not best practice).
Users localgroup	Add NETWORK SERVICE to the **Users** localgroup, and grant this group permissions on the folders. • Default **INSTALLDIR** does not need to be modified because **Users** localgroup has inherited **read & execute** permission • Default **LOGPATH** requires the inherited **Users** localgroup to be modified to give **Full Control** permission
Direct permissions	As above, but grant NETWORK SERVICE direct rights on the folders

Note

The Tachyon Server Installation Account should be a member of the **Administrators** localgroup, so that it has full rights on the server.

1.4.1.4.10.1 Using a non-default location for the Installation Folder

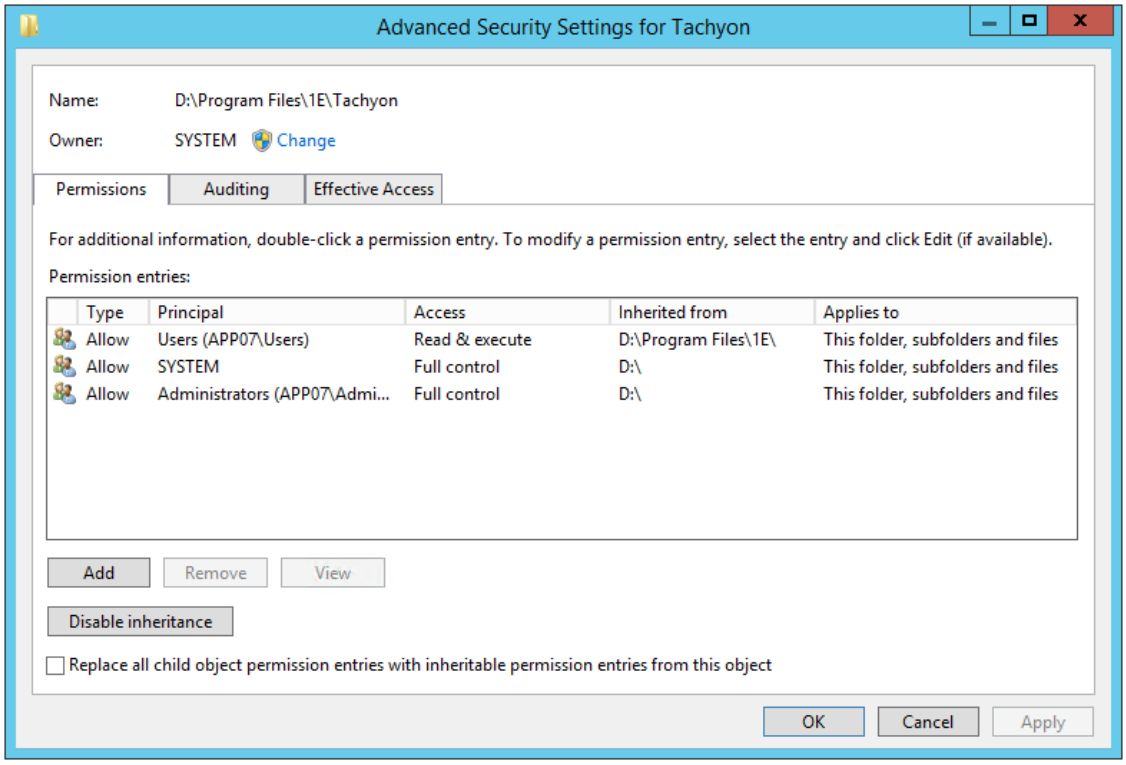
If you are installing in a non-default installation folder, or the default installation folder has non-standard NTFS security, then before installation, you must ensure the installation folder is pre-created with suitable NTFS security applied. If this is not done, some services will fail to start, or users will not be able to access the website.

The NTFS security for the service accounts described above must be explicitly applied.

In addition, the **Users** or **Authenticated Users** localgroup must have a minimum of **read & execute** permission on each of the Web application folders (**folder, subfolders and files**). This is simplest to achieve by granting permission on the INSTALLDIR folder.

The example screenshot shows:

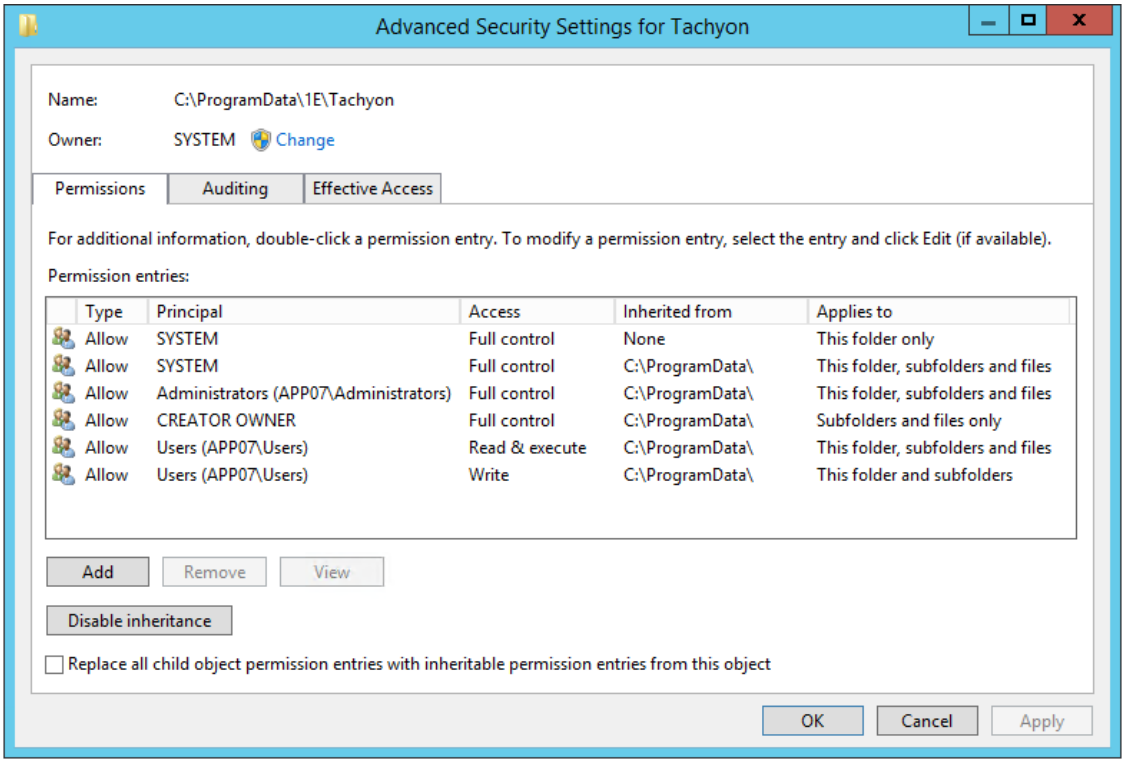
- A non-default installation INSTALLDIR=D:\Program Files\1E\Tachyon\
- RX permissions for the Users group is applied to the 1E folder
- Other permissions are inherited from the root of the D: drive
- INSTALLDIR permissions are inherited from the 1E folder
- NETWORK SERVICE is a member of the **Users** localgroup



1.4.1.4.10.2 Using a non-default location for the Logs Folder

The accounts used by Tachyon services and application pools must have a minimum of **Full Control** permission on the logs folder (**folder, subfolders and files**.

The example screenshot shows a default installation. For a default installation, the only permissions necessary are SYSTEM and Administrators, both Full Control.



1.4.1.5 SQL Databases

Tachyon platform databases can be installed on one or more SQL Server database instances. These SQL Server instances can be on the Tachyon application server (local) or remote. You can allow the Tachyon Setup to create the databases in their default locations, or you can pre-create them with appropriate permissions before installation if you want to select the location and sizes of the databases. For a new installation, and for upgrades, the Installation Accounts requires a SQL Login with appropriate permissions.

Please refer to High Availability options for SQL Server.

Tachyon platform supports the following High Availability (HA) options for SQL Server:

- AlwaysOn Availability Group (AG) using an AG Listener
- Failover Cluster Instance (FCI).

The following is a list of databases used by Tachyon platform. In the Database servers screen, you can select the name of the SQL Server instance, but it does not let you change the database names.

- 1ECatalog
- SLA databases must be installed on the same instance:
  - SLA-Data

  - SLA-Shared
  - SLA-Integrate.

- ContentDistribution (required for Nomad)
- SLA-BI (this is the Business Intelligence database required for Patch Success)
- TachyonMaster
- TachyonResponses (required for a Response Stack)
- TachyonExperience (required for Experience).

The following is a list of database cubes used by Tachyon platform. In the SSAS servers screen, you can select the name of the SQL Server instance, but it does not let you change the database names.

- SLA-BI (this is the Business Intelligence cube required for Patch Success).

1.4.1.5.1 Default configuration of databases

If you allow the installer to create new databases, they each have the following default settings. Databases will grow automatically to the sizes estimated in /document/preview/791302#UUID-aa1c2691-97ed-e134-ac7d-62b2ea04fe4a.

Property	Value
Owner	If the Installer is used to create the databases, this will be the Tachyon Server Installation Account . The best practice is to change the owner to 'sa' as shown in, Example SQL scripts for creating a SQL Login and granting roles.
Collation	SQL_Latin1_General_CP1_CI_AS
Path	Default SQL location
Initial Size MDF	128MB
Autogrowth MDF	By 128MB
Initial Size LDF	128MB
Autogrowth LDF	10%

Property	Value
Recovery Model	Simple

Note

If the **model** system database has been changed to have a larger size than the values specified in the table above, then the Tachyon Server installer may report an error executing 'Bootstrap.sql' on MasterDatabase. Rebooting the SQL Server may cure the error.

1.4.1.5.2 Creating your own databases

You may be required to create databases by hand before installation. This is also known as pre-creating databases. Below are some of the reasons why your SQL administrator may require you to do this:

- Tachyon Server Installation Account is only allowed rights on existing databases and not allowed rights to create them
- Locations of the database files need to be different from the defaults used on the SQL Server instance(s)
- The initial size of the database files needs to be set to their estimated full size given in /document/preview/791302#UUID-aa1c2691-97ed-e134-ac7d-62b2ea04fe4a.

1.4.1.5.3 SQL Login for the server installation account

The server installation account requires SQL permissions during installation and upgrade, which can be temporary or permanent. The level of SQL permissions required by the installation account depends on which Tachyon components it is installing.

1.4.1.5.3.1 Master Stacks

For master stacks **sysadmin** is required as follows, to:

- Install **1E Catalog**
- Create Linked Servers for **SLA,** which requires **sysadmin** for the SQL database instances for both SLA and 1E Catalog databases
- Create Linked Servers for **BI**, which requires **sysadmin** for the SQL database instances for both SLA and BI databases, and the SSAS instance for the BI cube (required only by Patch Success).

1.4.1.5.3.2 Response Stacks

Sysadmin availability on SQL instance(s)	SQL Login permissions
sysadmin SQL Server role is permitted	The server installation account requires the **sysadmin** SQL Server role on the SQL Server instance(s) that host the TachyonMaster and/or TachyonResponses database(s). This can be used for a new installation, or for an upgrade.
sysadmin SQL Server role is not permitted	The SQL Login permissions required by the server installation account vary depending on which choice is implemented, as described in the following table:

Choice implemented	Role required for the installation account's SQL Login
Database(s) created by the Tachyon Server installer *during* installation.	**dbcreator** SQL Server role on the SQL instance
Database(s) created *before* installation - a common scenario if you want to select database location and size. Also required when upgrading Tachyon.	**db_owner** database role on the pre-created databases: • **TachyonResponses**

Note

In addition to the permissions given in the table above, the server installation account also needs to **ALTER ANY LOGIN** Securables permission in order to allow the creation of the Example SQL scripts for creating a SQL Login and granting roles, used by the Tachyon Server web applications and services.

Example scripts are provided below to create a SQL Login and grant roles.

During installation, the Tachyon Server installer will **always** attempt to grant **db_owner** permission to the server installation account on each of the Tachyon databases.

Note

Databases must be configured in multi-user mode.

1.4.1.5.4 Example SQL scripts for creating a SQL Login and granting roles

The following examples assume **ACME\TCNinstaller01** is the Tachyon Server Installation Account.

When the account is not permitted to have the **sysadmin** SQL Server role, then a sysadmin can use the following script to create a SQL Login and grant it rights.

Create SQL Login and grant ALTER ANY LOGIN Expand source

```
USE [master]
GO
CREATE LOGIN [ACME\TCNinstaller01] FROM WINDOWS
GO
GRANT ALTER ANY LOGIN TO [ACME\TCNinstaller01]
GO
```

If the Tachyon Server Installation Account is permitted to create the databases, then a sysadmin can use the following script to add the SQL Login to the **dbcreator** role.

Grant dbcreator Expand source

```
USE [master]
GO
ALTER SERVER ROLE [dbcreator] ADD MEMBER [ACME\TCNinstaller01]
GO
```

If the databases have been pre-created, then a sysadmin can use the following script to add the SQL Login to the **db_owner** role on each pre-created database.

Grant db_owner Expand source

```
USE [TachyonMaster]
GO
CREATE USER [ACME\TCNinstaller01] FOR LOGIN [ACME\TCNinstaller01];
ALTER ROLE [db_owner] ADD member [ACME\TCNinstaller01];
GO
USE [TachyonResponses]
GO
CREATE USER [ACME\TCNinstaller01] FOR LOGIN [ACME\TCNinstaller01];
ALTER ROLE [db_owner] ADD member [ACME\TCNinstaller01];
GO
```

After the databases have been created, best practice is to change the **owner** of each database to **sa**, to avoid issues if the owner's Windows account is deleted in future.

The following script can be used to change the **owner** of each Tachyon database to **sa**. This will work even if the **sa** login has been disabled, which is also best practice.

Change owner to 'sa' Expand source.

```
ALTER AUTHORIZATION ON DATABASE::TachyonMaster To "sa"
GO
ALTER AUTHORIZATION ON DATABASE::TachyonResponses To "sa"
GO
```

Note

Ensure the Tachyon Server Installation Account retains the **db_owner** role on the database to support re-configuration and upgrades. If the account is removed from being **owner**, then it will also be removed from the **db_owner** role and will need to be re-assigned, for example by using the **Grant db_owner** SQL script.

The **owner** user and **db_owner** role are both mapped to the database **dbo** user. It is preferable for the account to be a member of the **db_owner** role, instead of being the **owner** user.

1.4.1.5.5 SQL Login for the Tachyon service account

The SQL Login that is used by the Tachyon Server web applications and services depends on whether the SQL Server is remote from the Tachyon Server or is local, as described in the following table:

Installation scenario	Service account SQL Login
Tachyon Server is remote from SQL	The computer account of the remote Tachyon Server. For example **ACME\ACME-TCN01$**
Tachyon Server and SQL are local	The local network service account, **NT AUTHORITY\NETWORK SERVICE**

Note

Before upgrading Tachyon, or installing or upgrading Consumer applications like Application Migration or AppClarity, the SQL Login must be granted the following rights to support Database Snapshot of the 1E Catalog and SLA databases, to restore them if an error occurs:

- **dbcreator** rights on the SQL database instance hosting the 1E Catalog database.
- **dbcreator** rights on the SQL database instance hosting the SLA databases.

During installation, the Tachyon Setup will **always**:

- Attempt to create the SQL Login
- Grant it **db_owner** permission on each of the Tachyon databases
- Remove the **db_owner** permissions when installation is completed.

1.4.1.5.6 Keeping databases during re-installation and upgrade

If re-installing or upgrading Tachyon, you need to decide if you will keep the existing databases or create new ones.

Note

Before doing a re-installation or upgrade of the Tachyon Platform, make a backup of the following (but first see the note below about automatic backups):

- Tachyon Master database

  Note

  Backing up the Tachyon Responses database is **not** usually needed, unless there are instruction responses that you need to keep. Tachyon responses are not permanently held data and will naturally expire according to the settings specified when an instruction was run, typically in hours or possibly days. If in doubt, there is no harm in backing up the Tachyon Responses database as well.

- Tachyon Server installation directory.
  - including the config files, which may have been manually updated in the previous installation.
  - Switch certificate files.
- Earlier versions of Product Packs that have been modified.

Note

Tachyon Setup will automatically perform a backup of the following items:

- Tachyon Server installation directory. This is backed up to a subfolder named Tachyon.bak under the root installation folder for Tachyon . All files, including the .config files and certificate files, will be copied.
- IIS configuration. This is done by taking a copy of the applicationhost.config file from the Windows system folders. The backup file is placed at the same location and is named like the original file with a suffix that indicates the date and time when the copy was taken.
- The following databases are backed up to the default location for backups that is configured in the database server. By default, this points to a subfolder named "Backups" under the folder where the executable for SQL Server is installed. Unless you are installing a small lab or proof-of-concept, this is usually *not* a good location for the backups, so make sure that you configure the backup location in SQL Server to an adequate folder before starting the Tachyon upgrade:
  - 1ECatalog
  - ContentDistribution (optional, required by Nomad)
  - SLA-Data
  - SLA-Shared
  - SLA-Integrate
  - TachyonMaster
  - TachyonResponses
  - TachyonExperience (optional, required for Experience).

The Product packs are not copied by themselves, but they are kept in a table within the TachyonMaster database, which *is* backed up.

1.4.1.6 SSAS Databases

If Business Intelligence is selected for installation, then you will need to provide an instance of SQL Server Analysis Services (SSAS) configured in Multidimensional (*not* Tabular) mode.

Make sure that the SSAS instance is enabled, reachable, configured in Multidimensional mode, and the Server installation account has sufficient permissions. The Setup program is not able to perform a full validation of the SSAS server, so you need to ensure a proper configuration during the preparation phase.

Business Intelligence is a component required by Patch Success and requires a **BI SSAS user**.

The **BI SSAS User** account has the following requirements:

- The account name and its password will be specified in the SSAS servers screen.
- Must be a **domain user account**
  - Configured with **Password never expires**
  - Although this user might be referred to as a service account, it does not require **Logon as a service** on the server.
- During installation, the SLA BI installer (used by Tachyon Setup) does the following with the user account:
  - Stores its credentials encrypted in the following places:
    - A linked server connection for the BI database to access the BI cube
    - In the configuration file used by the MDX API to query the BI cube.
  - Creates a SQL Login, with rights on the SLA-BI database.

Note

Prior to Tachyon 8.1, Experience required its own SSAS database.

This is no longer necessary. If you are upgrading to Tachyon 8.1 or later, then you can delete the Experience SSAS database after the upgrade is completed.

1.4.1.7 Email

Tachyon users and approvers require AD accounts with email addresses to support approval workflow and notifications.

1.4.1.7.1 Mail Server

For details about mail server requirements, please refer to SMTP server.

1.4.1.8 Active Directory

Tachyon Server must be installed on a domain-joined server, except for a DMZ Server, where this is optional. Clients do not have to be installed on domain-joined devices but must have a certificate.

1.4.1.8.1 Installation Accounts

1.4.1.8.1.1 Tachyon Server Installation Account

The server installation account has the following requirements on the server.

- **Local admin rights on the Tachyon Server**. It must be an Active Directory domain user account that is a direct or indirect member of the Administrators local group on the server where Tachyon Server will be installed.
- Can be disabled (not deleted) in Active Directory after additional Tachyon admin users have been created in Tachyon , and installation has been verified.

In addition, the server installation account requires SQL rights as described in SQL Databases above.

1.4.1.8.1.2 Tachyon client Windows Installation Account

The 1E Client installer installs a service as local system, therefore the installation account for Windows clients must be capable of being elevated in order to run the installer. The simplest way of achieving this is for the account to have full local administrator rights (as a member of the localgroup administrators, either directly or indirectly).

1.4.1.8.1.3 Tachyon client Non-Windows Installation Account

To install the 1E Client on a non-Windows client the installation account must have privileges to run the **sudo** command.

1.4.1.8.2 Tachyon Users Accounts

Each Tachyon user requires an account in the Identity Provider used. All accounts must have their userPrincipalName (UPN) attribute populated, which is normal, but may be missing if users accounts have been created using scripts.

Tachyon users and approvers should have email addresses to support approval workflow and notifications. Email addresses are mandatory if Two-factor Authentication is enabled.

Groups that are setup in the Identity Provider are recommended for role-based access control (RBAC) within Tachyon but are not mandatory. Groups can be assigned to Tachyon roles after installation, they are not required during installation. They are added as Tachyon groups and configured in the same way as user accounts. A Tachyon user can therefore be a user account or in a group within the Identity Provider. Groups are not mandatory because users can be assigned to roles and managed within Tachyon instead of the Identity Provider, or a combination.

Tachyon Setup assigns a limited set of permissions to the Setup user account (specified during installation/updates), as described on the Roles page which cannot be edited. It is possible to increase this user account to have Full Administrator access during installation/upgrade, 1E recommend that this user account is viewed as a service account and kept with the minimum permission.

A group is also useful to configure access to the CatalogWeb Admin page, as described in Rebuilding the 1E Catalog .

Note

AD *distribution* groups are not supported.

If AD *security* groups are nested (groups within groups), they can slow down the performance of the Tachyon Portal for administrators. Therefore, we recommend nesting is not used, and each administrator and approver account is a member of a group used in Tachyon . You can improve performance further by disabling the recursive search used by Tachyon , bearing in mind this will not support nested groups. Please refer to the Post Installation page.

Domain Local security groups are not supported.

1.4.1.8.3 Service accounts

Tachyon platform uses either **Network Service** or **Local system** for all its services and web application pools.

Please refer to the following sections regarding any rights these accounts may require:

- Service Principal Names
- Services and NTFS Security
- SQL Login for the server installation account
- SQL Login for the Tachyon service account
- Microsoft Endpoint Configuration Manager preparation.

1.4.1.9 Microsoft Endpoint Configuration Manager preparation

Tachyon platform requires permission to access various features of Configuration Manager when you implement any of the following optional features:

- Nomad
- System Center Configuration Manager connector.

1.4.1.9.1 Configuring SQL rights in the Configuration Manager database

The Network Service account of the Tachyon Master Stack server requires a SQL Login, with **all** the following rights in the Configuration Manager site database.

- **db_datareader** database role
- Explicit *Execute* permissions to the scalar value function **fn_GetAppState**
- Explicit *Execute* permissions to the scalar value function **fnGetSiteNumber**.

1. If the connector is using **Windows Authentication**, then you can use **one** of the following:

a. Create a SQL Login for the **Tachyon server's computer$ account**, and explicitly grant it the above rights.

b. Add the **Tachyon server's computer$ account** to the **ConfigMgr_DViewAccess** localgroup on the Configuration Manager database server - this is the preferred method.

Note

You may already be familiar with configuring **ConfigMgr_DViewAccess** if you have previously set up Configuration Manager access for older versions of Nomad Dashboard which used **ActiveEfficiency Server**, or the **ActiveEfficiency Scout**, as used for AppClarity 5.x or Shopping 5.x and 6.0

The existence of the **ConfigMgr_DViewAccess** localgroup depends on the version of Configuration Manager. It should exist for a Primary Site, but may not exist for a CAS. If it does not already exist, it is safe for you to manually create the localgroup on the SQL Server used by the Configuration Manager database. If it already exists, you will need to confirm it has a SQL Login and all the necessary rights, as the Configuration Manager setup does not always configure this group correctly.

The following SQL script can be used to create a SQL Login for **ConfigMgr_DViewAccess** and grant it permissions on the Configuration Manager database. Before you run the SQL script, you must first:

- Manually create the localgroup on the SQL Server
- Add the **Tachyon server's computer$ account** to the localgroup.

Click here to download - ConfigMgr_DViewAccess_permissions.SQL

```
-- Connect to the SQL instance using an account that has sysadmin r
ights.
-- Execute this SQL script on the Configuration Manager database.
-- The script creates a SQL Login on the instance for [hostname\Con
figMgr_DViewAccess]
-- and grants it the following rights on the Configuration Manager
database:
-- [db_datareader]
-- EXECUTE on [dbo].[fn_GetAppState]
-- EXECUTE on [dbo].[fnGetSiteNumber]

DECLARE @SqlLogin nvarchar(2000)
DECLARE @SqlString nvarchar(max)

SET @SqlLogin = CAST(host_name() AS varchar(512)) + '\ConfigMgr_DVi
ewAccess'
PRINT 'Granting permissions for ''' + @SqlLogin + ''' on database '
+ DB_NAME() + ' ...'

SET @SqlString = '
IF NOT EXISTS ( SELECT schema_name FROM information_schema.schemata
WHERE schema_name = '''+@SqlLogin +''' )
```

```
EXEC (''CREATE SCHEMA [' + @SqlLogin + ']'')
'
EXEC sp_executesql @SqlString

SET @SqlString = '
IF NOT EXISTS (SELECT * FROM sys.server_principals WHERE name = '''
+ @SqlLogin +''')
CREATE LOGIN [' + @SqlLogin + '] FROM WINDOWS WITH DEFAULT_DATABASE
=[master]
'
EXEC sp_executesql @SqlString

SET @SqlString = '
IF NOT EXISTS (SELECT * FROM sys.database_principals WHERE name = '
''+ @SqlLogin +''')
CREATE USER [' + @SqlLogin + '] FOR LOGIN [' + @SqlLogin + '] WITH
DEFAULT_SCHEMA=[' + @SqlLogin + ']
'
EXEC sp_executesql @SqlString
PRINT 'SQL Login created.'

SET @SqlString = '
ALTER ROLE [db_datareader] ADD MEMBER [' + @SqlLogin + ']
GRANT EXECUTE ON [dbo].[fn_GetAppState] TO [' + @SqlLogin + '] AS [
dbo]
GRANT EXECUTE ON [dbo].[fnGetSiteNumber] TO [' + @SqlLogin + '] AS
[dbo]
'
EXEC sp_executesql @SqlString
PRINT 'Permissions granted.'
```

When you run Tachyon Setup, the Nomad screen will attempt to validate the existence of the **ConfigMgr_DViewAccess** localgroup and membership of the Nomad server's computer$ account. The validation test will fail if the installation account does not have sysadmin rights on the SQL Server instance used by Configuration Manager. This is not a fatal error as long as you are sure the computer$ account is a member of the **ConfigMgr_DViewAccess** localgroup.

If you opt to use a specific SQL Login:

1. If the connector is using a **SQL Login**, then create the login on the Configuration Manager database and grant it the above rights.

To install Nomad features, Tachyon Setup requires your **server installation account** to have the following rights. Please refer to Tachyon Setup.

- **Read-only Analyst** rights in Configuration Manager Console - so that Setup can query the Site Server for details of the Configuration Manager database.

- SQL Login (with public role) on the SQL database instance that hosts the Configuration Manager database - so that Setup can run a SQL query to validate that the machine account is a member of the **ConfigMgr_DViewAccess** localgroup on the SQL Server.

Note

If either of the above rights are not provided then Setup will issue a warning to say it was not possible to verify the machine account is a member of the **ConfigMgr_DViewAccess** localgroup.

1.4.1.9.2 Configuring Site Settings in Configuration Manager

You must enable certain Configuration Manager site settings if you plan to use the System Center Configuration Manager connector to populate Inventory.

The following **Client Settings** must be configured to gather inventory and usage data from clients, and applied to relevant Collections containing in-scope devices:

- Software metering (metering rules are not necessary)
- Software inventory
- Hardware inventory

The following **Discovery Methods** must be configured to gather Active Directory data about clients, and applied to relevant Domains and OUs containing in-scope devices:

- Active Directory System Group Discovery (default attributes are sufficient)

1.4.1.10 Tachyon client devices preparation

Please ensure devices that will be used to validate and test the Tachyon installation has the following.

- Be a supported device platform, (refer to 1E Client requirements), capable of having the installed
- Have appropriate scripting support - please refer to Tachyon scripting requirements
- Have a computer certificate (refer to Tachyon client certificate requirements) suitable for use by the Tachyon platform client features of 1E Client.

1.4.1.10.1 Tachyon integration with Nomad on Windows devices

1.4.1.10.1.1 Configuration Manager present

You do not need to make any configuration changes to Nomad for it to integrate with Tachyon. Please refer Introducing Nomad for guidance on designing and deploying Nomad.

1.4.1.10.1.2 Configuration Manager not present

You can deploy Nomad to Windows devices where the Configuration Manager client is not present. You will need to enable the following bits in relevant installer properties:

- CompatibilityFlags bit 1 - enable long hashes

- SpecialNetShare bit 13 - enable HTTP(S)

These are enabled by default in the Nomad client module of the 1E Client.

1.4.1.10.2 Tachyon client certificate requirements

If you have configured Tachyon Server to require client certificates (Client certificates) then each device requires a certificate with the following properties, so the client can be authenticated by the Tachyon Switch.

1. Issued by a trusted Certificate Authority (CA)
   - The certificate for the Root CA in the Certification Path must exist in the Trusted Root CA store of the client.
   - If the issuing CA is not the Root CA then the certificate for the issuing CA and any intermediate CA in the Certification Path must exist in the Intermediate CA store of the client.
   - If either of these CA certificates is different from those used by the Tachyon Web Server, they will need to be exported and imported on the Tachyon Web Server.
   - Most organizations have automated distribution of these CA certificates to clients and servers, using Group Policy for example.
2. Has at least the following Enhanced Key Usage.
   - Client Authentication.
3. Has at least the following Key Usage.
   - Digital Signature
   - Key encipherment.
4. Has a private key.
   - For workgroup and non-Windows devices, the **private key must be exportable**.
5. Revocation information is included.
   - References at least one CRL Distribution point that uses HTTP.
6. Has a Subject Name of type Common Name (**CN=<computername>**) or Subject Alternative Name (**DNS Name=<computername>**) where <computername> depends on the type of device:
   - On domain-joined Windows PCs this must be the **computername FQDN** of the computer, for example **W701.ACME.LOCAL**.
   - On workgroup Windows PCs and non-Windows devices, this must be the computername of the computer - as returned by the **hostname** command, for example on Windows PC this could be **W701**, and on a Mac this could be **MAC01.local**.

Note

Tachyon clients and Switches use OpenSSL and its validation process to verify certificates.

In organizations that have an established PKI, the client devices will probably have a suitable certificate already, along with relevant Trusted Root CA certificates.

For non-Windows devices, the certificate files must be included in the 1E Client installation folder structure, as described below in Configuring the Non-Windows Tachyon certificate using OpenSSL.

1.4.1.10.2.1 Certificate Authority (CA) public keys

Tachyon clients need to authenticate Switches and Switches need to authenticate Tachyon clients. In each case, one end of a secure connection requires the public key for each CA in the other end's certificate certification path (trust chain).

The Tachyon client needs the public key of each CA in the Switch's certification path. These public keys are stored differently on the client device depending on the type of OS.

- For Windows devices, CA public keys are normally stored in the Windows Trusted Root Certification Authorities store.
- For non-Windows devices, CA public keys are stored in a **cacert.pem** located in the 1E Client installation folder.
- For macOS devices, you have a choice of storing CA public keys in the macOS KeyStore or using the cacert.pem file approach required by other non-Windows devices.

The following points should be noted for Windows devices:

- If each client device has an identical certification path as the Switch, then its CA certificates (public keys) will probably already exist in the Windows Trusted Root Certification Authorities store. This is a typical situation in a small-scale lab with a simple PKI.
- If any client device has a different certification path then the certificates (public keys) of the different CAs will need to be added to the corresponding certificate store on Windows devices, either Trusted Root Certification Authorities or Intermediate Certification Authorities.
- In each of the above cases, the CA certificates (public keys) may have been deployed by Group Policy.

Note

If any of these CAs has its certificate renewed or re-issued then:

- The appropriate Certification Authorities store will need to be updated on the Tachyon Server and Windows devices. Most organizations have automated processes for this task.
- An updated **cacert.pem** file must be distributed to non-Windows devices. This should include old and new keys to aid with the transition.

1.4.1.10.2.2 Configuring the Non-Windows Tachyon certificate using OpenSSL

Each non-Windows device requires its own certificate. Below is a guide for using a Microsoft CA to issue a certificate (which is the same for Windows computers), then exporting it and using OpenSSL to prepare it before installing it on a non-Windows device.

First, you will need to have created a new Certificate template on your Certificate Authority by making a duplicate of either the Computer or Workstation template and configuring it with at least the following properties:

- **General** - use a suitable name such as Tachyon **Devices** and validity period
- **Request Handling** - Allow private keys to be exported
- **Subject Name** - Allow information to be supplied in the certificate request, rather than being built from Active Directory information
- **Extensions** - Application Policies should contain only Client Authentication
- **Security** - ensure relevant users and computers will be able to request certificates.

Once the new template is created on the CA, issue it.

Using the issued template, request a certificate for a target device, export it in **.pfx** form and remember the password.

The target device requires a copy of the basic **cacert.pem** and the **.pfx** file with its password removed. You can do this using the following steps. Use the relevant OpenSSL version for the OS. OpenSSL is normally available by default on Linux and Mac devices. If you want to follow these steps on Windows, you will need to download the open-source version appropriate to your OS.

1. First, extract the certificate:

   ```
   openssl pkcs12 -clcerts -nokeys -in <YourPKCSFile>.pfx -out certificate.c
   rt
   ```

2. Second, the CA key:

   ```
   openssl pkcs12 -cacerts -nokeys -in <YourPKCSFile>.pfx -out ca-cert.ca
   ```

3. Now, the private key:

   ```
   openssl pkcs12 -nocerts -in <YourPKCSFile>.pfx -out private.key -passout
   pass:TemporaryPassword
   ```

4. Remove the passphrase:

   ```
   openssl rsa -in private.key -out new.key -passin pass:TemporaryPassword
   ```

5. Put things together for the new PKCS-File (on Windows, **type** can be used instead of **cat**):

   ```
   cat new.key > PEM.pem
   cat certificate.crt >> PEM.pem
   cat ca-cert.ca >> PEM.pem
   ```

6. And create the new **.pfx** file, when prompted for a password ensure that you enter an empty password (that is press enter when prompted for the password and confirmation without entering any text):

```
openssl pkcs12 -export -nodes -CAfile ca-cert.ca -in PEM.pem -out Tachyon
.pfx
```

Now you have a new PKCS12 key file without a passphrase on the private key part. This **Tachyon.pfx** file and the **cacert.pem** file, must be placed in one of the following locations - depending on the OS. These are hidden folders.

On Linux and Solaris:

```
/etc/1E/Client/.sslcerts
```

On Mac:

```
/Library/Application Support/1E/Client/.sslcerts
```

1.4.1.10.2.3 Configuring the Tachyon certificate for macOS

The 1E Client for macOS devices supports the Configuring the Non-Windows Tachyon certificate using OpenSSL approach described above. Alternatively, the 1E Client for macOS also supports certificates stored within the macOS Key Store.

1.4.1.11 1E Catalog

Tachyon Setup will install 1E Catalog on the Tachyon server and ensure the server meets the requirements for installation.

Ensure the following URL is whitelisted:

- https://catalog.1e.com

This URL must be accessible from the Tachyon Server during the setup and running of 1E 1E Catalog. This enables the Catalog Update service to connect to the 1E Cloud Catalog and download the latest catalog entries.

> **Note**
>
> 1E Catalog may need additional configuration to support proxy servers, but this depends on the configuration you have in your current environment. Please contact 1E Support if you need help doing this.

1.4.2 Tachyon Setup

Use the Tachyon Setup wizard to check and configure prerequisites, install and verify each Tachyon server that makes up your Tachyon platform. It installs the applications you are licensed for and does various maintenance and configuration tasks.

1.4.2.1 Required installation files

You can download the installer from https://support.1e.com/. Extracting the zip will create a folder structure containing the following, where the files highlighted in bold are required by Tachyon Setup.

- Licenses.txt
- TachyonRelease Information
- **Tachyon.Setup.exe**

Please refer to:

- Tachyon Setup, for detailed information about each screen.
- Quick Startif you want a brief overview of installing Tachyon.

- Installers**1ECatalog.msi**
- Installers**AppClarity.msi**
- Installers**ApplicationMigration.msi**
- Installers**ContentDistribution.msi**
- Installers**SLA.BI.Installer.msi**
- Installers**SLA.Platform.Installer.msi**
- Installers**TachyonServer.msi**
- Installers\TachyonToolkit.msi

This folder contains **msi installer files** for components and applications that will be installed by setup if their prerequisites are met.

- Installers\Apps\Experience**Experience.zip**
- Installers\Apps\Experience**metadata.json**
- Installers\Apps\Explorer**Explorer.zip**
- Installers\Apps\Explorer**metadata.json**
- Installers\Apps\GuaranteedState**GuaranteedState.zip**
- Installers\Apps\GuaranteedState**metadata.json**
- Installers\Apps\Inventory**Inventory.zip**

This folder contains **apps folders** for consumer applications that will be installed by setup if their prerequisites are met.

If you do not want to install a consumer application, then delete the folder before running setup.

Later, if you need to install the consumer application, then you can reinstate the folder and install the app using setup as described in Applications maintenance.

- Installers\Apps\Inventory**metadata.json**
- Installers\Apps\Nomad**metadata.json**
- Installers\Apps\Nomad**Nomad.zip**
- Installers\Apps\PatchSuccess**metadata.json**
- Installers\Apps\PatchSuccess**PatchSuccess.zip**
- Installers\Apps\Settings**metadata.json**
- Installers\Apps\Settings**Platform.zip**
- ProductPacks\Newtonsoft.Json.dll
- ProductPacks\Tachyon.ProductPackDeploymentTool.exe
- ProductPacks\Tachyon.ProductPackDeploymentTool.exe.config
- ProductPacks\Tachyon.SDK.Consumer.dll
- ProductPacks\Classic\1E-ConfigMgrConsoleExtensions.zip
- ProductPacks\Classic\1E-Experience.zip
- ProductPacks\Classic\1E-Explorer-TachyonAgent.zip
- ProductPacks\Classic\1E-Explorer-TachyonCore.zip
- ProductPacks\Classic\1E-Inventory.zip
- ProductPacks\Classic\1E-Nomad.zip
- ProductPacks\Classic\1E-Patch-Success.zip

These Product Packs are required to support various Tachyonfeatures, for more detail please refer to Tachyon Product Packs reference.

If your license permits, you can use additional Product Packs available from 1E Exchange to meet specific use cases.

Classic Product Packs	Contain instructions, for use in Explorerand other Tachyonapplications. They can be uploaded using the Tachyon Product Pack Deployment Tool, or using **Settings→Instructions→Instruction sets** page in the Tachyon portal.
Integrated Product Packs	Contain policies, rules, and fragments for use by Guaranteed State, and may also include instructions. They can only be uploaded using

- ProductPacks\Classic\1E-Tachyon-Platform.zip
- ProductPacks\Integrated\MEMCMClientHealth.zip
- ProductPacks\Integrated\NomadClientHealth.zip
- ProductPacks\Integrated\TachyonCore.zip
- ProductPacks\Integrated\WindowsClientHealth.zip

the Tachyon Product Pack Deployment Tool.

Note

You should also have access to the location of the **Tachyon.lic** file provided with your purchase or evaluation.

1.4.2.2 Running Setup

Logon to the server using the Server installation account.

To start the setup wizard, double-click on **Tachyon.Setup.exe**. It will then display the following screens, you may go directly to any screen by clicking on the list on the left side of the wizard, but for best results, we recommend that you follow these in the order they are presented.

Note

Parts of each Setup screen will be greyed out if they are not applicable for the selected configuration type.

Warning

If you are installing a DMZ Server, please refer to Implementing a Tachyon DMZ Server before running Tachyon Setup.

The setup provides a two-stage process to install a new DMZ Server:

1. Run Setup Maintenance on the Response Stack server (specifically the server that hosts the Core which the DMZ Server will connect to) to prepare the Response server and its database, and store details in an **ini** file.
2. Run Setup to install the DMZ Server using the prepared **ini** file.

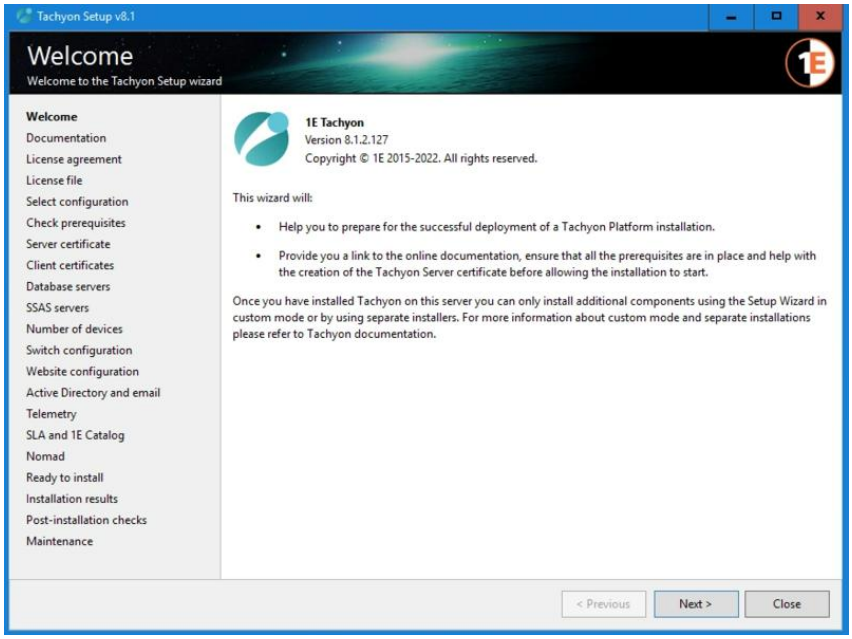
The two-stage process and its **ini** file are required because setup is unable to communicate through the DMZ firewall. In previous versions of Tachyon, the first stage required complex manual configuration.

To upgrade a DMZ Server, you only need to run setup on the DMZ Server, you do not require the **ini** file.

1.4.2.2.1 Welcome

This screen provides the version number for Tachyon platform and outlines what the wizard will do. It also examines the system for installed versions of the components and displays warning messages in case any of them cannot be upgraded to the versions that you are currently installing.

Click **Next** to go to the next screen.

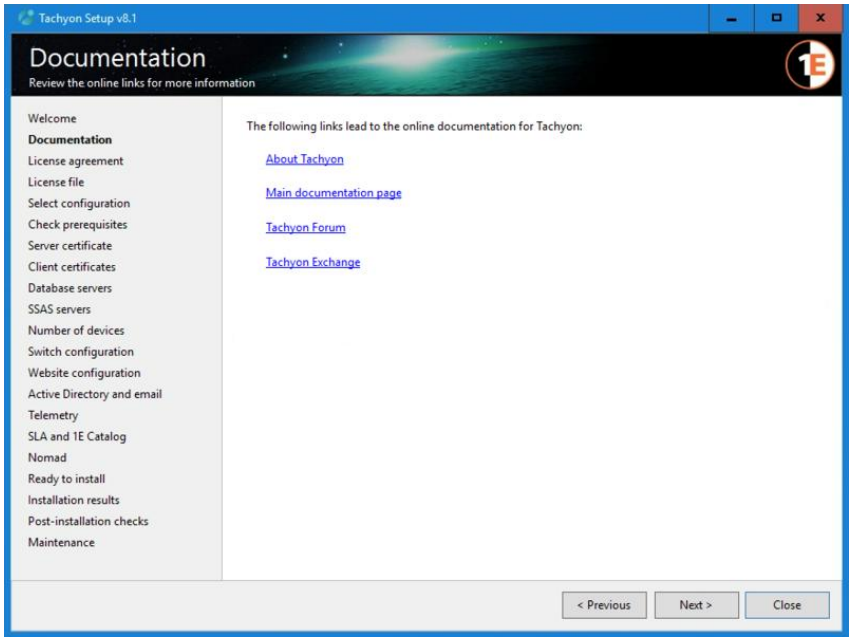


1.4.2.2.2 Documentation

This screen provides links to several online resources that provide additional information about how to use and configure Tachyon.

Link	Description
About 1E	Links to the Tachyon platform page on the 1E website.
Main documentation page	Links to the Welcome page for this documentation are on the help.1e.com website.
1E Forum	Links to the Tachyon Forum where you can find technical resources, such as troubleshooting and FAQs.
1E Exchange	Links to the 1E Exchange where you can find 1E and community-supported product packs to supplement the product packs included in the Tachyon Platform.

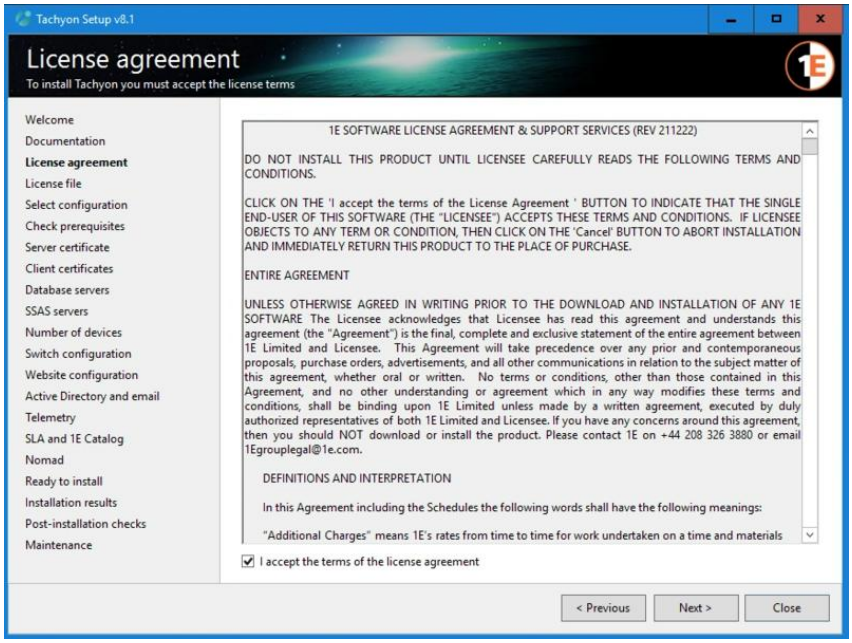
Once you've finished investigating the online resources, click **Next** to go to the next screen.



1.4.2.2.3 License agreement

You must read and then accept this license information by checking the **I accept the terms in the license agreement** checkbox. If you continue with the setup without checking the link to this screen will be highlighted in red and you won't be able to install it until it is checked.

Click **Next** to go to the next screen.



1.4.2.2.4 License File

On the **License File** field screen, you must enter the path to a valid 1E license file. You can also click **Browse** to locate the file using a standard file browser.

1E will provide you with a **Tachyon.lic** license file that defines the applications, tools, and features your system is able to use, for how long, and how many devices it supports, this may be an evaluation or subscription license.

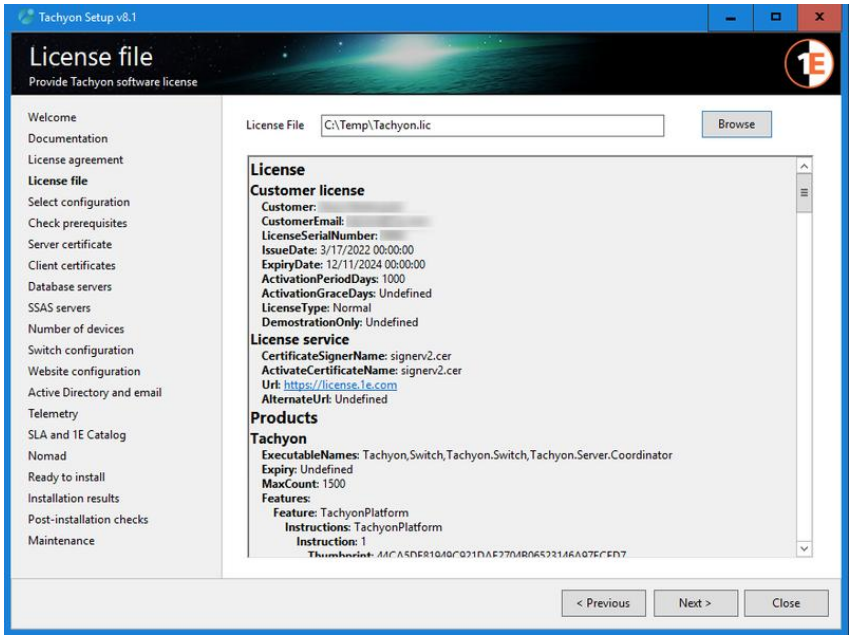
- The license must be activated. Once activated, it may be used only by the system that activated it.
- Licenses can be renewed or updated, but if allowed to expire, then the affected products or features will not be usable.
- For a new installation, the Tachyon Setup program will let you select the license file from any folder on disk.
- For an existing installation, the license file is copied into the folder: %PROGRAMDATA%\1E\Licensing on your Tachyon Server.

Setup will attempt to connect to the 1E license service in the 1E cloud, and warn you if a connection cannot be established. The product will still install successfully and you will be able to connect to the Tachyon portal but you won't be able to fully use the system until you enable communications with the 1E license service.

For more details please refer to the License requirements page.

Note

This screen displays the message "A DMZ Server installation does not require a license file" when installing a DMZ Server, and you have provided an **ini** file in the Setup folder that has the same name as the server hostname.



1.4.2.2.5 Select configuration

This screen lets you choose between installing all the Tachyon Server components onto a single server or selecting the components you want to install individually.

The options in the **Select configuration** list are:

- **All components on a single server** (default) - all components required for Tachyon Master and Response Stacks
- **Tachyon Master Stack** - all Tachyon systems require one Master Stack
- **Tachyon Response Stack** - this is required for Real-time features of Tachyon
- **DMZ Server** - this is required to provide Real-time features to Internet-facing clients

Note

This screen automatically selects "DMZ Server" when installing a DMZ Server, and you have provided an **ini** file in the Setup folder that has the same name as the server hostname. For more detail, please refer to Implementing a Tachyon DMZ Server.

Optional components

When you select **All components on a single server** or **Tachyon Master Stack**, you can also select optional components:

- **Tachyon Experience** - if you want to use the Experience application from 1E
- **Nomad** - if you want to monitor Nomad in your environment, and features such as Single-Site Download and Pre-cache
- **AppClarity**
- **Application Migration**.

A component is included in this list because its installer **.msi** file has been detected by Setup in its **Installers** folder. A component is automatically enabled if its feature is enabled in the License File.

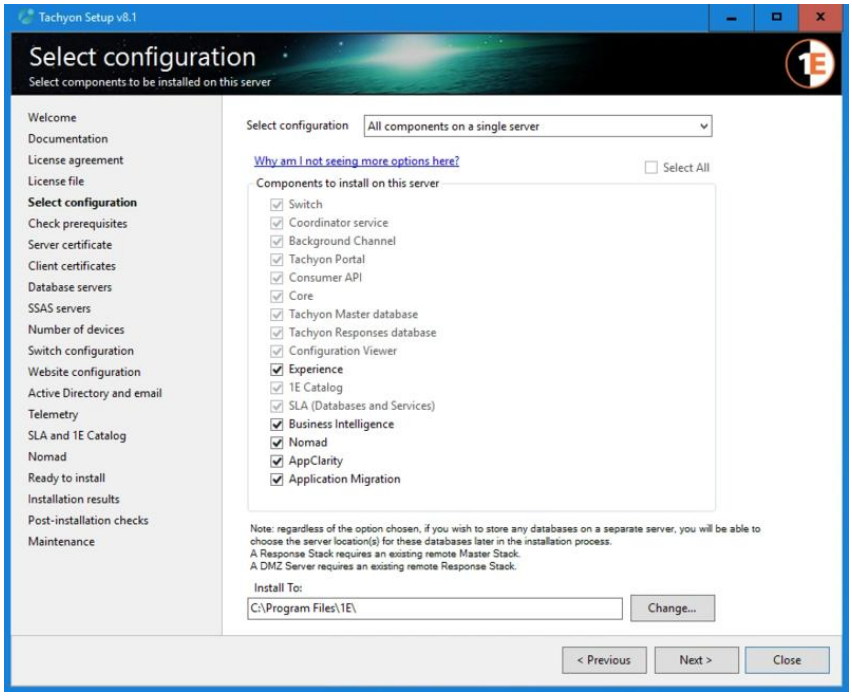
Setup will also automatically install additional applications it detects in its **Installers\Apps** folder, which includes apps that do not have their own installers, such as Explorer , Guaranteed State , Inventory , and Patch Success . After installation, these apps are visible in the Tachyon portal if their consumer is enabled in the License File. The Settings app is always available.

Custom configuration

A **custom configuration** can be made available where you can select the components you wish to install on the server. For guidance please contact 1E.

You can also change the folder you wish to install to.

After selecting the installation options you want, click **Next**.



1.4.2.2.6 Check prerequisites

This screen performs prerequisite checks on the local server and user account. The list varies depending on which components you selected on the Select configuration screen.

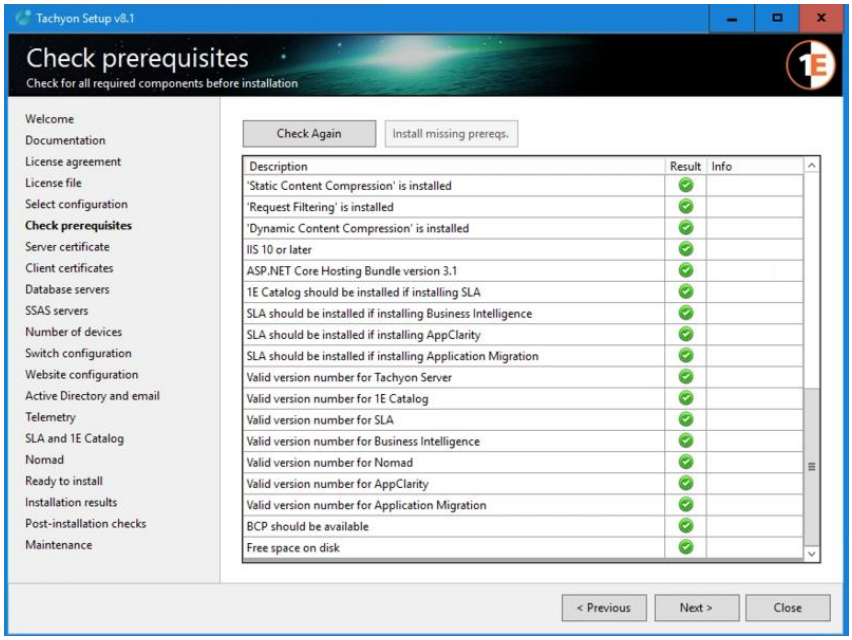
Click **Start Checking** to start the checks.

If any of the checks fail, **Tachyon Setup** may be able to install the missing prerequisites. To install these, click the **Install missing prereqs.** button.

> **Note**
>
> If .NET Framework 4.8 is missing, the checker will stop at this point, for you to select **Get & Install**. You must reboot after you have installed .NET Framework, and then start Tachyon Setup again.

> **Note**
>
> If there are missing prerequisites that **Tachyon Setup** is able to install, then the **Install missing prereqs.** button is enabled. If you click this button, the missing prerequisites will start the installation immediately.
>
> Not all prerequisite checks have automated fixes. If your environment fails a check and the **Install missing prereqs.** button has not been enabled then you will need to install or configure the missing prerequisites by hand.

You can click **Check Again** to re-run the checks once any remediation steps have been made.



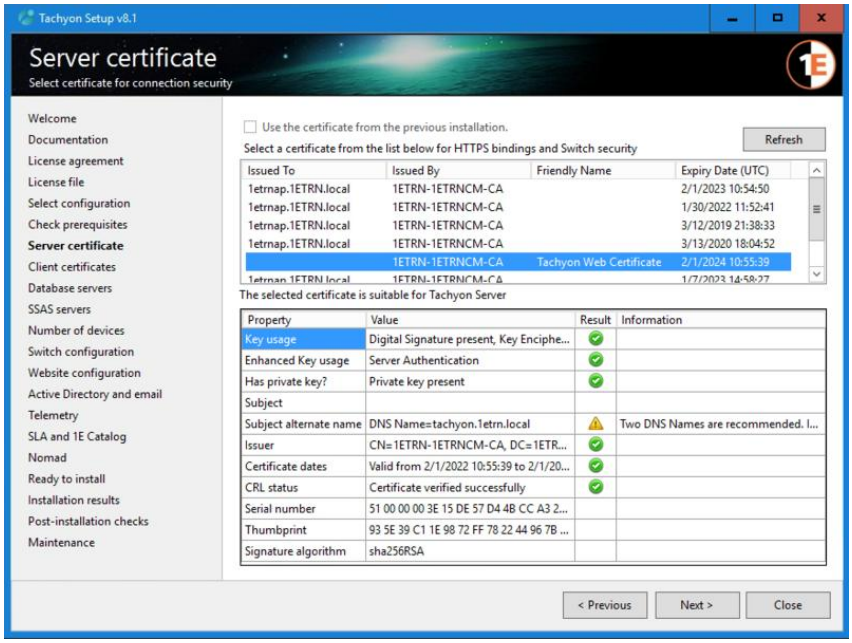
1.4.2.2.7 Server certificate

This screen displays a list of certificates from the Local Computer\Personal certificate store, letting you select a specific certificate you want to use for the Tachyon Server website and Tachyon Switches. Tachyon Setup will then evaluate the suitability of the selected certificate.

> **Note**
>
> You may notice a warning for the **Subject alternate name** indicating that **Two DNS Names are recommended**. This is a requirement when performing a Tachyon Setup in a DMZ scenario. In all other scenarios, although recommended this warning can be ignored and still result in a successful setup.

The option to **Use the Switch certificate from a previous installation** can be used if you are upgrading, or you can choose a different certificate.

If there are issues with the certificate after installation, they may be resolved using the steps in Server installation issues.



1.4.2.2.8 Client certificates

This screen lets you manage the trust(s) between the Tachyon Server and clients.

If your clients do not have certificates or you do not want to use them, then uncheck **Switches require client certificates to be presented by Tachyon client features of the 1E Client**. This option configures Switch(es) to not require client certificates. Clients will effectively use anonymous authentication.

Note

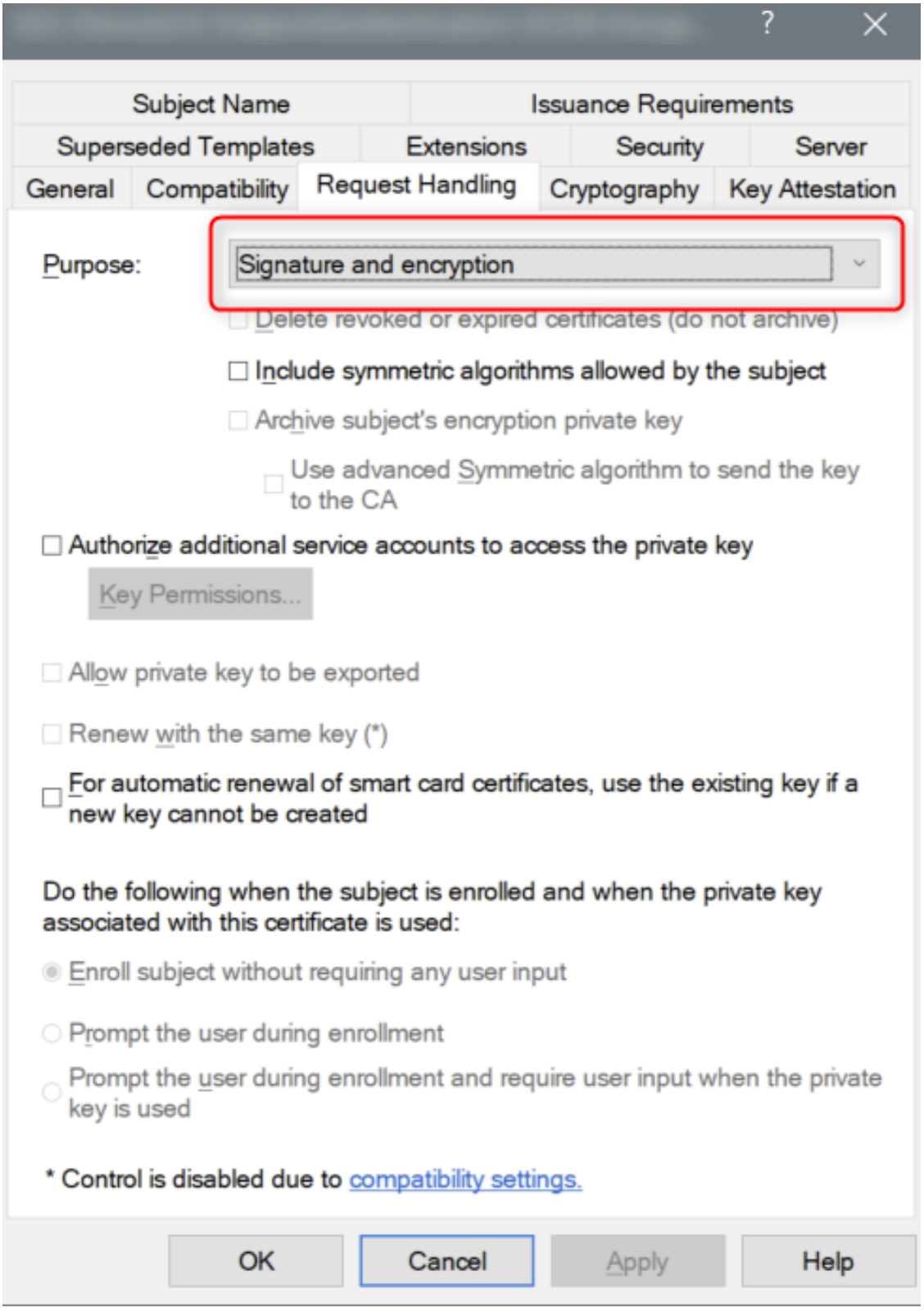
For a new installation, this setting is checked by default.

For an upgrade, this setting is determined by the current configuration of the Switch(es). If any Switch is configured to require client certificates, then this setting will be checked and re-applied to all Switches.

Please refer to Switch Command Lines if you want to reconfigure switches post-installation.

Note

The 1E Client requires that the client certificate it presents to the platform has both the **Signature** and **Encryption** request handling options. These options are the defaults if provisioning using a Computer Certificate template from a Microsoft Windows Certificate Authority. If you are using a custom template, or an alternative certificate authority, you should confirm that both these options are enabled.



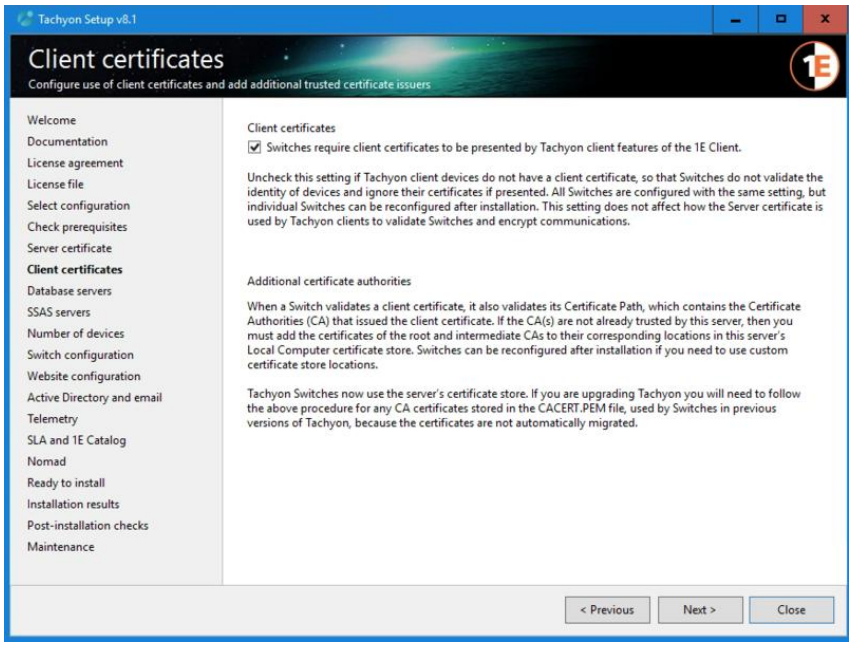
Using certificates issued by a differant CA

If you want clients to present certificates, that were issued by a different Certificate Authority than the certificate used by Switch(es), then the process described below must be used for each *different* Certificate Authority:

1. Create **.cer** or **.pfx** files containing the public key of the issuing CA, its root CA, and any intermediate CA in the trust path of the client certificate.

2. Import the CA files into the corresponding CA stores on the Tachyon server.

For more detail about client certificates, please refer to Tachyon client certificate requirements.



1.4.2.2.9 Database servers

On this screen, you select the SQL Server instances where you want to install each of the databases that will be deployed:

- Master
- Responses
- 1E Catalog
- SLA databases (SLA-Data, SLA-Shared, and SLA-Integrate databases must be installed on the same instance)
- Content Distribution
- Experience .

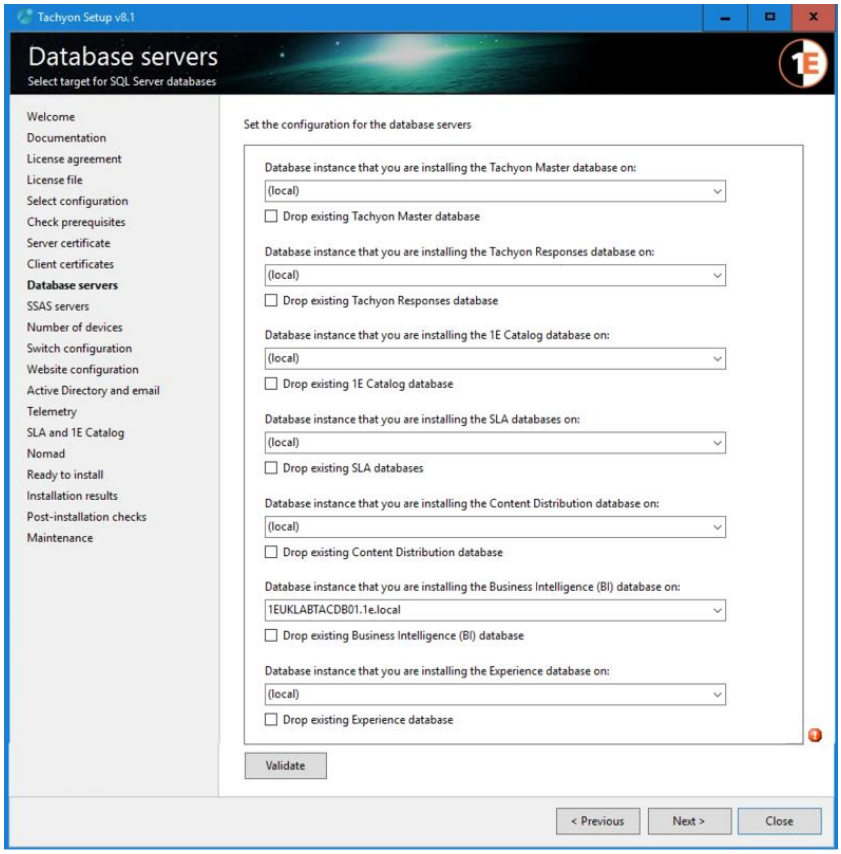
For each database, a combo box containing a list of available SQL Server instances is displayed. This list of instances is generated as a background task, so it may take a few seconds to populate. It may also return instances that are accessible but not necessarily on the local network. You may

select one from the list or type in your own. 1E recommends all databases are installed on the same SQL Server instance.

For each database, there is a **Drop existing <title> database** checkbox, which if you are upgrading you can check to remove any existing data from that database on the specified database server. You should be careful when checking these checkboxes and sure that you want to continue, as data will be deleted if they are checked and the installation is started.

A **Validate** button is provided that performs some basic tests to check that the selected SQL instances can be accessed using the current user account.

Once the SQL Server instances have been selected and validated, click **Next** to continue.



1.4.2.2.10 SSAS servers

This screen is only relevant if you selected the option to install **Business Intelligence** on the **Select Configuration** screen.

On this screen:

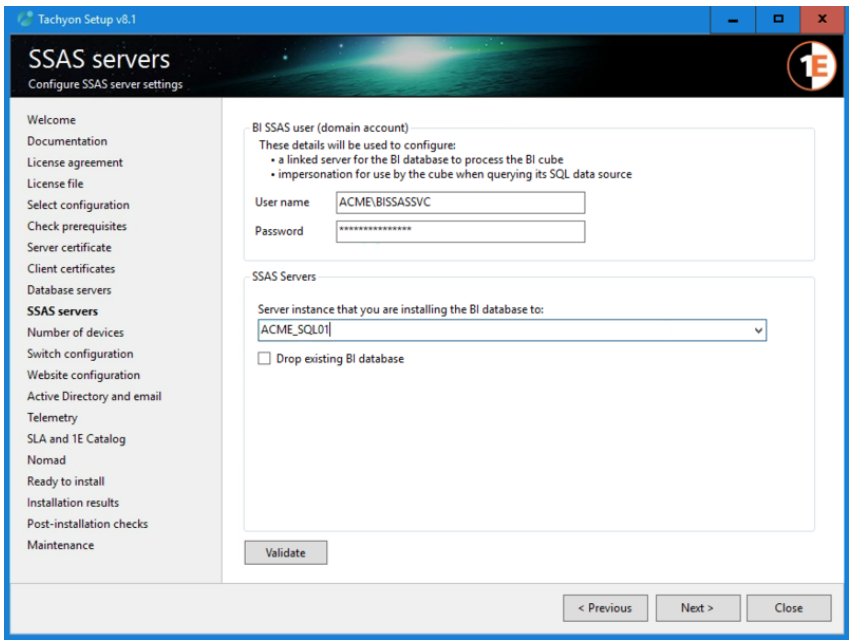
- Enter the credentials for the **BI SSAS User** account, that will be used to connect to the SSAS server (Patch Success)
- Select the server instance for the SQL Server Analysis Service where you want to deploy the Business Intelligence cube (Patch Success).

The **Validate** button lets you performs some basic tests (but not a full validation of permissions and functionality on the SSAS server).

Once you have entered and validated the settings, click **Next** to continue.

Note

For more information about the **BI SSAS User** account, please refer to Service accounts.



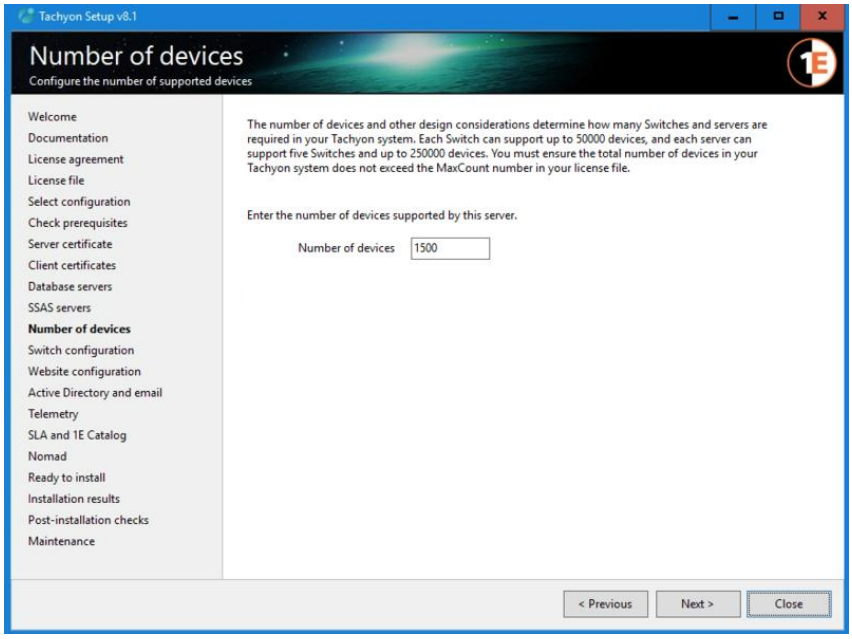
1.4.2.2.11 Number of devices

Enter the number of devices supported by this server.

The number of devices supported by a Tachyon Server determines the number of Switches configured on the server.

The range is 1 to 250,000; default is 1,000.

A single server with suitable resources can support up to five Switches and up to 250,000 devices, with each Switch supporting up to 50,000 devices. Additional servers or configurations may be required according to the design of the system. The total number of devices supported across the system must not exceed the license file allocation.



1.4.2.2.12 Switch configuration

This screen is only relevant if you selected one of the following configuration options:

- All components on a single server
- Tachyon Response Stack
- DMZ Server.

This screen displays a list of IP Addresses that can be assigned to each Switch in your configuration. Tachyon Setup will estimate how many Switches are required for the number of devices selected in the earlier setup screen and try to assign an IP Address for each. You will need to confirm or change which IP Address is used by each Switch.

IPv6

The screen only displays a list of IPv4 IP Addresses available on the server. If you need to use IPv6 and have a functioning IPv6 network infrastructure then please contact 1E for further advice on how to use this screen.

Ideally, to maximize the performance of Tachyon you should have the following configuration:

- You have enough Switches configured to support the selected number of devices - you can add additional Switches by clicking extra checkboxes if you have enough IP Addresses configured
- One interface per Switch - interfaces may have more than one associated IP Address, so you'll need to check the MAC Addresses to make sure that the IP Addresses are on different interfaces
- An additional interface if you have a remote SQL Server, is necessary to separate incoming and outgoing response traffic, using a persistent route as described in Configuring a persistent route for SQL traffic.

However, in a lab or other environment which has less than 500 devices, you can have all components using a single IP Address.

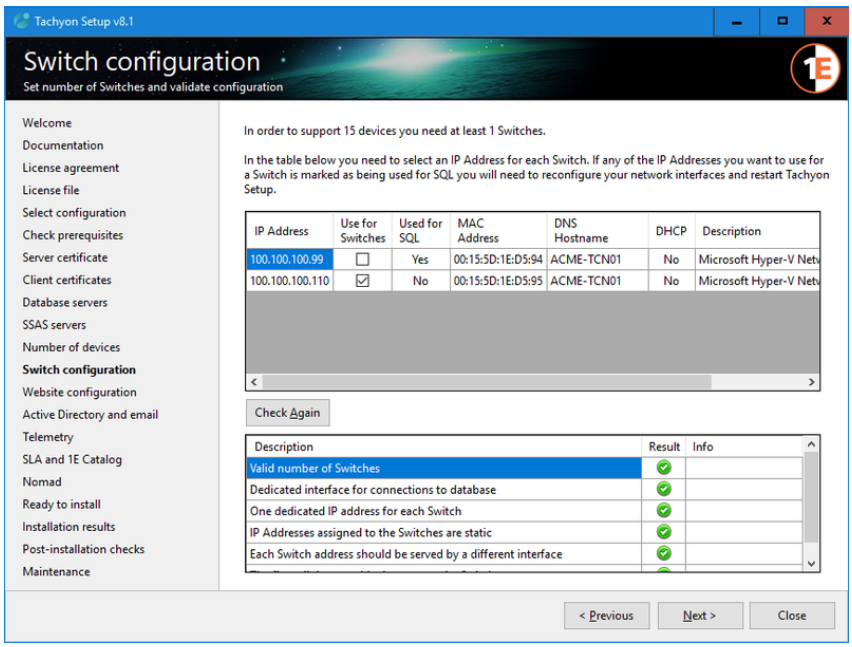
If you have a local installation of SQL Server, then **Used for SQL** will show **No** for all IP Addresses, and you can select whichever IP Address you wish to for each Switch.

If you are using a remote SQL Server, then **Used for SQL** will show **Yes** for the IP Address, which is the validation process used in the Database servers screen to validate the connection to the SQL Server you selected for the Responses database. If this is not the same interface you prepared a persistent route for, then you will need to configure the persistent route and restart Tachyon Setup. The validation checks do not test if the route is persistent.

For an installation with multiple Switches, aside from each selected IP Address, all Switches will have an identical configuration.

Click **Validate** to check that your selection conforms to the best practice rules for configuring switches.

Once the selection has been validated, click **Next** to continue.



1.4.2.2.13 Website configuration

Confirm that the details are correct on this screen. If the defaults are changed, then ensure you use the **Validate** button.

> **Note**
>
> Many of the fields on his screen are pre-populated with default ports (the Main website binding ports should not be changed), and DNS Names found in the certificate selected in the Server certificate screen.
>
> When installing a DMZ Server, and you have provided an **ini** file in the Setup folder that has the same name as the server hostname, the fields are pre-populated using values from the **ini** file. You should not change these.
>
> For more detail, please refer to Implementing a Tachyon DMZ Server.

Parameter	Description
HTTP Host Header (Main binding)	Sets the **host header** used by the **main HTTP binding** for the website. The default value is set to the FQDN for the local computer, and should not need to be changed. **Note** If you are upgrading from SLA Platform 3.3 and SLA Platform had a custom host header defined for HTTP, you should change the host header to the host header used for the SLA Platform website. If the Tachyon website uses a different host header port than was previously used by SLA Platform and you are using Application Migration, the Application Migration Task sequence step and Shopping integration will stop working until these URLs are updated.
HTTP Port (Main binding)	Sets the **port** used by the **main HTTP binding** for the website. Together with the Host Header and IP Address, these bindings uniquely identify the website which Tachyon Switches use to connect to the Tachyon Core. The default value is set to 80, and should not need to be changed. **Note** If you are upgrading from SLA Platform 3.3, you should change this port to the **HTTP port** previously used for the SLA Platform website (default **8080**). If the Tachyon website uses a different port than was previously used by SLA Platform and you are using Application Migration, the Application Migration Task sequence step and Shopping integration will stop working until these URLs are updated.
HTTPS Host Header (Main binding)	Sets the **host header** used by the **main HTTPS binding** used by the website. This is used by: • Tachyon administrators to communicate with the Tachyon portal and apps • Tachyon clients connecting to the background channel, if installed. **Note** The FQDN used for the host header must be included as a Subject Alternate Name (SAN) in the Web certificate. The default value is set to Tachyon .<domainFQDN>
HTTPS Port	Sets the **port** used by the **main HTTPS binding** used by the website. The default value is set to 443, and should not need to be changed.

Parameter	Description
(Main binding)	
HTTPS Host Header (Alternate binding)	Sets the **host header** used by the **alternate HTTPS binding** used by the website. This is mandatory when installing on a DMZ Server, and used for the internal-facing network. Optionally used by the following if you do not want the main HTTPS binding, for example if you want to use a different HTTPS port: • Tachyon clients connecting to the background channel • Application Migration clients running task sequences and connecting to the SLA Provider API • AppClarity software reclaimer connecting to the SLA Provider API. **Note** If used, the FQDN used for the host header must be included as a Subject Alternate Name (SAN) in the Web certificate. **Note** If you are upgrading from SLA Platform 3.3 and SLA Platform had a custom host header defined, you should change the host header to the host header used for the SLA Platform website. If the Tachyon website uses a different host header port than was previously used by SLA Platform and you are using Application Migration, the Application Migration Task sequence step and Shopping integration will stop working until these URLs are updated.
HTTPS Port (Alternate binding)	Sets the **port** used by the **alternate HTTPS binding** used by the Tachyon portal website. This is used by clients to communicate with the Tachyon server using the background channel. The default value is set to 443. **Note** If you are upgrading from SLA Platform 3.3, you should change this port to the **HTTPS port** previously used for the SLA Platform website (default **8443**). If the Tachyon website uses a different port than was previously used by SLA Platform and you are using Application Migration, the Application Migration Task sequence step and Shopping integration will stop working until these URLs are updated.

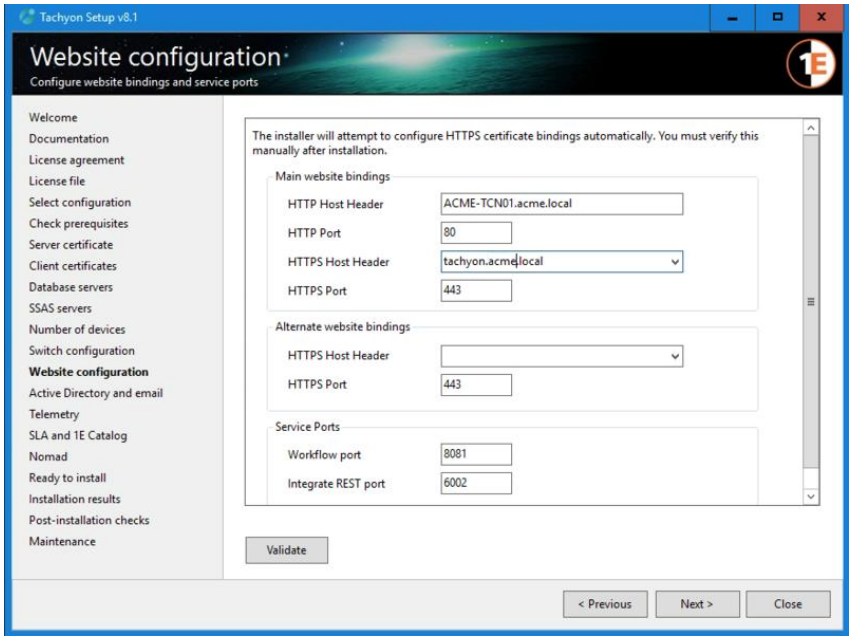
Parameter	Description
Workflow port	Sets the port used by HTTPS binding of the Coordinator Workflow module. This is separate from the Tachyon website. **Tachyon Setup** suggests **8081** by default, and should not need to be changed.
Integrate REST port	This is used internally by the SLA Integrate services. You will normally not need to change it unless it conflicts with any other service that is already using the same port.

After installation, you will need to manually verify the certificate bindings, as described in Tachyon Server post-installation tasks.

A **Validate** button is provided that performs some basic tests to check that the selected HTTP/HTTPS Host Header and ports as well as the service ports do not conflict with each other and that the addresses are resolvable from DNS.

When all the settings have been made and validated, click **Next** to continue.

> **Note**
>
> Versions of Tachyon Setup before 5.2 had the option to change the IP Address used by the Main website bindings for HTTPS and HTTP. By default, this is * for both bindings. You can manually edit the bindings later using IIS Manager if you need to change the IP Address for any binding.



1.4.2.2.14 Active Directory and email

On this screen you enter the details for the Active Directory search method. You can choose to enable email and enter the SMTP server details. When email is enabled you can also select if you want two-factor authentication to be enabled.

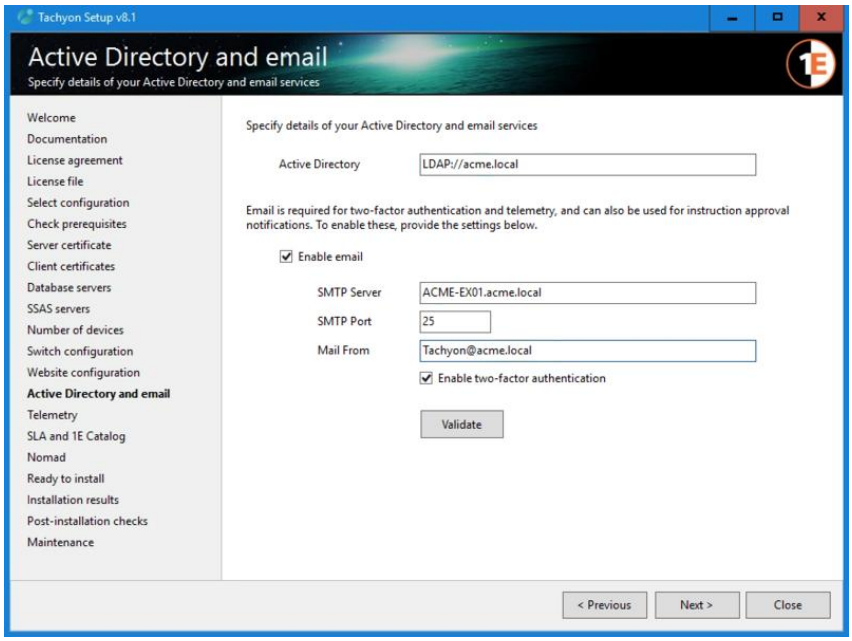
Parameter	Description
Active Directory	A list of Active Directory URLs. Tachyon services locate users and computers and membership of security groups by querying a semi-colon delimited list of Active Directory GC and/or LDAP URLs. **GC URL** This is the quickest and simplest method of resolving users and group membership. A single GC URL will normally resolve all users and groups within a single **forest**. Supports only Universal security groups. **LDAP URL** A single LDAP URL will normally resolve all users and groups within a single **domain**. Supports Universal and Global security groups. Required if a Global Catalog (GC) server does not exist in a trusted forest, or if Global security groups must be used. Any domain which contains Tachyon servers, users or groups must: • Be resolvable from the Tachyon Server using DNS - that is, the server must be able to resolve domain names using DNS • Have a two-way trust with the domain in which the Tachyon (Master Stack) Server exists - so that users trust the server, and the server trusts users • Allow the Tachyon Server to read computer, user, and security group objects in each domain. The default **GC://** is sufficient for a Tachyon Server in a simple Active Directory environment of one forest which has a Global Catalog. You can include, but it is not required, the name of the server's local domain or root domain, for example: **GC://acme.local**

Parameter	Description
	To add support for a remote forest which has its own GC, you would for example have **GC://acme.local;GC://nadir.local** and so forth adding the root domain of any other forests to the list of GC URLs. If you prefer to use LDAP, or there are difficulties with trusts between forest domains, then you would create a list of LDAP URLs including *all* domains that have Tachyon users and groups, as well as domains in which a Tachyon server resides. For example: **LDAP://acme.local;LDAP://pop.acme.local;LDAP://rock.acme.local;LDAP://country.acme.local;LDAP://nadir.local;LDAP://disco.nadir.local** You can mix GC and LDAP URLs, but you should avoid mixing LDAP URLs that are also resolved by a GC URL. For example: **GC://;LDAP://nadir.local;LDAP://disco.nadir.local** The Coordinator Workflow module queries AD for email details of Tachyon users, and the Consumer API queries AD for security details of Tachyon users to support Role-Based Access Control.
Enable Email	Determines whether email features are available. Tachyon uses email for: • Notifications • Two-factor authentication • Sending Telemetry data to 1E. For guidance about using non-default SMTP settings, see Email and 2FA requirements. If email notifications need to be disabled after installation, then see Changing the SMTP Host configuration. To configure Telemetry after installation, please refer to Enabling or disabling Telemetry features.
SMTP Server	Sets the FQDN of the SMTP relay/gateway. If the FQDN needs to be changed after installation, then see Changing the SMTP Host configuration.
SMTP Port	Sets the port used to connect to the SMTP relay/gateway. Default is 25.

Parameter	Description
	If the port needs to be changed after installation, then see Changing the SMTP Host configuration.
Mail from	Sets the mail-from email address used by the Tachyon Server when it sends emails. For guidance about the Mail-From address see Mail-From address.
Enable two-factor authentication	Determines whether Tachyon uses two-factor authentication. If email is disabled then so is two-factor authentication which relies on email. See Email and 2FA requirements.

A **Validate** button is provided that performs some basic tests to check that the selected SMTP server and port can be contacted.

Click **Next** to continue.



1.4.2.2.15 Telemetry

On this screen, you choose whether to enable or disable the Tachyon telemetry features.

The Default setting of **Server telemetry** feature is enabled

The Default setting of **User Interface telemetry** feature Is Full

Click **Next** to continue.

Note

Server telemetry

Tachyon will periodically send summarized, statistical information about the usage of the product to 1E. This enables 1E to improve your experience as it helps us understand how features are being used, focus future development, ensure we continue to support the Operating Systems you currently use, spot early warning signs of potential issues, and identify instructions that may be causing issues or could be improved. No personally identifiable data is collected. The data is compressed, encrypted, and sent to 1E through email.

Full details of what data is collected are provided here: Server telemetry data.

How to configure the frequency with this data sent to 1E is described here: Enabling or disabling Telemetry features.

The **Server Telemetry** feature is only available if the following dependencies are enabled:

- Coordinator service - this component is enabled when installing a Tachyon Master Stack, visible in the Select configuration
- Email - this is an optional feature in Active Directory and email screen.

1E Cloud connection from the server must also be whitelisted, as described in Whitelisting connections to 1E Cloud.

You can change the configuration after installation, as described in Enabling or disabling Telemetry features.

Note

User Interface telemetry

User Interface telemetry reports how the user interface is used, and data is sent directly from administrator browsers to the 1E Cloud.

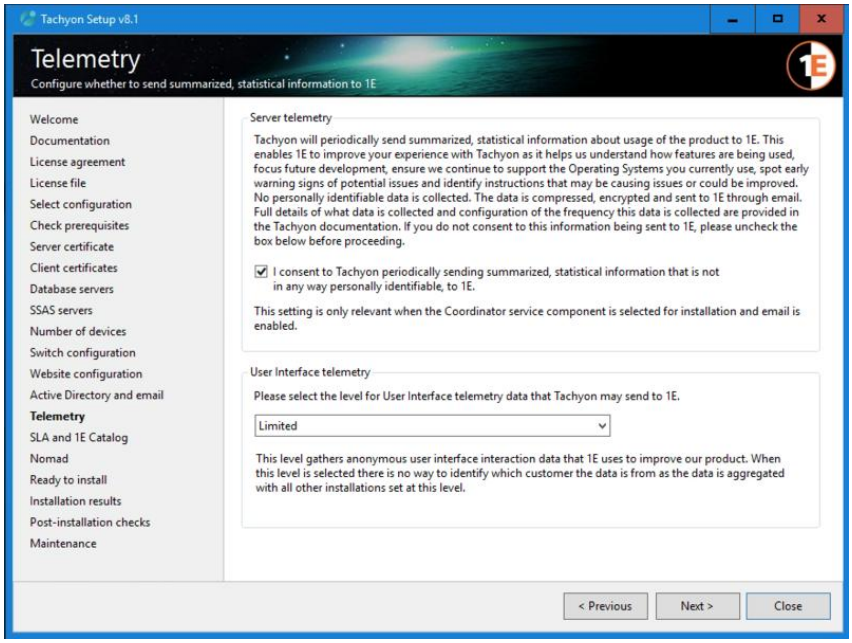
1E Cloud connection from administrator browsers must also be whitelisted, as described in Whitelisting connections to 1E Cloud.

You can change the configuration after installation, as described in Enabling or disabling Telemetry features.

There are three options available, they all gather user interaction data that 1E uses to improve Tachyon platform and its associated applications. They are described in the following table:

Option	Description
Limited	When this option is selected the data is aggregated and anonymized so there is no way to identify the customer the data is being collected from.
Basic	The data collected for this option is the same as the **Limited** option, except that it is associated with the name used in the

Option	Description
	license file. The 1E customer success team can use this information to help improve the experience for our customers.
Full	The data collected for this option is the same as the **Basic** option, except that it also records a unique identifier for each user. The user's name is not captured. The 1E product team can use this information to see how users are interacting with our products and understand their user journeys.



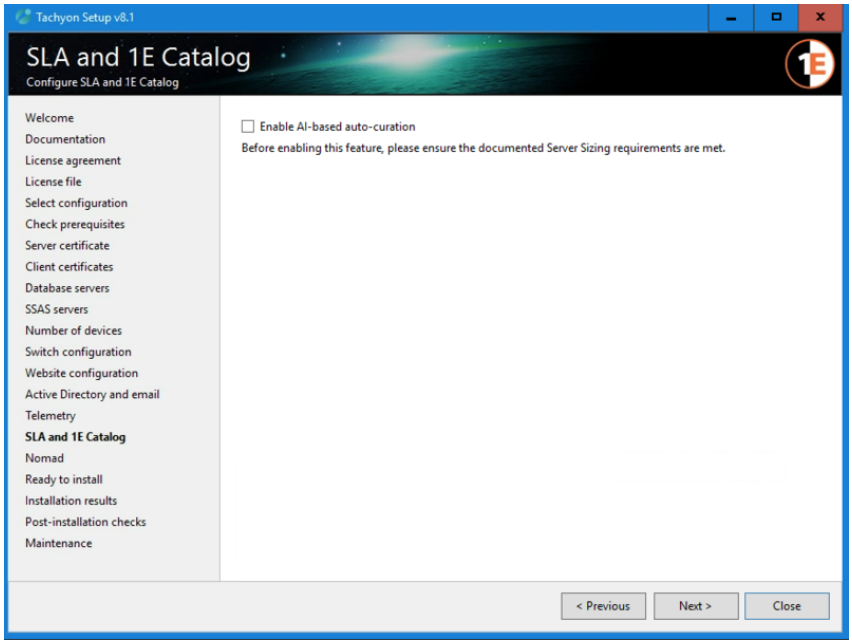
1.4.2.2.16 SLA and 1E Catalog

Tachyon AI Powered Auto-curation feature automatically recognizes software without the need to first create mapping rules in the 1E Catalog . This means you can have greater visibility of software installed across your organization. Please refer to AI Powered Auto-curation for more details, this also includes information on how to enable the feature post setup.

On this screen, you can configure whether the AI Powered Auto-curation feature is enabled or not. If you are installing or upgrading 1E Catalog using Tachyon Setup , enabling this will also configure 1E Catalog to download the files needed by SLA to support this feature.

To enable the feature, check the **Enable AI-based auto-curation** checkbox.

Click **Next** to continue.



1.4.2.2.17 Nomad

If you have selected the option to install Nomad on the **Select Configuration** screen, then you need to set the following options.

Name for the Configuration Manager Site server

Provide the name for the Configuration Manager Site server.

Doing this allows the Configuration Manager database to be located using a WMI query - for this to work the installation account must have Read-only Analyst permissions in Configuration Manager.

Use the **Validate** button to verify the specified Configuration Manager Site server can be located, and that the installation account has the required permissions in Configuration Manager.

> **Note**
>
> If your installation account does not have sysadmin rights on the SQL instance that hosts the Configuration Manager database, then you will see a popup warning you that Setup could not validate the membership of the Tachyon

	server's computer$ account in the **ConfigMgr_DViewAccess** localgroup. This is not a fatal error as long as you are sure the account is a member of the localgroup. If you proceed without this, then you will need to add it later to ensure Nomad functions correctly. For more information about the **ConfigMgr_DViewAccess** localgroup, please refer to Microsoft Endpoint Configuration Manager preparation.
Synchronization interval	Select a synchronization interval in minutes that governs how often the Nomad app and Pre-cache feature synchronizations will happen. This is set to 30 minutes by default.

You must also configure the following authentication options. If you do not configure these settings now, then you will have to manually configure them later if you decide to use Nomad .

Authentication from Background Channel Proxy to Content Distribution	Determines how the Background Channel Proxy communications with the Nomad application. You have the following options: **Windows authentication** — Windows authentication will be used to authenticate communications between the Background Channel and Content Distribution. **Certificate** — On choosing this option, you then need to select a valid **Client Authentication certificate** on the

	local server, that will be used to authenticate communications from the Background Channel by the Content Distribution component. Use the **Validate** button to verify the selected certificate.
Authentication used by Nomad clients connecting to the Background Channel Proxy	Determine how the Nomad clients will authenticate with the Background Channel Proxy. This is separate from the Nomad client configuration for Peer-to-Peer communication features. You have the following choices:
Client certificates	This option is the natural choice if you have also chosen, in the Client certificates screen above, for clients to their present client authentication certificates to Switches on the same server as the local Background Channel. Use this if either of the following is true:

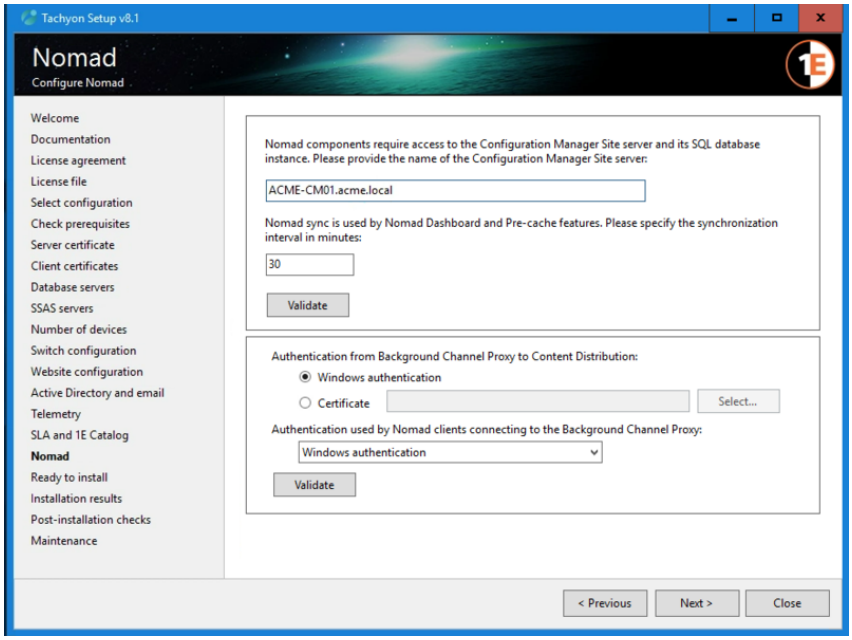
	• You are installing the Background Channel on a DMZ Server that is not domain-joined • Any of your 1E Clients are non-Windows or not domain-joined (workgroup) computers.
Windows authentication	Use this if you do not wish to use client certificates. This option is only possible if the local server is domain-joined, which is not typical for a DMZ Server. All your 1E Client must be domain-joined computers in domains trusted by the

	domain of the Response server.
None	If neither of the above options is possible. This means any clients will connect Anonymously.

Note

The Background Channel provides a reverse proxy feature that forwards communications from Nomad clients (internal and external) to the Content Distribution API, devices that are external to the organisation will communicate via the 1E DMZ server.

Click **Next** to continue.



1.4.2.2.18 Ready to Install

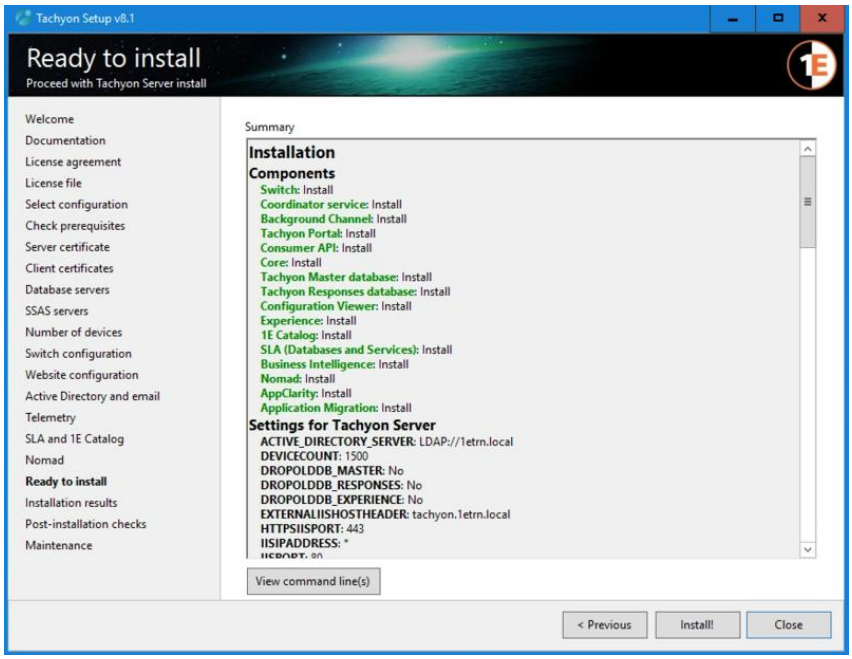
To start the Tachyon Server installation with the information you have provided, click the **Install!** button at the bottom of the **Ready to Install** screen.

Note

Because you can click on this screen at any point, the **Install!** button is only enabled when enough information and responses have been provided on the other screens to enable installation to start.

For example, one of the conditions is that until you respond by checking the **I accept the terms in the license agreement** checkbox on the **License Agreement** screen the **Install!** button will not be enabled. Other items such as selecting a valid Tachyon Server website certificate are also requirements.

Once you have reached this stage and no errors are displayed, a file named Tachyon.Setup.ini is written to disk in the same folder that contains Tachyon.setup.exe. This .ini file contains the selections that you made up to this point, and can be used to re-launch the installer without having to re-enter all the settings.



When you've configured the installation properties you can click the **View command line** button to view the command lines used to run the various **.msi** installers to install Tachyon Server along with the bundled components with the settings you have entered.

Warning

Tachyon Setup is the only supported method of installing, upgrading, and patching a Tachyon server.

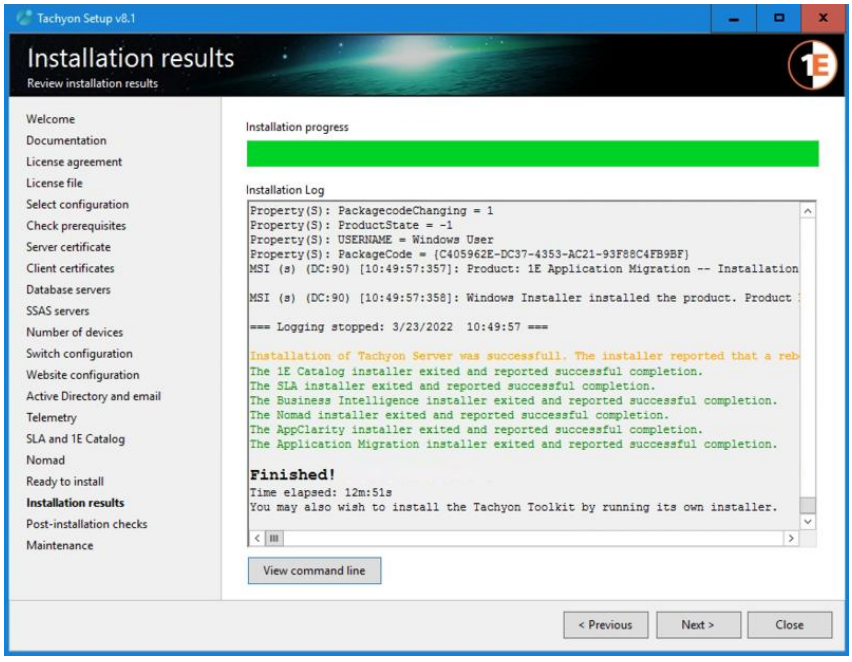
Installation using standalone **msi** or **msp** files is not supported unless advised by 1E, which may be necessary in complex installations, using non-interactive (quiet/silent) command-lines, and may require further post-install configuration steps.

1.4.2.2.19 Installation results

This screen displays the current progress of the installer. The installer log information is displayed as it occurs in the Installation Log window.

Once the installation has finished successfully the message:
The installer exited and reported successful completion, will be displayed in the **Installation Log** window.

You can find the installation logs on disk (*.log) in the same folder from where Tachyon.Setup.exe was launched.

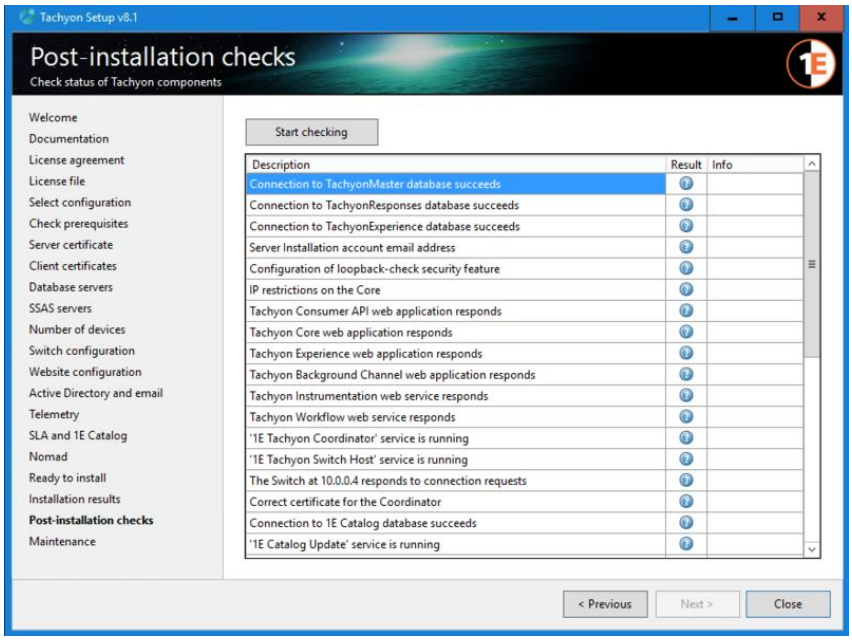


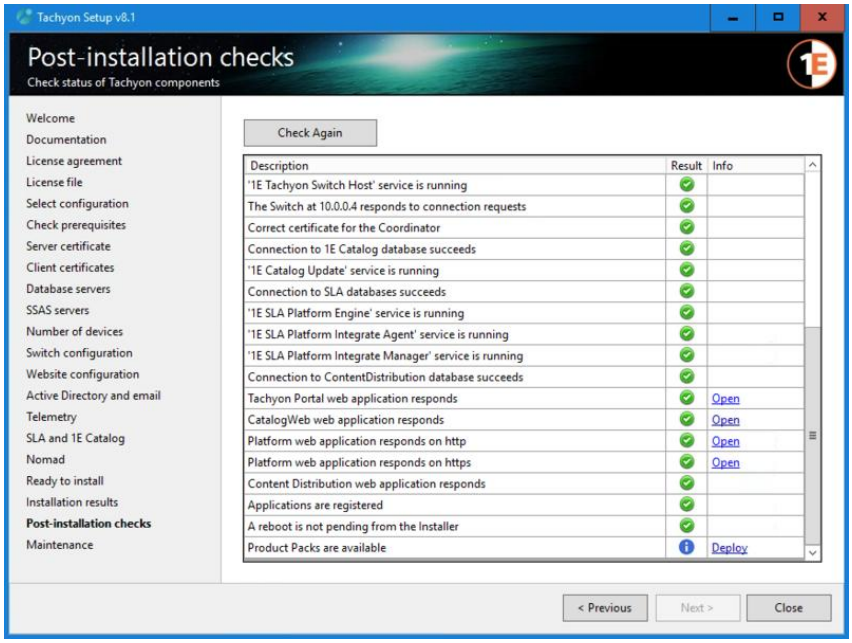
1.4.2.2.20 Post-installation checks

After an installation, you can opt to run the **Post-installation checks** by clicking on the **Start checking** button.

The aim is to achieve 100% check success results in the **Result** column. If any of the checks fail, look for additional information in the **Info** column. You can use this information to help troubleshoot the issue in combination with the Troubleshooting section and/or share with 1E Support.

One of the post-installation checks is: **Tachyon Portal web application responds**. When this check passes, it will display a link **Open** which can be used to start the default browser and connect to the **Tachyon Portal**.





1.4.2.3 Maintenance

You can start **Tachyon.Setup** and click directly on the **Maintenance** link in the left-hand menu.

1.4.2.3.1 Maintenance

From this screen, you can:

- **Uninstall...** all or part of the components deployed from Tachyon Setup
- Install, re-install or update any **Applications...**
- Change the **Server certificate...** used by the Tachyon website, switches, and services - or fix their bindings
- Upload and apply a 1E Hotfix bundle by clicking on **Hotfixing...**.

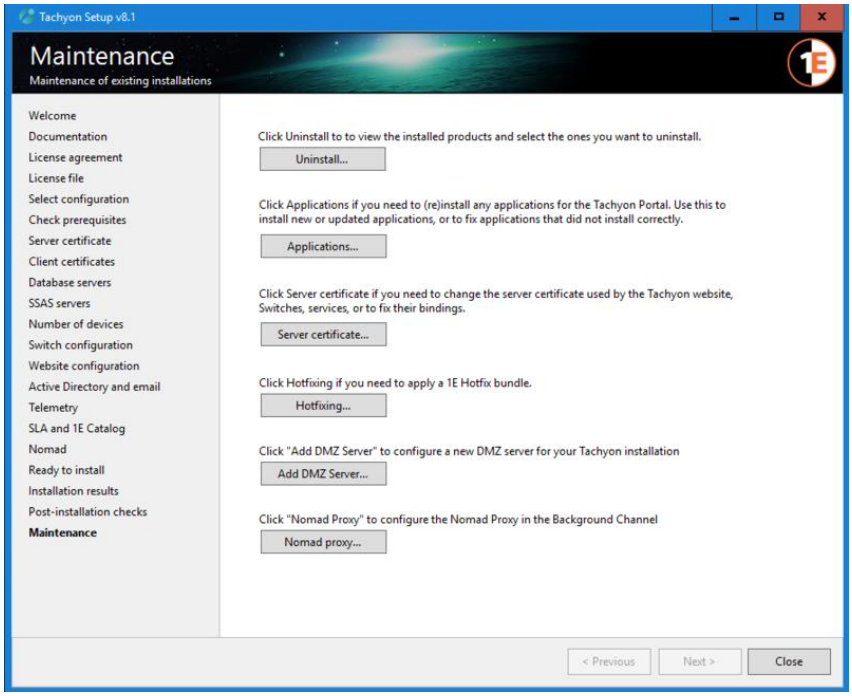
Note

A 1E Hotfix bundle contains the latest hotfixes for a specific version of Tachyon. It consists of a manifest XML file containing commands, and files which can include scripts as well as MSP files, to patch one or more components on the local server.

If you need to apply a 1E Hotfix bundle, then you must run Tachyon Setup on all of your Tachyon servers, according to the instructions provided with the bundle.

See screens below:

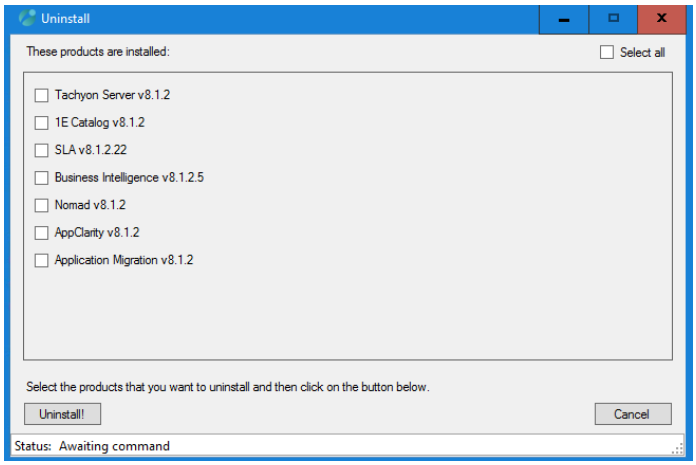
- Uninstall
- Applications maintenance
- Certificate Bindings
- Upload and apply a 1E Hotfix bundle
- Add DMZ Server
- Nomad Proxy.



1.4.2.3.2 Uninstall

From this screen, you can **uninstall** all or some of the components deployed from **Tachyon Setup**.

> **Note**
>
> **Tachyon Setup** is the recommended method of uninstalling all or individual components instead of using the Windows Control Panel.
>
> This is because Tachyon Setup can undo any changes that were done after deploying the components, which would not be undone by the standard application uninstaller. For an example of why this is important, see the information box below.



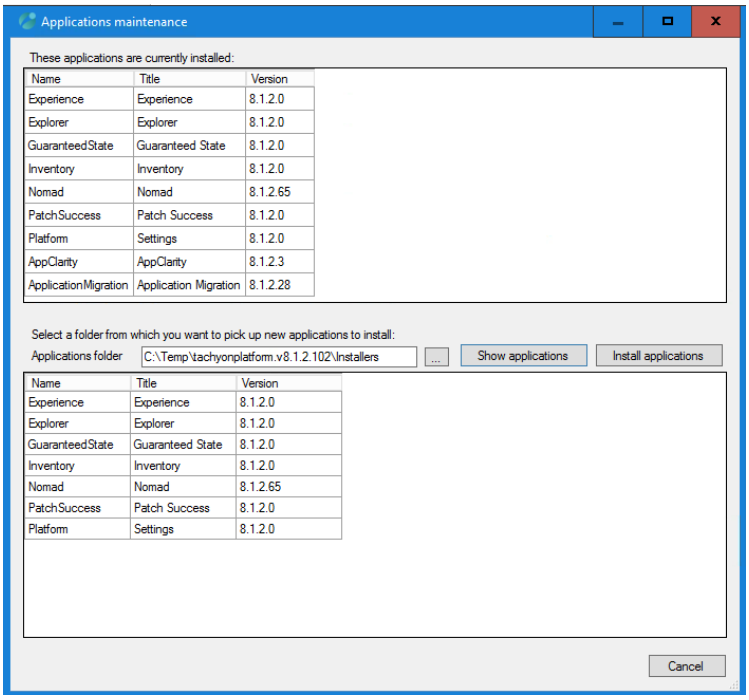
1.4.2.3.3 Applications maintenance

In this dialog, you can select to install or re-install any Applications used by the Portal.

The top grid displays the Applications that are already installed and their versions.

To install or re-install applications:

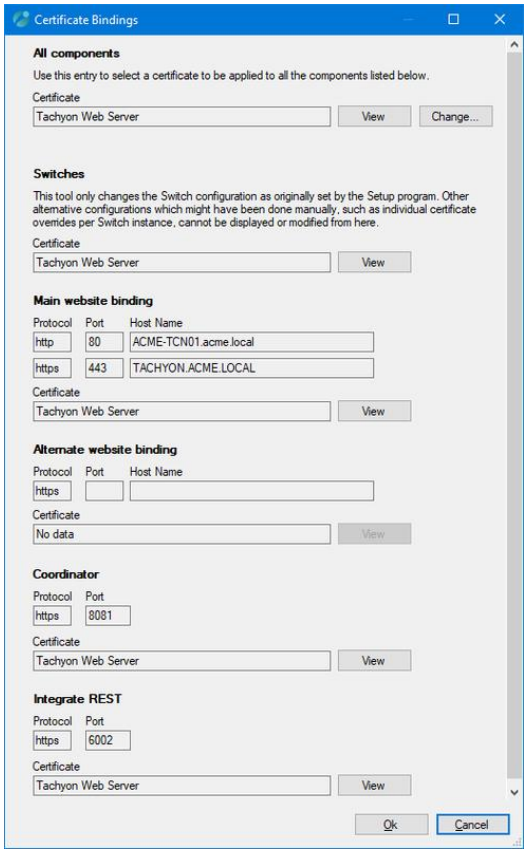
1. Type or select a folder in the **Applications folder** field.
2. Click on **Show Applications**. Doing this displays all applications found under the selected folder. The Applications are displayed using the **Name**, **Title** , and **Version**.
3. Click on **Install Applications**. This will upload the Applications into the server:
   - Any newly uploaded Applications are added to the server
   - Any uploaded Applications with a newer version number will replace the older versions
   - If any uploaded Application has a version number prior to an existing Application, an error message will be generated and the version will not be downgraded.



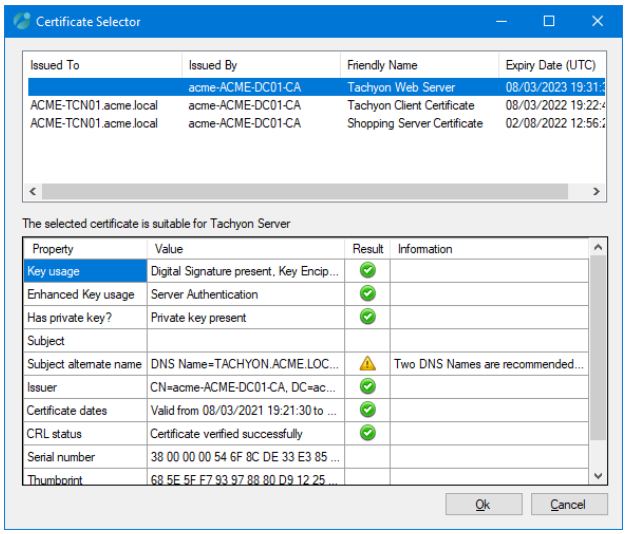
1.4.2.3.4 Certificate Bindings

In this dialog, you can change the certificate bindings used by the Switches, Website, Coordinator, and Integrate REST components. Currently, you can apply one certificate across all the components.

To view the certificate that is being used, click on any of the View buttons.



To change the certificate, click the **Change...** button and select the new certificate from the **Certificate Selector** dialog subsequently displayed. This dialog behaves in a similar way to the Server certificate screen displayed earlier in Tachyon Setup. When you've finished making the selection in the **Certificate Selector**, click **Ok**.



The certificate displayed for the Switches, Website, Coordinator, and Integrate REST components will then change to the selected certificate. Click **Ok** in the **Certificate Bindings** dialog to apply the changes.

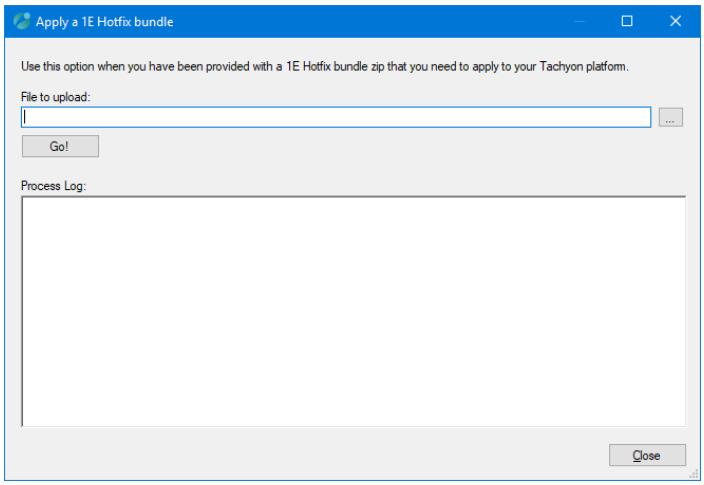
1.4.2.3.5 Upload and apply a 1E Hotfix bundle

In this dialog, you can locate and upload a 1E Hotfix file, using the **...** button at the end of the **File to upload:** field.

After locating the file, you click on the **Go!** button.

The **Process Log** will show the result of attempting to upload the Hotfix.

> **Note**
>
> A 1E Hotfix bundle contains the latest hotfixes for a specific version of Tachyon. It consists of a manifest XML file containing commands, and files which can include scripts as well as MSP files, to patch one or more components on the local server.
>
> If you need to apply a 1E Hotfix bundle, then you must run Tachyon Setup on all of your Tachyon servers, according to the instructions provided with the bundle.



1.4.2.3.6 Add DMZ Server

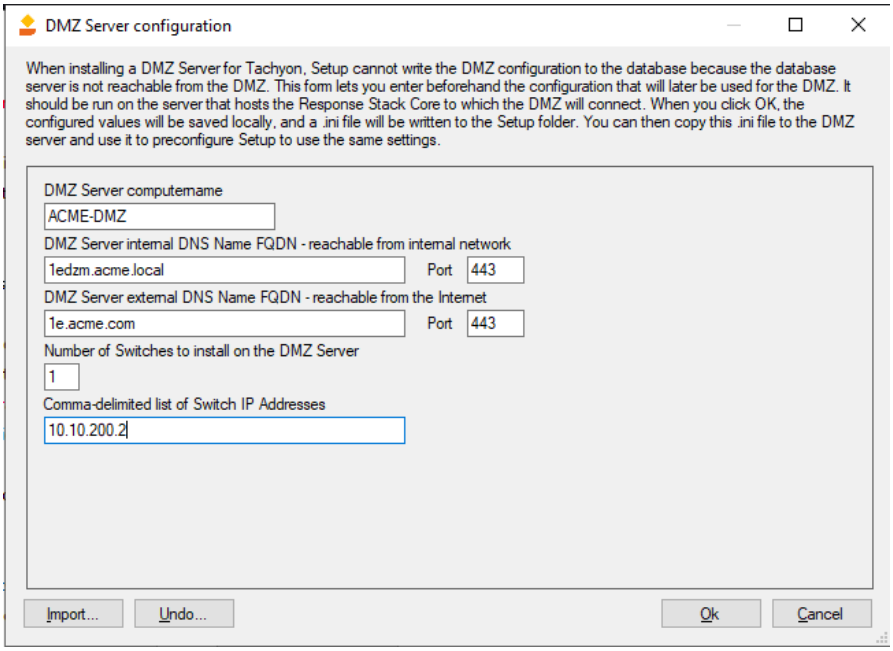
> **Note**
>
> Tachyon Setup provides a two-stage process to install a new DMZ Server:
>
> 1. Run Setup Maintenance on the Response Stack server (specifically the server that hosts the Core which the DMZ Server will connect to) to prepare the Response server and its database, and store details in an **ini** file
> 2. Run Setup to install the DMZ Server using the prepared **ini** file.
>
> The two-stage process and its **ini** file are required because the setup is unable to communicate through the DMZ firewall. In previous versions of Tachyon , the first stage required complex manual configuration.
>
> To upgrade a DMZ Server, you only need to run setup on the DMZ Server, you do not require the **ini** file.

Stage 1 of a two-stage process for installing the DMZ Server. Please refer to Implementing a Tachyon DMZ Server for full details on how to use this screen and install a 1E on a DMZ Server.

The **Import...** button allows you to read an existing or prepared **ini** file.

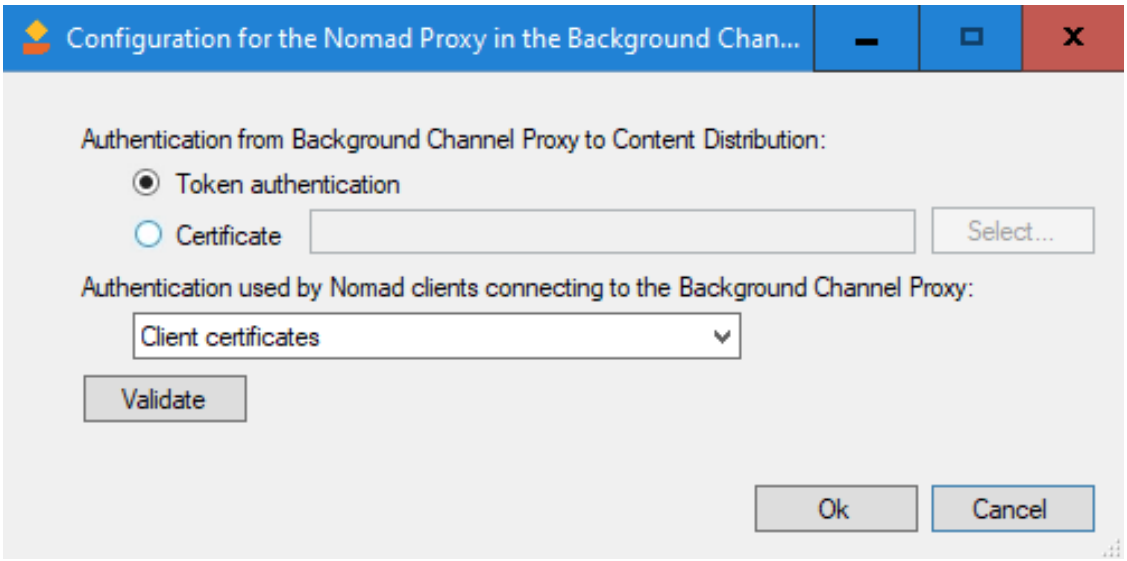
The **Undo...** button allows you to undo the changes written to the database so that your server will not think anymore that you have a DMZ Switch and Background Channel. This can be useful if you find an error in your configuration or if you need to revert the changes to avoid the errors mentioned above, or if you wish to uninstall your DMZ server.

If you need to do this after you have already closed the form, you can re-open it and reload the information by means of the **Import...** button.



1.4.2.3.7 Nomad Proxy

Selecting the proxy option lets you configure the communications and certification options for the Background Channel Proxy.



Authentication from Background Channel Proxy to Content Distribution	Determines how the Background Channel Proxy communicates with the Content Distribution application. You have the following options: **Windows authentication** — Windows authentication will be used to authenticate communications between the Background Channel and Content Distribution. **Certificate** — On choosing this option, you then need to select a valid **Client Authentication certificate** on the local server, that will be used to authenticate communications from the Background Channel by the Content Distribution component. Use the **Validate** button to verify the selected certificate.
Authentication used by Nomad clients connecting to the Background Channel Proxy	Determine how the Nomad clients will authenticate with the Background Channel Proxy. This is separate from the Nomad client configuration for Peer-to-Peer communication features. You have the following choices:

Client certificates	This option is the natural choice if you have also chosen, in the Client certificates screen above, for clients to their present client authentication certificates to Switches on the same server as the local Background Channel. Use this if either of the following is true: • You are installing the Background Channel on a DMZ Server that is not domain-joined • Any of your 1E Clients are non-Windows or not domain-joined

	(workgroup) computers.
Windows authentication	Use this if you do not wish to use client certificates. This option is only possible if the local server is domain-joined, which is not typical for a DMZ Server. All your 1E Clients must be domain-joined computers in domains trusted by the domain of the Response server.
None	If neither of the above options is possible. This means any clients will connect Anonymously.

Note

The Background Channel provides a reverse proxy feature that forwards communications from Nomad clients (internal and external) to the Content Distribution API, devices that are external to the organisation will communicate via the 1E DMZ server.

1.4.2.4 Next Steps

After installation, you should do the following:

- Tachyon Server post-installation tasks
- Deploying 1E Client
- Verifying.

1.4.3 Verifying

Basic verification tests that cover a single-server installation of the Tachyon Server. These tests only cover Tachyon and do not verify the configuration of 1E client modules with other 1E products. These tests should be run in series. They start with basic server checks, then testing 1E Clients, and finally, use the verification instructions from the **Tachyon platform** Product Pack to do end-to-end tests that confirm all components are working. Depending on the decisions you have made during the design phase of your implementation you may need additional tests to verify your implementation.

> **Note**
>
> Please ensure you complete all verification tests. They not only confirm your system is operational, but they also introduce you to concepts and tasks that you will use later when using Tachyon.

To run these tests you need:

1. Tachyon Server installed.
2. Remote workstation with a Supported Platforms.
3. The name and password for the **server installation account**.
    a. The AD account must be enabled.
    b. The account may already be assigned to other Tachyon roles either directly or via membership of an AD group role.
4. Two AD User accounts, **Test User 1** and **2**.
    a. Must not be existing Tachyon users because they will be assigned specific roles for the purpose of these tests.
    b. Must have email addresses and be able to read emails.
5. The **1E Tachyon Platform** instruction set with two Verification instructions.
    a. The verification steps describe how to create this instruction set by uploading the 1E Tachyon Platform Product Pack.
    b. You may have already uploaded this Product Pack using the Tachyon Product Pack Deployment Tool, either during setup or after.
    c. The 1E Tachyon Platform Product Pack is included in the **TachyonPlatform zip** file that you can download from the 1E Support Portal (https://1e.my.site.com/s).
6. At least one test device on which the 1E Client will be installed.

7. 1E Client installation source files and configuration details required by your implementation.

1.4.3.1 Verify Tachyon Server installation

To run the following tests you need:

1. Tachyon Server installed.
2. The name and password for the **server installation account**, account must also be enabled.

Ref	Test	Expected	Remediation
TCNI01	• Logon to the Tachyon Server using the **server installation account** • Confirm Tachyon Server is listed in Apps/Programs and Features • Confirm Windows services are running.	Programs and Features (appwiz.cpl) displays **Tachyon Server** with the correct version number. If an MSP update has been installed, the Installed Updates displays **1E Tachyon Server Update (Qnnnnn)**. The following Windows services exist and are running. • **1E Catalog Update Service** (Automatic) (Network Service) • **1E SLA Platform Engine** (Automatic Delayed start) (Network Service) • **1E SLA Platform Integrate Agent** (Automatic Delayed start) (Network Service) • **1E SLA Platform Integrate Manager** (Automatic Delayed start) (Network Service) • **1E Tachyon Coordinator** (Automatic Delayed start) (Network Service) • **1E Tachyon Switch Host** (Automatic Delayed start) (Local System)	If any of the services are not running, then check the corresponding log(s). The **Switch Host** service will stop after several seconds if it is unable to start any Switches. The **ConsumerAPI** log is not created until a user (the **server installation account**) successfully connects to the Tachyon portal. The **Background**

<table>
<tr><th>Ref</th><th>Test</th><th>Expected</th><th>Remediation</th></tr>
<tr><td></td><td></td><td></td><td>API log is not created until a 1E Client attempts to download content. The 1E Tachyon Platform Product Pack can be used to trigger this.

The Coordinator service will stop after several seconds if it is unable to activate the license.</td></tr>
<tr><td>TCNI02</td><td>• Check the Tachyon Server logs.</td><td>The default location for all logs is the folder %ALLUSERSPROFILE%\1E

<table>
<tr><th>Subsystem</th><th>Component</th><th></th><th></th></tr>
<tr><td>Tachyon Master</td><td>Tachyon Portal UI and applications.</td><td>1E\Tachyon\</td><td>Tachyon.Portal.log</td></tr>
</table>
</td><td></td></tr>
</table>

Ref	Test	Expected				Remediation
		Consumer API	1E\Tachyon\	*Tachyon.ConsumerAPI.log*		
		Coordinator service	1E\Tachyon\	*Tachyon.Coordinator.log* *Tachyon.Instrumentation.log*		
		Experience web application	1E\Tachyon\	*Tachyon.Experience.log*		
		Catalog	Catalog UI (CatalogWeb - Admin sync)	1E\Catalog\	*Catalog.Integration.UI.log*	
		Catalog API				
		Catalog Update Service	1E\Catalog\	*Catalog.UpdateService.log*		
		Content Distribution	Nomad web application	1E\ContentDistribution	*ContentDistribution.log*	
		SLA	SLA/Platform APIs	1E\Tachyon\	*Tachyon.AdminAPI.log*	

Ref	Test	Expected			Remediation
			(Admin, Core External)		
		SLA Platform UI (Platform)	1E\SLA Platform\	*Web.log*	
		SLA Engine	1E\SLA Platform\	*Engine.log*	
		SLA Integrate Services (Connector Manager)	1E\SLA Platform\	*1E.SLAPlatformIntegrateAgent.log* *1E.SLAPlatformIntegrateManager.log* *1E.SLAConnector.<type>_sync.log*	
		SLA Inventory	n/a	*n/a*	
		SLA Operations Provider (not currently used)	1E\Platform Consumer\	*n/a*	

Ref	Test	Expected				Remediation
		SLA databases (Data, Integrate, Shared)	n/a	*n/a*		
		BI	MDX API	SQL database	*[SLA-BI].[BI].[Event Log]*	
		Tachyon Response	Core	1E\Tachyon\	*Tachyon.CoreAPI.log*	
		Background Channel (Background)	1E\Tachyon\	*Tachyon.BackgroundAPI.log*		
		Switch(es) (also includes a single Switch Host service)	1E\Tachyon\	*Tachyon.Switch.4000.SW1.log* *Tachyon.Switch.Host.log*		

Please refer to Services and NTFS Security if changing the location of log files.

In this version of Tachyon Server, some installers do not support the LOGPATH property and the logs folder is not configurable during installation.

Each component has a configuration file in the Tachyon Server installation folder structure, which contains log configuration details. Defaults are:

Ref	Test	Expected	Remediation

- Filepath *%ALLUSERSPROFILE%\1E\<product>* where product is Tachyon, SLA Platform, and Catalog
- Filename as shown in the table above.
- Maximum size 10MB (2MB for Switch logs).
- 2 rollover files numbered 1 to 2 with the rollover number included as n.log (5 rollover files for Switch logs).
- Date and timestamps are UTC to help troubleshooters synchronize logs on systems in different time zones.

Switch logs have the following names:

- The first Switch installed will typically have a log filename **Tachyon.Switch.4000.SW1.log** (where 4000 is the port it is listening on and SW1 is the **config name** in the SwitchConfiguration table in the TachyonMaster database).
- Other Switches on the same server will have different config names appended.
- The log filename will be unique on a server, but there may be the same named log on a different server.
- A Switch will continue to use the same log unless the SwitchConfiguration table is modified so that a different ID is used.
- If you see a Tachyon.Switch.log without a config name appended, this is a special case where a Switch cannot find its correct configuration and has fallen back to using the template * row which has ID=1. In which case you will need to troubleshoot how that happened.

Ref	Test	Expected	Remediation
		• Rollover logs have numbers appended, for example, Tachyon.Switch_A.1.log, up to a default maximum of 5. Tachyon server components use the **log4net RollingFileAppender** class. Details can be found in http://logging.apache.org/log4net.	

1.4.3.2 Verify IIS security of the Tachyon website

The following are basic verification tests. If you want a detailed check of IIS configuration, please refer to Server installation issues.

To run the following tests, you need:

1. Tachyon Server installed.
2. The name and password for the **server installation account**, account must also be enabled.
3. Remote workstation with a Supported Platforms - using a remote workstation is important because you will get different results if using a local browser.

Ref	Test	Expected	Remediation
TCNI03	• Start a Supported Platforms on a workstation (not the Tachyon Server) • Connect to the portal using: – **server installation account** – URL for example https://tachyon.acme.local/Tachyon	Successful connection to the **Tachyon portal** showing the following applications, if licensed: • **AppClarity** • **Application Migration** • **Experience** • **Explorer** (included with all licenses) • **Guaranteed State** • **Inventory** (included with all licenses)	Ensure the **server installation account** is enabled to do this test. It has the necessary rights to access Tachyon, as well as NTFS rights on the Tachyon Server. **401 'Unauthorized'** Typically, the website also prompts you to provide an account and password. This may occur if you are using invalid credentials or an account in a domain that is not trusted by the Tachyon Server.

- **Nomad**
- **Patch Success**
- **Settings** (included with all licenses).

The ability to open applications and navigate around them will depend on which roles have been assigned to the logged-on account.

For a new installation, the**server installation account**is only able to open the**Settings**application and view the following pages, because it is only assigned to the **Installer** role:

- Configuration
  - Custom properties
    - Device Tags (view)
    - Software Tags (view).
  - Consumers (view, add)
  - License information (view, reactivate)

403 'Access denied'

When you use a browser to open an application in the Tachyon portal, you will see **Server Error 403 - Forbidden: 'Access denied'** if the internal account used by the Application Pool does not have read access to the Tachyon web application folders. This can happen if Tachyon is installed in a non-default location and the NTFS permissions on the installation folder are not correct. To remedy the issue, you should review and correct NTFS permissions as described in Services and NTFS Security.

404 'File or directory not found'

Is the URL you entered correct, and have the correct spelling?

Is the corresponding web application installed? For example, the Consumer application may not be installed.

Contact system administrator to get access

– System information (view, export telemetry) – Branding (view, edit, reset). • Monitoring – Infrastructure log (view) – Audit information log (view) – System health (view) – Audit information log (view). • Permissions – Users and Groups (view, add) – Roles (view all roles - add, edit, and delete custom roles) – Management groups (view)	When you use a browser to open an application in the Tachyon portal and you see the message **Unauthorized access**, it means your AD account is not a Tachyon user. Try using an AD account that you know is a Tachyon user that is assigned to a Tachyon system role or custom role. For example, use the **server installation account** which is automatically installed as a Tachyon user. For a new installation, the **server installation account** must be used to add other users before their AD accounts can be used to access Tachyon applications. This process is described in the Users and Groups page and the Roles page. It is used in the following TCNU verification tests, refer to Verify user rights assignment for details.

		– Assignments (view, edit). • Instructions – Instruction sets (view, add, move, delete, upload, download).
TCNI04	• Change the web browser URL from /Tachyon to **/Consumer**	The web browser will respond with the version number of the **Tachyon platform** (IE will download as a JSON file, and other browsers will display a response in XML format). Confirm the Version number is as expected.
TCNI05	• Change the web browser URL from /Tachyon to **/**Admin	The web browser will respond with the version number of the **SLA Platform** (IE will download as a JSON file, and other browsers will display a response in XML format). Confirm the Version number is as expected.
TCNI06	• Change the web browser URL from /Tachyon to **/**Background	The web browser will respond with **You have reached Tachyon background API.** (IE will download as a JSON file, other browsers will display a response in XML format).

TCN I07	• Change the web browser URL from /Tachyon to **/Core**	The expected response is **Server Error 403 - Forbidden: Access is denied**. For security reasons, access to these web applications is allowed for local users and services only and denied to remote devices. If the response is **You have reached Tachyon Core API** then there is an issue with IIS configuration. Or, you are using a browser on the actual Tachyon Server, and should do the test on a remote workstation.	**Access Allowed** It should not be possible for a remote web browser to have access to the **Core** web application. If access is possible, then it is probable that the IIS role feature **IP Address and Domain Restrictions** is not installed on the Tachyon Server. You must ensure this IIS feature is installed, as described in the Server installation issues page. The setup installer verifies this prerequisite and optionally deploys the feature if it is missing.
TCN I08	Deleted test		
TCN I09	• Change the web browser URL from /Tachyon to **/Platform**	The web browser will take you to the SLA Inventory web application.	
TCN I10	• Change the web browser URL from /Tachyon to **/CatalogWeb** • Change the web browser URL from **https** to **http** and also change the server name so	In both cases, the web browser will take you to the **1E Catalog** website. If you use **http** while leaving the same server address used for **https**, the expected response is	To access the **Admins** tab in the CatalogWeb, you must manually add one or more administrator accounts or groups to the website configuration. Please refer to Rebuilding the 1E Catalog.

that it matches the value that you specified during installation for the *HTTP host header*. For example: http://ACME-TCN01.acme.local/CatalogWeb	**HTTP Error 404 - Not Found**. The 1E Catalog can use both **http** and **https** provided that you specify the correct server name for each protocol. For interactive use, you are recommended to use https. Http is provided for internal compatibility with existing consumers. **Note** An HTTP connection will fail if the HTTP binding has been deliberately removed (Tachyon Server post-installation tasks).

1.4.3.3 Verify user rights assignment

To run the following tests, you need:

1. Tachyon Server installed and above TCNI verification tests passed, refer to Verify Tachyon Server installation for details.
2. The name and password for the **server installation account**, account must also be enabled.
3. Two AD User accounts, **Test User 1** and **2**.
    a. Must not be existing Tachyon users because they will be assigned specific roles for the purpose of these tests.
    b. Must have email addresses and be able to read emails.
4. The **1E Tachyon Platform** Product Pack, if not already installed.

Note

1E is often asked why the **1E Tachyon Platform** Product Pack is not built into the product. The reason is that uploading a known Product Pack is part of the verification process and ensures the user is able to upload at least one pack and carry out all the other necessary tasks at least once before exploring other aspects of Tachyon.

Ref	Test	Expected Response	Remediation
TCN U01	• Download the **TachyonPlatform.zip** file from the https://support.1e.com/. • Extract the **1E-Tachyon-Platform.zip** from the ProductPacks\Classic folder • Start a Supported Platforms on a workstation • Connect to the Tachyon portal as the **server installation account** • Open the **Settings** application and go to the **Settings→Instructions→Instruction sets** page • Click on the **Upload** button • In the Open dialog navigate to the location of the **1E-Tachyon-Platform.zip** file • Select the **1E-Tachyon-Platform.zip** file and click **Open**. All the instructions contained in the zip file will initially be added to the default **Unassigned** instruction set. Instructions in the **Unassigned** instruction set cannot be used, so you will need to add the instructions to a new instruction set:	You will upload the **1E Tachyon Platform** Product Pack and assign them to a new instruction set called **1E Tachyon Platform**. For a new installation, the **Instruction sets** page will not contain any instruction definitions. After uploading the **1E Tachyon Platform** Product Pack, the two instructions contained in the Product Pack will be displayed on the **Product packs** page. After creating the **1E Tachyon Platform** instruction set, this will appear in the Instruction sets list. After moving the verification instructions from **Unassigned** to the **1E Tachyon Platform** instruction set, the instruction count for the **1E Tachyon Platfor**	If the **server installation account** is not able to add instructions from a Product Pack, then the installation account is not assigned to the **Full Administrator** role. You can confirm if this is the case by viewing the rights of the **server installation account** in the **Settings→Permissions→Users** page. You may have upgraded from a previous version where the **server installation account** was not automatically assigned to this role. Contact 1E for advice on how to fix this.

	• Select the 2 verification instructions to the new set, by clicking the checkbox at the start of each instruction row in the list. • Click the **Add new set** button in the button panel to the right of the page • In the **Add new instruction set** popup subsequently displayed, and type **1E Tachyon Platform** as the name • Ensure that the **Include 2 selected instructions** checkbox is checked • Click the **Add** button to add the new instruction set, with the selected instructions.	**m** instruction set will go up by **2**. **Note** Unlike some earlier versions of Tachyon, this version does not support the drag+drop method of uploading Product Packs. **Tip** You can use the Tachyon Product Pack Deployment Tool tool instead.	
TCN U02	• Connect to the Tachyon portal as the **server installation account** • Open the **Settings** application and go to the **Settings→Permissions→ Users and Groups** page	Entering one or more characters and clicking the search icon returns a list of matching user accounts and security groups. Selecting a group and viewing its members shows the	The purpose of this step is to confirm the system is capable of searching Active Directory. You do not need to add the group; you will add users in the next step. The ability to search and find different types of AD security groups depends on the search method selected during the installation of the Tachyon

	• Click **Add** and search for an AD Universal security group • Select one of the AD security groups and click **Add** • Click on the name of the AD group just added • In the **Group:** details page, view the group members • Navigate back to the **Users and Groups** page • Check the checkbox for the group just added and click **Remove** and then click **Yes, remove group**.	Name and Email of each member.	Server, as described in Directory requirements.
TCN U03	• Connect to the Tachyon portal as the **server installation account** • Open the **Settings** application and go to **Permissions→Users and Groups** page • In the **Users and Groups** page click on **Add**. • In the **Add User** prompt under **Select AD user or security group** type in the search box **Test User 1** and click on the search icon	The following custom role exists: • **1E Tachyon Platform** The following users are included in the list of Users. • **Server installation account** - assigned to the **Installer** role • **Test User 1** - assigned to roles: – •	

- Select **Test User 1** from the search results and click on **Add**.
- Repeat the same steps to add **Test User 2**.
- Go to the **Permissions→Roles** pag e
- Add a custom role named **1E Tachyon Platform**.
- Click on the name of the role that you just added. This will take you to the Permissions tab. Add permission with the following properties:
  - Type: **Instruction Set**
  - Name (of the Instruction Set): **1ETachyonPlatfo rm**
  - Permissions: **Actioner, Approv er, Questioner, V iewer**
- Click on **Add**
- Assign Management Group: **All Devices**
- Go to the **Members** tab and add **Test User 1**
- Role: **1E Tachyon Platform**
- Repeat for **Test User 2**.

- **Test User 2** - assigned to roles:
  - –
    -

Note

You will also see some system and machine accounts in the list of users.

			These are used internally for interaction with other components and should not concern you at this time.
TCN U04	• Connect to the Tachyon portal as **Test User 1** and confirm access to **Explorer** pages • Repeat for **Test User 2**	Each Test User is able to view the following menu pages in the **Explorer** application: • Home • Instructions – History – Tasks – Scheduled • Devices – Table – Dashboard • Notifications	**Contact system administrator to get access** When you use a browser to open an application in the Tachyon portal and you see the message **Unauthorized access**, it means your AD account is not a Tachyon user. Try using an AD account that you know is a Tachyon user that is assigned to a Tachyon system role or custom role. For example, use the **server installation account** which is automatically installed as a Tachyon user. For a new installation, the **server installation account** must be used to

add other Tachyon users before their AD accounts can be used to access Explorer. This process is described on the Users and Groups page and the Roles page.

403 'Access denied'

When you use a browser to open an application in the Tachyon portal, you will see **Server Error 403 - For bidden: 'Access denie d'** if the internal account used by the Application Pool does not have read access to the Tachyon web application folders. This can happen if Tachyon is installed in a non-default location and the NTFS permissions on the installation folder are not correct. To remedy the issue, you should review and correct NTFS permissions as described in Services and NTFS Security.

1.4.3.4 Verify 1E Client installation

To run the following tests you need:

1. Tachyon Server installed and TCNI verification tests passed, refer to Verify Tachyon Server installation for details.
2. Two user accounts, **Test User 1** and **2** , and above TCNU verification tests passed, refer to Verify user rights assignment for details.

3. At least one test device on which the 1E Client will be installed.
4. 1E Client installation source files and configuration details required by your Tachyon implementation.

Ref	Test	Expected Response	Remediation
TCNA01	• Install the 1E Client on the test device using the configuration settings required for your implementation – DNS Alias of Tachyon Server	1E Client installed. Programs and Features display **1E Client**. • Correct platform x86 or x64 • Correct version number. If an MSP update has been installed, the Installed Updates displays **1E Client Update (Qnnnnn)**.	The first clients can be installed manually or using a script. You should repeat this set of tests when you have deployed a few clients using your organization's preferred deployment method. You may need to edit the 1E Client configuration file after installation, to suit the requirements of your implementation, and restart the 1E Client service.

- Portusedbythe Tachyon Switch
- Portusedbythe Tach

	y o n B a c k g r o u n d C h a n n e l. • Include optional MSP update • Confirm Programs and Features.		
TCN A02	• Confirm Windows services are running	The following Windows services exist and are running. • **1E Client** • **1E Nomad Branch** - only if Module.Nomad.Enabled=true	If the **1E Client** service is not running, then check the Client log.
TCN A03	• Check the 1E Client log.	No errors.	Check the **Switch** setting in the Client configuration file is using the correct DNS Alias for the

		To view LOG file locations for each OS platform, click to expand... **1E Client logs on Windows** %ALLUSERSPROFILE%\1E\Client\1E.Client.log (used by 1E Client and Tachyon features, and Shopping client) %ALLUSERSPROFILE%\1E\Client\NomadBranchUninstall-YYYY_MM_HHTMM_HH_SS_000Z.log **1E Client logs on macOS** /Library/Logs/1E.Client.Daemon.log (shows any service start errors) /Library/Logs/1E.Client.log (shows the current operation of the 1E Client) **1E Client logs on other non-Windows platforms** /var/log/1E/Client/1E.Client.log	Tachyon Server, and the correct port for the Switch. If errors in the Client log relate to certificates, then see Client issues.
TCN A04	• Start a supported browser on a workstation, refer to Supported Platforms for details. • Connect to the Tachyon	Each **Test Device** is listed on the Tachyon **Devices Table** page. The device details show information about the device's system, activity, certificate, and configuration settings.	If you cannot use the **Test User 1** or **2** accounts, then use another Tachyon user account. All Tachyon users are able to view the **Devices Table** page. Check the configuration of the client and review the Tachyon client settings in the 1E Client configuration file. To view CONF file locations for each platform, click to expand... The 1E Client is controlled via the 1E Client configuration file **1E.Client.conf** which resides in the

portal as **Test User 1**

- Open the **Explorer** application and go to the **Devices →Table** page
- For each **Test Device** that has had the 1E Client installed, confirm the device is listed in the **Table** page.
- Click on each device and view the device properties.

installation folder along with the 1E Client executable.

The default installation location used for the different OS supported by the 1E Client are given in the following table:

OS	Default install location
Windows	**%ProgramFiles%\1E\Client**
Linux and Solaris	**/etc/1E/Client**
Mac	**'/Library/Application Support/1E/Client'**

Note

The configuration file uses ASCII encoding.

A comment line starts with the # symbol.

1.4.3.5 Verify Tachyon client-server communications (stage 1 and 2 instructions)

To run the following tests you need:

- Tachyon Server installed and above TCNI verification tests passed, refer to Verify Tachyon Server installation.
- At least one test device has 1E Client installed and above TCNA verification tests passed, refer to Verify 1E Client installation.
- Two AD user accounts configured as Tachyon users and above TCNU verification tests passed, refer to Verify user rights assignment.

To run the following tests you need to logon to a workstation with a user account that is assigned to at least one of the Tachyon administration roles. 1E Tachyon Platform Product Pack describes the purpose of each of its verification instructions.

Ref	Test	Expected Response	Remediation
TCNA01	See TCNA01 above.	Each **Test Device** is listed on the Explorer Devices page.	
TCNA05	• Connect to the Tachyon portal as **Test User 1** • Open the **Explorer** application and go to the **Home** page • Type **verification** • Select **Tachyon Platform verification stage 1** • Click **Ask this question**	When the **Tachyon Platform verification stage 1** question is asked, the Explorer view changes to the **Instruction History Responses** page. The **Instruction History Responses** page lists the software products installed on each Test Device. Contents are shown for online Devices that have the 1E Client installed and running. If you view other Explorer pages and want to get back to the **Instruction History Responses** page, then you should select	You may need to refresh the **Instruction History Responses** page. Verification stage 1 tests communication between the 1E Client and Switch. Any issues will appear in the Client log. Check each test device has the 1E Client running and is online.

		Instruction History from the navigation menu on the left side, and you should see a list of the instructions that have been run. You may then click on the name of the instruction to view its responses. The Client log indicates: • Running instruction • Successfully processed instruction.	
TCN A06	• Connect to the Tachyon portal as **Test User 1** • Open the **Explorer** application and go to the **Instructions→History** page • Click on the **Tachyon Platform verification stage 1** instruction to view the response details • Click on the **Actions** tab • Type **verification** • Select **Tachyon Platform verification stage 2 (all platforms)** • Click **Perform this action** • Enter the password for the **Test User 1** account • If 2FA is enabled, enter the **authentication code**	If Two-Factor authentication (2FA) is enabled, then Explorer will prompt for an authentication code, and **Test User 1** should receive an authentication code by email. The Explorer view changes to **Instruction pending approval**. **Test User 2** should receive an email asking for approval.	This stage of the Verification tests communication between the Tachyon Server and the SMTP relay/gateway. If 2FA is enabled and **Test User 1** does not receive an email with the authentication code, then: • Check the Coordinator log and confirm it is using the correct configuration for the SMTP server

				If **Test User 2** does not receive an email, then: • Check the user is assigned to the **1E Tachyon Platform** role • The **1E Tachyon Platform** role has access rights which include **Approver** • Check the Coordinator log and confirm it is using the correct configuration for the SMTP server.
TCN A07	• Either connect to the Tachyon portal as **Test User 2** and click on the **notification icon** • Or click on the link in an email received in the previous step and wait for a browser to connect you to the Tachyon portal • View the **Request for action approval** for the	When clicking on the link in the request for approval email, a browser should open automatically and take you to the Notifications page. You can view notifications and approval requests at any time by clicking on the notification icon. The icon will show the number of actions pending		If **Test User 2** is unable to approve the request, then: • check the user is assigned to the **1E Tachyon Platform** role • the **1E Tachyon Platform**

	Tachyon Platform verification stage 2 (all platforms) action • Tick the box **I understand approving my request impacts my IT environment** • Click **Approve**.	approval by the logged-on user. When the request is approved by **Test User 2**: • The Explorer view changes to **Approval has been processed successfully** • **Test User 1** should receive an email saying the action has been approved.	role has access rights which include **Approver**.
TCNA08	• Connect to the Tachyon portal as either **Test User 1** or **2** • Open the **Explorer** application and go to the **Instructions→History** page • Click on the **Tachyon Platform verification stage 2** instruction to view the response details.	Response details show a list of devices and their Client configuration details. You may need to refresh the Details page. This stage of the Verification tests the Client's connection to the Background Channel. Successful execution of the action will cause the following to appear in the Client log: • Duplicate log entries showing a repeat run of the previous question • A series of log entries showing a connection to the Background Channel, then a script is	Repeat test TCNIO5 using a browser on the test device to confirm the Background Channel has been configured correctly. A common error is an incorrect value for the **BackgroundChannelUrl** setting in a 1E Client configuration file. If you deployed the client using a software deployment tool like Microsoft's ConfigMgr then look to see if similar devices have the same issue. Check the 1E Client configuration file on problem devices to see if the setting has

	downloaded and run: – Windows - **getConfig.ps1** PowerShell file – Linux and MacOS - **parseconfigStarter.sh** bash and **parseconfig.pl** perl files • Successfully processed instruction. You may have to wait up to 5 minutes for the action to complete on each device. This is because the default 1E Client setting for DefaultStaggerRangeSeconds=300.		the correct URL for the Background Channel. Check to see if the Background Channel has the scripts used by the Stage 2 instruction. Review the contents of **C:\ProgramData\1E\Tachyon\Content** folder on the server hosting your Background Channel. The Content folder should contain at a folder named **1E Tachyon Platform-VerificationStage2** which contains a sub-folders with a PowerShell file, and another subfolder containing a bash and a perl files.

1.4.3.6 Verify extended features

To run the following tests you need:

- All the above tests completed
- To logon to a workstation with a user account that is assigned to at least one of the Tachyon administration roles that allows you to run some instructions, which can include a Verification instruction already used above.

Ref	Test	Expected Response	Remediation
TCNX01	**Export All feature** • To confirm the **Export All** share is accessible, use	This test verifies BCP has been installed on the Tachyon Server,	If you see a popup error initiating an export operation

Windows Explorer to **browse to the share name** specified when the Export all feature was configured

- Connect to the Tachyon portal, open the **Explorer** application and **ask a question**
- After at least one device has responded with content, **stop** the question and **keep** the responses
- In the **Content** or **Status** tab on the **Responses** page, click on **Export all results**
- Enter the **share name** and click **Save**
- Use Windows Explorer to **browse to the share name** and observe a TSV file has been created
- Use Microsoft Excel or Notepad to view the contents of the TSV file.

and an Export share is correctly configured, as described in Tachyon Server post-installation tasks.

When you stop the question or wait for the question to complete its gather duration, then the Export all results button will be enabled.

TSV is a tab-delimited text file.

after clicking on the Export All results button, then:

- Ensure you specify the hostname or hostname FQDN of the Windows computer where the share has been created; do not use a DNS Alias
- Check the share permissions
- Check the share NTFS security.

1.4.3.7 1E Tachyon Platform Product Pack

Instruction text (ReadablePayload)	Type	Description	Instruction file name	Version
Tachyon Platform verification stage 1	Question	Stage 1 of the verification will return all software installed on each 1E Client endpoint. Verification stage 1 is a simple question-type instruction used to verify the:	**1E-TachyonPlatform-VerificationStage1**	19

Instruction text (ReadablePayload)	Type	Description	Instruction file name	Version
		• Authenticated user is able to access and use Tachyon Explorer • End-to-end communication between the Tachyon system, the **Switch** and the platform client.		
Tachyon Platform verification stage 2 (all platforms)	Action	Stage 2 of the verification will run a PowerShell script to return a subset of the current configuration of the platform client features of 1E Client. Verification Stage 2 is normally expected to be run as a follow-up action for Verification Stage 1. Verification stage 2 is a simple action-type instruction used to verify: • Two-factor authentication (if enabled) and approval workflow, which tests email (if enabled) - necessary for action-type instructions • End-to-end communication between the Tachyon system, the **Background Channel** and platform client • The client is able to run PowerShell scripts on Windows OS - many Tachyon instructions and	**1E-TachyonPlatform-VerificationStage2**	21

Instruction text (ReadablePayload)	Type	Description	Instruction file name	Version
		Guaranteed State rules use PowerShell version 3.0 and later • The client is able to run Bash script on non-Windows OS. For details about PowerShell and Bash support please refer to Tachyon scripting requirements. The rate at which Responses are returned to the Tachyon system via the Switch is affected by the 1E Client setting **DefaultStaggerRangeSeconds**. This setting governs a random delay before the instruction downloads the script from the Background Channel. This stagger setting is ignored on Windows OS if Nomad client is enabled - instead only one client per subnet (or site if Nomad SSD is used) will act as master and download the script from the Background Channel, and peer clients will download the script from the master.		

1.4.4 Tachyon Server post-installation tasks

Post-installation tasks, which include verification checks and mandatory and optional configuration tasks.

1.4.4.1 Required tasks

The following tasks must be performed post-installation. You may have already performed some of these tasks as part of following the instructions on the Quick Start.

The Tachyon portal website will be available after installation using the Tachyon DNS Alias FQDN. For example:

Note

https://1e.acme.local/Tachyon/app

1.4.4.1.1 Verify installation

Note

You must perform the verification tests provided on the Verifying page.

1.4.4.1.2 Confirming the Tachyon website HTTPS binding

If you have implemented Tachyon Server on an IIS server that has previously been or is currently used by other applications then there may be other Web Server certificates in the **Local Computer's Personal Certificates store** in addition to the Tachyon Web Server certificate. In earlier versions of Tachyon, it was possible under these circumstances for the Tachyon Server installer to bind to the wrong certificate. The current version contains improved logic for avoiding this problem, but it is still good practice to verify that the configuration is indeed as expected.

To select the correct certificate for the HTTPS binding see the troubleshooting steps for Server installation issues.

If you want to optionally remove the HTTP binding, please refer below to the optional task Removing the HTTP binding from the Tachyon website.

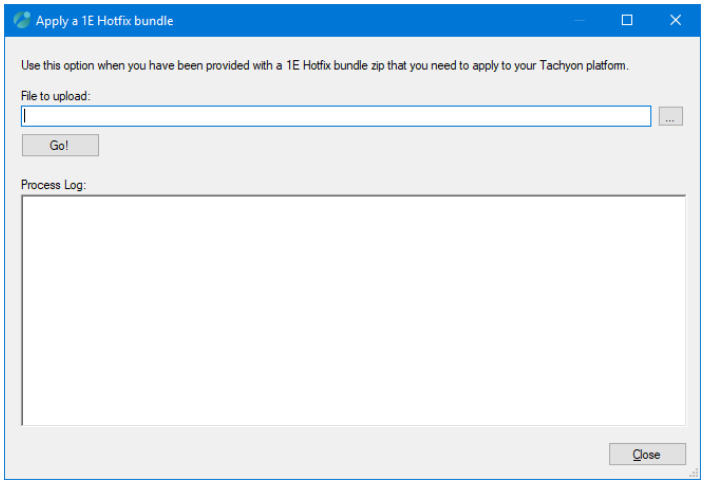
1.4.4.1.3 Apply a 1E Hotfix bundle

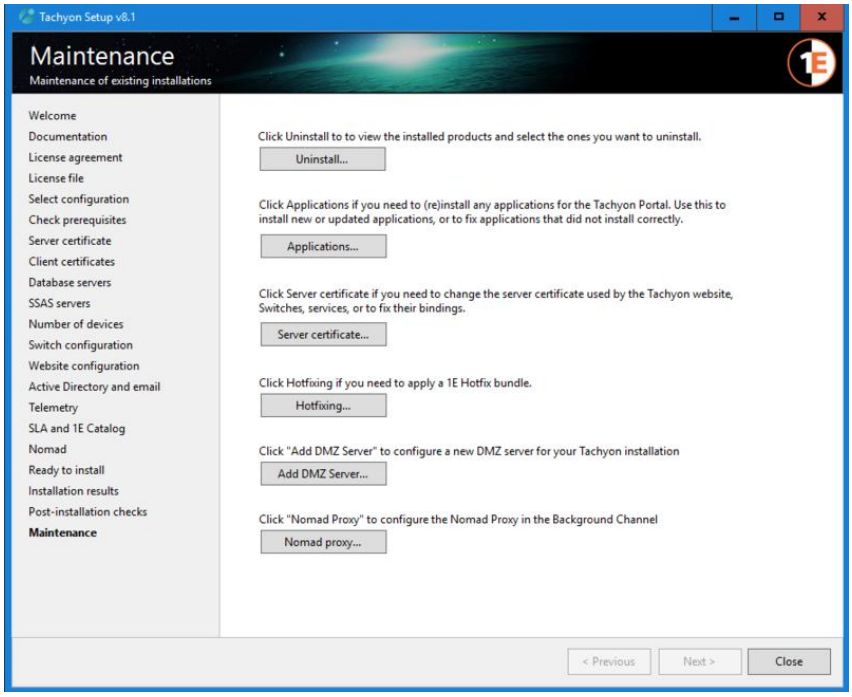
Note

A 1E Hotfix bundle contains the latest hotfixes for a specific version of Tachyon. It consists of a manifest XML file containing commands, and files which can include scripts as well as MSP files, to patch one or more components on the local server.

If you need to apply a 1E Hotfix bundle, then you must run Tachyon Setup on all of your Tachyon servers, according to the instructions provided with the bundle.

1. Start **Tachyon.Setup**
2. Click directly on the **Maintenance** link in the left-hand menu
3. In the **Maintenance** screen, click the **Hotfixing...** button
4. In the **Apply a 1E Hotfix bundle** dialog, click the **...** button to browse for the **File to upload**
5. After locating the file you click on the **Go!** button
6. The **Process Log** shows the result of attempting to upload and apply the 1E Hotfix bundle
7. Click **Close**





1.4.4.1.4 Configure permissions

Immediately after installation, you can only access the **Tachyon portal** and the **Settings** application using the server installation account, until additional users have been added and assigned to their roles.

The installation account is assigned the **Installer** role and cannot be modified because it is a System Principal.

This means that one of your first steps after the installation is to connect to the Portal using the installation account and add other Tachyon users with necessary roles as described in the Users and Groups page and the Roles page.

> **Tip**
>
> After the initial configuration of Tachyon users and groups have been performed, we recommend that the **Installer** role is assigned to one or more other Tachyon users, and

that your server installation account is disabled. It can be enabled later for the installation of updates and upgrades.

This approach of having a dedicated installation account ensures the same account is used for all installation activities and has relevant rights on the Tachyon server and in SQL Server. Disabling it makes it more secure than a normal user account. If an ordinary user account is used for installation tasks, there is a risk the account may be deleted, causing difficulties for future upgrades or re-installation.

1.4.4.1.5 Add Product Packs and configure Instruction Sets

Tachyon functionality is based on Instructions, until these are added to the system you will not be able to ask questions or perform actions. 1E provides instructions in zip files called Product Packs. A collection of Product Packs necessary for zip files is available in the **Tachyon Setup** zip (available on the https://support.1e.com/ and from the 1E Exchange. Each Product Pack contains a related collection of Instruction Definitions. Product Packs and Instruction Definitions can be added by a **Full Administrator**.

When added, Instructions are immediately allocated to the built-in **Unassigned** Instruction set. Instruction sets provide a way of determining the permissions for the Instructions they contain, but the **Unsassigned** Instruction set is only intended as a staging area for newly loaded Instructions - and Instructions in this set cannot be used directly. An Instruction can only belong to a single Instruction set, so after loading it, and before it can be used, it must be moved to another Instruction set - one created by a **Full Administrator**.

Instruction sets created by a **Full Administrator** can be used as the basis for custom roles created by a **Full Administrator** or **Group Administrator**. These custom roles determine the permissions for the Instruction sets and all the Instructions they contain. This enables the administrator to complete the assignment of specific Instruction set roles to users and determine which Instructions they can action, approve, question, or view.

You can either load instructions and create Instruction Sets for them automatically from Tachyon Setup by using the **Tachyon Product Pack Deployment Tool**, as described in Uploading with the Tachyon Product Pack Deployment Tool. Or, you can load the Product Packs and create their associated instruction sets by hand.

The tool is included in the Tachyon Platform zip file under the **ProductPacks** folder.

- **Tachyon.ProductPackDeploymentTool.exe** (and its supporting files) is used to upload Product Packs
- The tool creates a log file called **Tachyon.ProductPackDeploymentTool.log** in the same folder.

The **ProductPacks** folder contains two directories, **Classic** and **Integrated**.

- The **Classic** directory holds a number of Classic Product Packs that contain Instructions.
- The **Integrated** directory holds a number of Integrated Product Packs that contain definitions for some Guaranteed State Policies, associated Fragments, and Instructions. In addition, a core utility pack has been provided with common Fragments that you can use to build your own Policies.

Tachyon Product Packs reference provides full details of all the product packs included in the Tachyon Platform zip.

The account used to run the **Tachyon.ProductPackDeploymentTool.exe** must:

- Have local administrator rights on the computer it is running on

- Exist as a Tachyon user assigned to either **Installer** or **Full Administrator** role.

1.4.4.1.6 Deploy Tachyon clients

You will need to deploy the 1E Client (with Tachyon enabled) to at least one device in order to use any instructions. You will need to do this in order to fully verify the installation of your Tachyon Platform.

Please refer to Deploying Tachyon clients for guidance on deploying clients to Windows and non-Windows devices.

1.4.4.1.7 Configure Tachyon to support the Export all responses feature

The **Export all** feature is displayed on the responses page for a question once it has finished retrieving all its responses. To enable this to work you need to configure the following:

1. **Configure BCP**:

   The **Export all** feature is described in Exporting data from Explorer. To enable Tachyon users with the appropriate permissions to use the **Export all** feature you must ensure that **Microsoft Bulk Copy Program (BCP)** is installed on each **Response Stack**, specifically the Response server where the Core component is hosted.

   - If Microsoft SQL Server is installed on the same server as the Response Stack, then BCP will normally be present.
   - If the TachyonResponses database is remote to the Response Stack and there is no local copy of Microsoft SQL Server, then you will need to install BCP.

   You can confirm BCP is installed by starting a command prompt and typing **bcp** and usage information is displayed. The command **bcp -v** displays the version.

   Note

   The information here applies regardless of which version of SQL Server is being used. This does not imply that Tachyon itself is supported under every possible version of SQL Server that falls within those ranges. See Windows Server requirements for the supported versions and required Service Packs.

   Install the following components to get BCP working:

Installer file name	Product Name	Where to get it from
vc_redist.x64.exe	Visual C++ 2017 Redistributable	https://support.microsoft.com/en-gb/help/2977003/the-latest-supported-visual-c-downloads
msodbcsql.msi	Microsoft® ODBC Driver 13.1 for SQL Server®	https://www.microsoft.com/en-us/download/details.aspx?id=53339 This needs to be installed because of a known issue in the

Installer file name	Product Name	Where to get it from
		Microsoft Command Line Utilities 15 for SQL Server.
msodbcsql.msi	Microsoft® ODBC Driver 17 for SQL Server®	https://docs.microsoft.com/en-us/sql/connect/odbc/download-odbc-driver-for-sql-server Use version 17 (x64).
MsSqlCmdLnUtils.msi	Microsoft Command Line Utilities 15 for SQL Server	https://docs.microsoft.com/en-us/sql/tools/bcp-utility The msi includes **BCP** and **SQLCMD**.

To verify the components have been installed, you can use **AppWiz.cpl** and check for the **Product Name**.

2. **Configure the share**:

The **Export all** feature enables the bulk copying of the entire completed responses for a Tachyon question to a specified **network share**.

Note

As this may potentially be a very large data set the **l**ocation must have sufficient disk-space to store the exported data.

To use this feature you must create one or more network shares on the Tachyon Server or other location, and configure NTFS and share permissions as follows. If desired, it can be hidden using a $ at the end of the share name.

Share permissions

Configure the share with **Everyone modify** access, or the same as the NTFS security.

NTFS Security

The share folder needs **modify** access configured for the service account(s) used by the Tachyon Core application pool on *each* Response Stack server and the service account used by the Tachyon Consumer application pool on the Master Stack server. By default, this account is NT AUTHORITY\NETWORK SERVICE (if the share folder is located on a Tachyon' all-in-one' server where both the Tachyon Consumer and Core components are installed e.g. Master Stack and Response stack). However, there is another scenario where the share folder is neither located on the same server as the Tachyon Consumer or Tachyon Core components, but on a remote fileserver (like a NAS device, DFS share, etc). In this case, the Tachyon Consumer AND Tachyon Core components will attempt to connect to the share folder as their respective computer accounts, for example <domain>\<computer$>.

Therefore, depending on where the share folder is located, you will need to configure NTFS permissions for the following:

- If the share is on the same server as the Tachyon Core application pool, the share must have NTFS **Modify** permissions added for the built-in **NT AUTHORITY\NETWORK SERVICE** account local to the server.
- If the share is remote from the server used by a Tachyon Core application pool, the share must have NTFS **Modify** permissions added for the **server$ account**. For example, if the Tachyon Core application pool is running on a server called **ACME-TCN01** the server account **ACME-TCN01$** would need to be added to the remote share with NTFS **Modify** permissions.
- If you have installed multiple Response Stacks, then repeat the preceding step, adding permissions on the share for each of the computers that are running a Tachyon Core. For instance, if you have deployed Response Stacks on two computers called **ACME-TCN01** and **ACME-TCN02**, then the server accounts **ACME-TCN01$** and **ACME-TCN02$** would need to be added to the share with NTFS **Modify** permissions.

Tip

Alternatively, you can use an AD security group that contains the computer$ account of all your Tachyon Servers.

Note

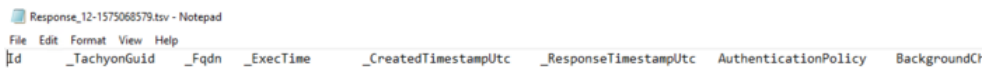
Include any user accounts or AD groups that would require access to the share.

The preceding are the *minimum* permissions required. Of course, if your share has *more* permissions, it will also work for **Export All**. For example, if your share inherits the **Modify** permission for **Authenticated Users** from its parent, then this will automatically include permission for local and remote computer$ accounts, so you will not need to explicitly grant the permissions mentioned above.

Common security issues

Error: Header-row missing in .tsv file export	Tachyon Consumer has no access to share folder

Error: Contents missing in .tsv file export	Tachyon Core(s) has no access to share folder



Successful: Both header-row and contents correctly included in .tsv file export	Tachyon Consumer and Tachyon Core(s) have access to share folder	

1.4.4.2 Optional tasks

The following tasks are not essential, but may enhance the performance and use of Tachyon in your environment. If you are carrying out a fresh installation, then you should consider implementing them. If you have upgraded from a supported version to version, then review each one and confirm that the previous configuration is still in place, and then consider whether your update requires you to implement any of these optional tasks.

1.4.4.2.1 Add an inventory connector

You can add an inventory connector to Tachyon that will sync data from a data source to an inventory repository. Typically, this connector would be to another system such as Configuration Manager or to Tachyon itself. For more details please refer to the Connectors page. At least one configured inventory connector is required to support management groups.

1.4.4.2.2 Create management groups

You can create Management groups to partition your estate into groups of devices that can be managed separately. This is done by creating a management group in the Settings application, please refer to Management Groups page and Management Groups - tutorial for more details. To synchronize the management groups with Explorer you'll need to add a Tachyon connector, please refer to Tachyon connector for more details.

1.4.4.2.3 Change Tachyon database owner to 'sa'

After the databases have been created, the best practice is to change the **owner** of each database to **sa**, to avoid issues if the owner's Windows account is deleted in the future.

The following script can be used to change the **owner** of each database to **sa**. This will work even if the **sa** login has been disabled, which is also best practice.

Change owner to 'sa' Expand source

```
ALTER AUTHORIZATION ON DATABASE::TachyonMaster To "sa"
GO
ALTER AUTHORIZATION ON DATABASE::TachyonResponses To "sa"
GO
```

Note

Ensure the Server Installation Account retains the **db_owner** role on the database to support re-configuration and upgrades. If the account is removed from being **owner**, then it will also be removed from the **db_owner** role and will need to be re-assigned, for example by using the **Grant db_owner** SQL script.

The **owner** user and **db_owner** role are both mapped to the database **dbo** user. It is preferable for the account to be a member of the **db_owner** role, instead of being the **owner** user.

Grant db_owner Expand source

```
USE [TachyonMaster]
GO
CREATE USER [ACME\TCNinstaller01] FOR LOGIN [ACME\TCNinstaller01];
ALTER ROLE [db_owner] ADD member [ACME\TCNinstaller01];
GO
USE [TachyonResponses]
GO
CREATE USER [ACME\TCNinstaller01] FOR LOGIN [ACME\TCNinstaller01];
ALTER ROLE [db_owner] ADD member [ACME\TCNinstaller01];
GO
```

1.4.4.2.4

1.4.4.2.5 Changing the SMTP Host configuration

The server installer does not support configuration of SMTP credentials, but these can be configured post-installation. By default, Tachyon assumes port 25 and anonymous authentication.

Tachyon stores its SMTP configuration in

- **<INSTALLDIR>\Tachyon\Coordinator\Tachyon.Server.Coordinator.exe.config** (workflow emails)

After any changes reboot the server or restart the **1E Tachyon Coordinator** service.

```
<configuration>
  ...
  <appSettings>
    ...
    <add key="smtpHost" value="ACME-EXC01.acme.local"/>
    <add key="TachyonEmail" value="Tachyon@acme.local"/>
    ...
    <add key="2FAEnabled" value="true" />
    ...
  </appSettings>
  ...
  </entityFramework>
  <!-- The settings in the following section can be modified to provide custom
port and authentication options for SMTP -->
  <system.net>
    <mailSettings>
```

```
      <smtp deliveryMethod="Network">
        <network
          port="25"
          defaultCredentials="true"
          userName=""
          password=""
        />
      </smtp>
    </mailSettings>
  </system.net>
</configuration>
```

Note

Microsoft's documentation for the SMTP network section can be found here: https://msdn.microsoft.com/en-us/library/ms164242(v=vs.110).aspx.

When **defaultCredentials** is set to true, the mail subsystem uses the Windows credentials from the process under which the coordinator service is running to connect to the mail server. In general, this will only work with Microsoft servers, or servers that allow anonymous connections. To use different credentials, set defaultCredentials="false" and add values for **username** and **password** (and, optionally, **clientDomain**).

To use an encrypted connection, if the server supports it, add **enableSsl**="true". Change the **port** as needed, for example, port="465" or port="587".

Microsoft supports parameters named **host** and **From**, but these are ignored by Tachyon because the **smtpHost** and **TachyonEmail** keys in the <appSettings> section take precedence.

Note

If **smtpHost** is set to empty (blank) in a config file then email is disabled for the corresponding feature.

The Email and 2FA requirements feature requires email. Therefore, if **smtpHost** is set to empty, then the 2FA feature must be disabled by setting **<add key="2FAEnabled" value="false" />** in the **<INSTALLDIR>\Tachyon\Coordinator\Tachyon.Server.Coordinator.exe.config** file.

Finally, reboot the server or restart the **1E Tachyon Coordinator** service.

1.4.4.2.6 Enabling or disabling Denial-of-Service Blocking

By default, a Switch will temporarily blacklist the IP addresses of devices that "misbehave" - that is, if an external device, browser or other endpoint, sends a message other than Online when it first connects. This is to handle denial-of-service attacks or other malicious attempts to connect to the Switch.

However, you may wish to disable this feature in some circumstances. For example, if you are using a load balancer that sends a probe which triggers the block on its IP address, potentially blocking all clients using the load balancer.

You can configure this feature by editing the **TACHYON_SWITCH_DOSBLOCK_OFF** setting in the **<INSTALLDIR>\Tachyon\Switch\Tachyon.Switch.Host.exe.config** file.

- By default, the setting is not present in the config file. If not present, empty, 1, or any value other than 0, then DoS blocking is disabled (off).
- Set to 0 to enable (turn on) DoS blocking.

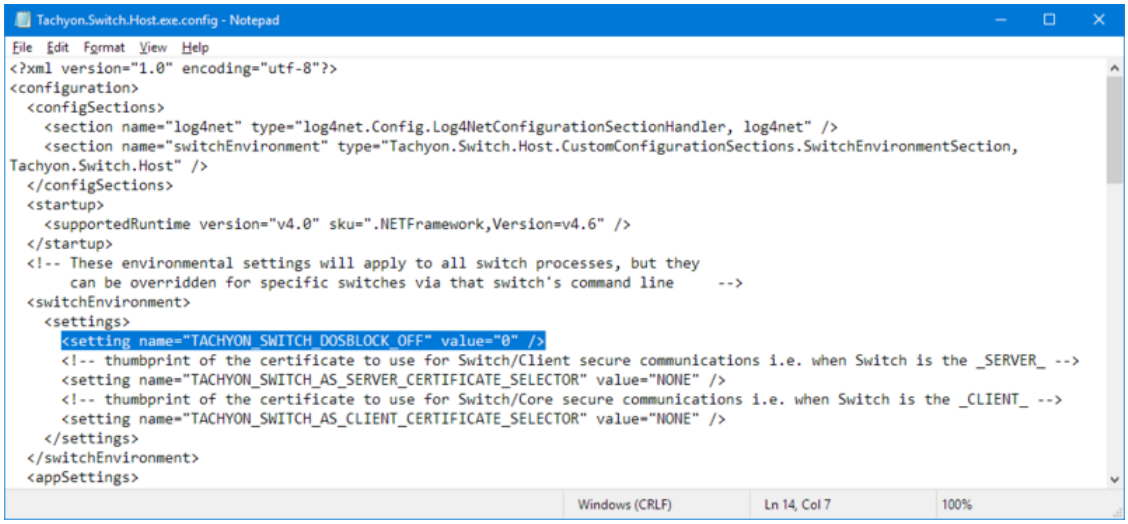
For a change of setting to take effect, restart the Switch Host service.

```
<switchEnvironment>
  <settings>
    <setting name="TACHYON_SWITCH_DOSBLOCK_OFF" value="0" />
    ...
  </settings>
</switchEnvironment>
```

You can test this by using a browser to go to:

http://tachyon.acme.local:4000

if the blocking is enabled this will be blocked for a few seconds, and if you refresh the browser you will see the connection is immediately rejected, but if the blocking is disabled you will see these are not rejected.



1.4.4.2.6.1 Blocking: On

When the blocking is on you will see **Agent blocked** warning messages in the Switch log when a device misbehaves:

1.4.4.2.6.2 Blocking: Off (default)

When the blocking is off, the first time it would have triggered you will see an INFO message saying it is disabled.

1.4.4.2.7 Enabling or disabling Device Deduplication

Please refer to the Device Deduplication page for further information about how the process works, and how to configure the settings.

> **Warning**
>
> The Device Deduplication feature is not enabled until you have modified the Coordinator configuration settings.
>
> The configuration steps describe updating the Coordinator configuration file, specify False (default) for each of the configuration arguments. You are strongly advised that all configuration arguments - except for DeviceIdentifier - are set to False (default) for the first run or for whenever a new DeviceIdentifier value is being set. Results should then be analysed to ensure that the DeviceIdentifier specified is correct for your environment.

Tachyon stores its Device Deduplication configuration in the **<INSTALLDIR>\Tachyon\Coordinator\Tachyon.Server.Coordinator.exe.config** file.

After any changes reboot the server or restart the **1E Tachyon Coordinator** service.

The time and frequency of when the Device Deduplication process runs is changed by adding and editing the **DeviceDeduplication** setting.

```
<module assemblyName="Tachyon.Server.Coordinator" providerName="Tachyon.Server.
Coordinator.Scheduling.SchedulingModule">
  <settings>
    <add key="Crontab1" value="50 23 * * * LogDevicesSeenInTheLast7Days" />
    <add key="Crontab2" value="15 * * * * MaintainPolicyRulePartitioning" />
    <add key="Telemetry" value="40 23 * * 5 SendTelemetryStats" />
    <add key="DeviceDeduplication" value="0 1 * * 0 DeviceDeduplication {Delete
Devices:'false',UpdateDeviceData:'false',DeleteOrphanedDeviceData:'false',Devic
eIdentifier:['FQDN']}" />
  </settings>
</module>
```

The numbers that you see after **value** is a crontab schedule expression. The schedule **0 1 * * 0** means "at 01:00 hours, any day of the month, any month of the year, on weekday 0 (Sunday)". In other words, this configuration runs the Device Deduplication process at 1AM UTC every Sunday night.

You can use an online tool such as https://crontab.guru/ to verify your crontab schedule expression.

Warning

Please ensure there are no spaces in the **arguments** text {within the brackets}.

Do not change the other crontab keys unless advised by 1E.

1.4.4.2.8 Enabling or disabling Telemetry features

Telemetry helps 1E to continually improve your experience. Only summarized statistical information is collected, which enables 1E to see how customers use features of the application. No personally identifiable data is collected. 1E use this information to:

- Understand how the product is being used to influence future development decisions
- Plan supported platforms (OS, SQL etc. versions) over time
- Deliver a smooth upgrade experience as we can focus testing on implemented scenarios
- Improve system performance
- Identify early warning signs of potential issues such as excessive growth of database tables, instruction failures etc. so we can pro-actively address them.

Server telemetry reports how the platform is used and data is compressed, encrypted and sent to 1E through email on a configurable schedule. Full details of the Server telemetry data sent to 1E is provided in Server telemetry data.

User Interface telemetry reports how the user interface is used, and data is sent directly from administrator browsers to the 1E Cloud.

1.4.4.2.8.1 Server telemetry

Note

By default, Tachyon collects data continuously and sends a **compressed** and **encrypted** summary by email to 1E **every Friday at 23:40 UTC**.

If you have disabled the **email feature** then Server telemetry will not be sent to 1E.

In this version of Tachyon Platform, you must edit the **Server telemetry** configuration in the **<INSTALLDIR>\Tachyon\Coordinator\Tachyon.Server.Coordinator.exe.config** file.

After any changes reboot the server or restart the **1E Tachyon Coordinator** service.

Note

Changes to the Telemetry configuration do not affect the data exported into an unencrypted CSV file by the **Export Telemetry** button on the Settings→System information page.

The time and frequency of when Telemetry is sent to 1E is changed by editing the **Telemetry** line.

```
<module assemblyName="Tachyon.Server.Coordinator" providerName="Tachyon.Server.
Coordinator.Scheduling.SchedulingModule">
  <settings>
    <add key="Crontab1" value="50 23 * * * LogDevicesSeenInTheLast7Days" />
```

```
    <add key="Crontab2" value="15 * * * * MaintainPolicyRulePartitioning" />
    <add key="Telemetry" value="40 23 * * 5 SendTelemetryStats" />
  </settings>
</module>
```

Telemetry emails can be disabled by changing the key name from *"Telemetry"* to *"DISABLED"*. To enable them, change it back to *"Telemetry"*.

The numbers that you see after **value** is a crontab schedule expression. The schedule **40 23 * * 5** means "at 23:40 hours, any day of the month, any month of the year, on the 5th day of the week (Friday)". In other words, this configuration sends the telemetry data every Friday night.

You can use an online tool such as https://crontab.guru/ to verify your crontab schedule expression.

> **Warning**
>
> Do not change the other crontab keys unless advised by 1E.

1.4.4.2.8.2 User interface telemetry

In this version of the platform, you must edit the **User interface telemetry** configuration in the Master database.

Connect to the **TachyonMaster** database and edit the **GlobalSetting** table. Locate the entry whose **Name** is **UITelemetryLevel** and change the **Value** to 0, 1, 2 or 3, to reflect the type of data that is reported to 1E.

0 - Off

1 - Anonymous

2 - License Name

3 - License Name and Unique user ID

The change takes effect for each user when they close and reopen their browser to connect to the portal.

> **Note**
>
> **License Name** is **Customer** name as it appears in the license file and License information page.
>
> **Unique user ID** is a random ID number representing an individual user.

	Name	Value	Hidden
21	PolicyDirty	false	1
22	PolicyRuleDeviceThreshold	1000	1
23	PolicyRuleStatusPartition	true	1
24	RequireReauthenticationForInstr...	true	0
25	SychronousInstructionCacheDur...	180	0
26	SychronousInstructionWaitTime...	30	0
27	UITelemetryKey	a33401cd-7dc1-4e66-4689-daa2a88d37eb	1
28	UITelemetryLevel	0	1
29	UseStartsWithMatchingForADPri...	false	0

1.4.4.2.9 Enabling or disabling Two-factor Authentication

2FA is optionally disabled (enabled by default) in the Active Directory and email screen. If you need to change this after installation, then you need to edit the setting **<add key="2FAEnabled" value="true" />** in the **<INSTALLDIR>\Tachyon\Coordinator\Tachyon.Server.Coordinator.exe.config** file.

If enabling 2FA, please refer to Email and 2FA requirements.

1.4.4.2.10 Removing the HTTP binding from the Tachyon website

You can optionally remove the HTTP binding from the Tachyon website on any Tachyon server (Master, Response, DMZ or other server). You can do this by simply deleting the HTTP binding in IIS Manager.

The table below lists 1E products and apps that may depend on the website HTTP binding, which you should consider before removing it from the Master Stack.

> **Note**
>
> In this version of platform, upgrading will re-instate the HTTP binding. Therefore, you will need to repeat the removal process described below.

App	Tachyon Master Stack	Tachyon Response server
AppClarity (Software Reclaimer)	No dependency on HTTP, although the Reclaimer uses HTTP by default. To use HTTPS, Software Reclaimer requires its Reclaimer XML to be reconfigured to use HTTPS. Please refer to Configuring Software Reclaimer to use HTTP or HTTPS.	No dependency on HTTP. Software Reclaimer does not use Response Servers.
Application Migration (Task Sequences)	No dependency on HTTP.	No dependency on HTTP. Application Migration does not use Response Servers.
Content Distribution	You will need to keep the HTTP binding only if you are still in the process of upgrading from Nomad 7.0.200 or earlier, which uses HTTP to connect to the Master Stack server. Nomad clients (in 1E Client 5.2, 8.0, 8.1, 8.1 and later) do not connect to the Master Stack.	No dependency on HTTP. Nomad clients (in 1E Client) use HTTPS by default, and connect to the Background Channel.

App	Tachyon Master Stack	Tachyon Response server
PXE Everywhere Central	Although PXE Everywhere Central is not an app, it can be installed on a Tachyon server. It requires HTTP, but this will be normally under the Default Web Site, which means you can safely remove the HTTP binding from the Tachyon website. However, there are circumstances where PXE Everywhere Central may have installed under the Tachyon website, in which case you will need to keep the HTTP binding, or remove the HTTP binding and re-install PXE Everywhere Central. PXE Everywhere Central will automatically install under the Tachyon website, or create its own website, if the Default Web Site does not exist or does not have an HTTP 80 binding. PXE Everywhere does not support HTTPS and uses/creates a HTTP 80 binding by default. You can optionally change the HTTP port after installation, but you must ensure PXE Everywhere Agents are also configured to use the same port.	See Master Stack.
ServiceNow apps	No dependency on HTTP.	No dependency on HTTP.

The following apps have no dependency on HTTP.

- Experience
- Explorer
- Guaranteed State

1.4.5 Implementing a Tachyon DMZ Server

The process for installing a Tachyon DMZ Server to support Internet-facing 1E Client devices.

Enabling Tachyon to support devices that are external to your company network is done by slightly extending the default single-server architecture.

To enable external 1E Client devices to interact with Tachyon , the DMZ requires at least one Background Channel and at least one Switch.

The Responses Stack handles communications between Master Stack and 1E Client devices. The Background Channel and Switch components handle the direct communication with clients, the Core processes the information in both directions between the Master Stack and the Switches.

Tip

Tachyon Setup provides a two-stage process to install a new DMZ Server:

1. Run Setup Maintenance on the Response Stack server (specifically the server that hosts the Core which the DMZ Server will connect to) to prepare the Response server and its database, and store details in an **ini** file
2. Run Setup to install the DMZ Server using the prepared **ini** file.

The two-stage process and its **ini** file are required because Tachyon Setup is unable to communicate through the DMZ firewall. In previous versions of Tachyon, the first stage required complex manual configuration.

To upgrade a DMZ Server, you only need to run setup on the DMZ Server, you do not require the **ini** file.

Note

You should not start Stage 1 until you are also prepared to complete Stage 2. This is because Stage 1 Tachyon reconfigures to think the DMZ Server already exists and is working before Stage 2 completes the process. This may cause the following problems:

- Tachyon will attempt to send instructions to the Switch in the DMZ, and will log an error because such Switch is not yet installed. The error is harmless and will not prevent the instruction from being sent to other existing Switches, but you should be prepared to see the error message in the Log without being alarmed.
- You will not be able to upload any new instructions which contain resources. If you try to upload an instruction definition that contains resources, the Consumer API will try to upload the resources to all Background Channels, including the one in the DMZ. This will, of course, fail, and it will cause the Consumer API to revert the changes made to all other Background Channels and return an error result.
- You will not be able to deploy a Policy, because Policies also require one or more files to be uploaded to all Background Channels, which will be reverted when the DMZ Server fails to update.

If for any reason you are unable to complete Stage 2, you can revert the Stage 1 changes by using the **Undo** button in DMZ Server form in the Tachyon Setup Maintenance screen.

1.4.5.1 Assumptions

The steps given on this page assume:

- If the Tachyon DMZ Server is domain-joined, it is either in the same domain in which the internal Tachyon Server resides or there is a two-way trust between domains
- The Tachyon DMZ Server will host only Tachyon Switch and Background Channel components and is installed in a DMZ
- Tachyon is already installed on the internal (corporate) network, with clients successfully using the internal Response Stack Switch and Background Channel, which the DMZ Server will connect to.

In our example, the DMZ Server has only one Switch, and the internal Tachyon Server is a single-server configuration with Master and Response Stacks. If your system has different requirements, please contact 1E for advice.

Client devices will be configured to swap between being on the internal network and being external to the network and therefore will communicate with the internal Tachyon Server when connected internally and the external Tachyon DMZ Server when accessing externally (for example Internet). Client devices must have the appropriate certificates installed. Please refer to Certificate requirements for more details.

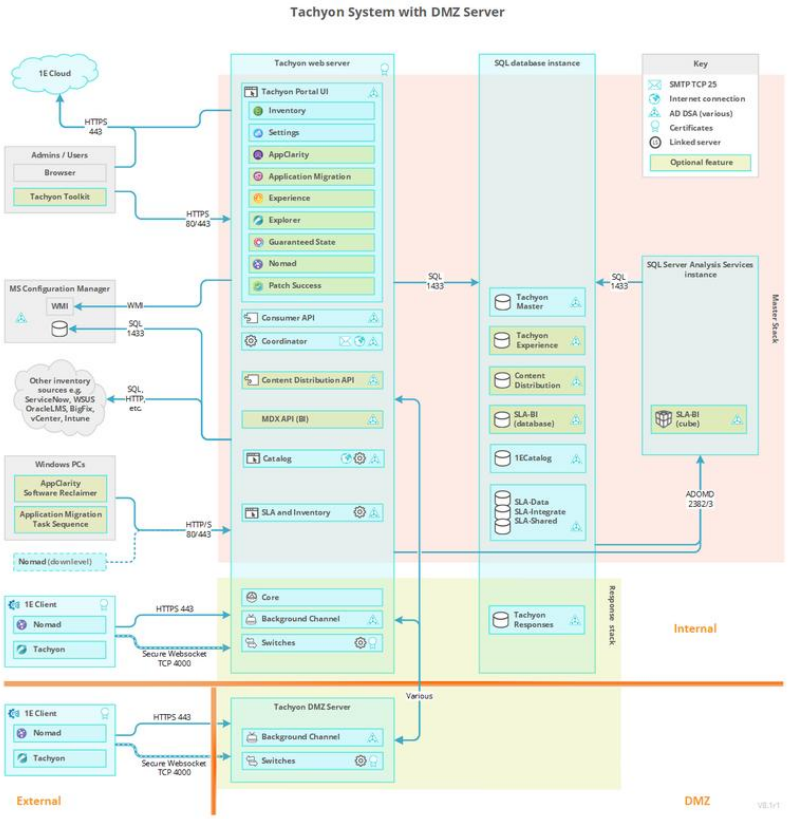
1.4.5.2 Communications ports

The Tachyon communications ports between the Tachyon Master Server and the Tachyon DMZ Server must be opened, as illustrated in the picture. Please refer to the Communication Ports page for more details.

Warning

The web server certificate on the DMZ Server needs to reference at least one CRL Distribution point that uses HTTP. These CRL DPs are likely to be in the internal network, and the firewall will need to allow the DMZ server to access these internal servers.

Tachyon Setup will warn you if the certificate does not reference a CRL Distribution point that uses HTTP, but does not tell you if it cannot connect to the CRL DP, and will allow installation to proceed.



1.4.5.3 Preparation

In the following summary and configuration steps, the following terminology is used:

- **Relevant internal servers**
  - Any internal server which hosts a Tachyon Server component that communicates with any DMZ Server
  - Typically this will include the servers which host the Coordinator, the Consumer API, and any Core bound to a DMZ switch that is registered in the dbo.SwitchToCoreApi table in the TachyonMaster database
  - The example diagrams and steps refer to only one internal server, but there may be separate servers for Master Stack (with Coordinator and Consumer API) and Response Stack (with Core).
- **DMZ Server**
  - Any server that has Tachyon Server components installed that is not on the internal network (that is, outside of the corporate network)
  - This includes a Tachyon DMZ Server (which has one or more Switches and a Background Channel).

You must ensure the following before installation of Tachyon on a DMZ Server.

- The **Master Server** is installed and verified with internal Tachyon clients.
  - Ensure the certificate(s) used on the internal server(s) already meet the additional requirements for implementing a DMZ Server. Tachyon Setup does not check these requirements.
  - The documentation below assumes this has a Master Stack and Response Stack on the same server.
  - A Response Stack is required in order to provide the Core component that will be used by the remote DMZ Server. Internal clients are not required to use the Switch and Background Channel of this Response Stack.
- The **DMZ internal and external firewall** are configured correctly. Please refer to the Communication Ports page for more details.
- The **DMZ Server** is provisioned. Although a DMZ Server does not have all Tachyon components, all prerequisites must be met in order for Tachyon Setup to run. In particular, the following must be prepared before installation. For more detail about each requirement, click on the relevant link.
  - **Network requirements** (**DNS Names**)
    - The DMZ Server requires two DNS Names, even if the DMZ Server is configured with one network interface. **Two network interfaces** are required to prevent response traffic from clients to server, and from server to Core, using the same network interface.

- A **DMZ Server internal DNS Name** so that the internal Tachyon Server can connect to the DMZ Server. The documentation below assumes this DNS Name exists, but it can alternatively be the server's computer name FQDN.
- A **DMZ Server external DNS Name** so that Internet devices can connect to the DMZ Server, which is the name included in the client configuration for Switch and Background Channel settings (1E Client configuration file). This DNS Name is not necessarily for the actual IP Address(es) of the external network interfaces if DMZ firewall, Network Address Translation (NAT), or other routing is employed.
- Both DNS Names must be included in the Web server certificate. Please see Certificate requirements below for more information on certificate DNS Name requirements.
- If the DMZ Server is domain-joined, both DNS Names require an HTTP class Service Principal Name (SPN) registered on the DMZ Server's computer$ account. Please refer to Service Principal Names for more details.

– **Network requirements (Network interfaces)**

- The DMZ Server should have an internal network interface, and an external network interface for each Switch, in order to keep Core and Switch traffic apart. This recommendation is for performance reasons when supporting over 500 devices.
- If an internal interface is *not* used, then the external interface will use both DNS Names.
- If using two interfaces...
  - The internal interface will use the internal DNS Name, and the external interface(s) will use the external DNS Name. This is the assumption made in the configuration steps below.
  - Internal and external interfaces will typically be on different subnets.
  - Ensure your network routing is configured to route outgoing traffic using the internal interface. You may need to configure a persistent route, for example using the same steps described in Configuring a persistent route for SQL traffic.

– **Certificate requirements (Web Server Certificate)**

- Each DMZ Server requires its own web server certificate. Please see Certificate requirements below for more information.

– **Windows Server roles and features**

- IIS to host the Background Channel application.
- Windows Authentication role if the server is domain joined and has a trust relationship with the domain that Master Stack is configured to use.

- **Test devices** with the client installed.
  - At least one is connected to the internal network; another is connected to the external network.

1.4.5.4 Certificate requirements

Tachyon Server certificate requirements are defined in Certificate requirements.

Implementing a Tachyon DMZ Server installation has the following additional certificate requirements for the internal server(s) as well as the Tachyon DMZ Server itself.

Relevant internal servers

Type	Additional certificate requirements	Where used
Tachyon Server certificate	The Certificate requirements require the **Tachyon Server DNS Name FQDN** and **computername FQDN** to be present in the certificate. However, it has an additional requirement to separate communications between internal and external Switches: • A **Subject Alternative Name** Extension (extensions:subjectAltName), of type **dnsName**, which must contain: – **Alternate DNS Name FQDN** - for example **Tachyonalt.acme.local**	This is the usual Tachyon website certificate. A DMZ Server installation has additional needs to allow Switches on the DMZ Server to communicate with: • Tachyon Master Stack (Coordinator) • Tachyon Response Stack (Core).
Tachyon Consumer API client certificate	The client certificate on the Tachyon Master Stack has the following requirements: 1. Issued by a trusted Certificate Authority (CA) – The certificate for the Root CA in the Certification Path must exist in the Trusted Root CA store of the server – If the issuing CA is not the Root CA then the certificate for the issuing CA and any intermediate CA in the Certification Path must exist in the Intermediate CA store of the server – If the above CA certificates are different from those used by the DMZ Server, they	Used by the Tachyon Master Stack (Consumer API) to perform client authentication with the Background Channel on the DMZ Server. Required only if certificate authentication is used instead of domain authentication. **Note**

Type	Additional certificate requirements	Where used
	will need to be exported and then imported into the DMZ Server. 2. Has at least the following Enhanced Key Usage – Client Authentication (OID 1.3.6.1.5.5.7.3.2) 3. Has a private key 4. Revocation information is included. – References at least one CRL Distribution point that uses HTTP. 5. A **Subject Alternative Name** Extension (extensions:subjectAltName), of type **dnsName**, which must contain one of the following: – **Tachyon Server DNS Name FQDN** - in our example **Tachyon.acme.local** – **Alternate DNS Name FQDN** - as specified above - for example **Tachyonalt.acme.local** – **Tachyon Server computername FQDN** - in our example **ACME-MST.acme.local** 6. The client authentication certificate, used by the Consumer API to communicate with the DMZ Background Channel, must have a subject. **Note** You will need the thumbprint for this certificate. In our example, this is **95dfcc47c31c8bf201104da27ba8a6d792e83665**.	This certificate is only used if your DMZ Server is not domain-joined, or does not have a two-way trust between your internal domain and your DMZ domain.

1.4.5.4.1 DMZ Server

Type	Additional certificate requirements	Where used
DMZ Server certificate	The Certificate requirements are valid with regard to trust, usage, enhanced key usage, the private key, and revocation. However, as this is an externally reachable certificate, it is not recommended that the computername FQDN is present in the	Used by the Switch(es) and Background Channel to secure

Type	Additional certificate requirements	Where used
	certificate. As such, the certificate must meet the following requirements: • A **Subject Alternative Name** Extension (extensions:subjectAltName), of type **dnsName**, which must contain: – **DMZ Server external DNS Name FQDN** - in our example: **Tachyon.acme.com** – **DMZ Server internal DNS Name FQDN** - in our example **Tachyondmz.acme.local** Optionally, it may also contain a Subject Common Name Field (subject:commonName) that is unique within the organization that identifies the certificate (https://cabforum.org/wp-content/uploads/CA-Browser-Forum-BR-1.6.5.pdf#page=54).	communication to clients.
DMZ Server client certificate	The client certificate on the Tachyon DMZ Server has the following requirements: 1. Issued by a trusted Certificate Authority (CA) – The certificate for the Root CA in the Certification Path must exist in the Trusted Root CA store. – If the issuing CA is not the Root CA then the certificate for the issuing CA and any intermediate CA in the Certification Path must exist in the Intermediate CA store. – If the above CA certificates are different to those used by the Tachyon Master Stack server, they will need to be exported and then imported on the Tachyon Web Server. 2. Has at least the following Enhanced Key Usage. – Client Authentication (OID 1.3.6.1.5.5.7.3.2). 3. Has a private key. 4. Revocation information is included.	Used by Switch(es) to perform client certificate authentication with its assigned Response Stack (Core).

Type	Additional certificate requirements	Where used

– References at least one CRL Distribution point that uses HTTP.

5. A **Subject Alternative Name** Extension (extensions:subjectAltName), of type **dnsName**, which must contain:

   – **DMZ Server internal DNS Name FQDN** - in our example **Tachyondmz.acme.local**.

1.4.5.4.2 Certificate trust

For each of the following scenarios, ensure you import the CA certificate(s) of the trust chain into the server's Local Machine's Trusted Root Certification Authority or Intermediate Certification Authorities stores (as appropriate).

- Relevant internal servers must trust the DMZ Server certificate therefore you must import the CA certificates used by the DMZ Server into the CA stores on the relevant internal servers.
- DMZ Server must trust the relevant internal server certificate(s), therefore you must import the CA certificates used by the relevant internal server(s) into the CA stores on the DMZ Server.
- The DMZ Server must also trust client certificates, therefore you import the CA certificates used by clients into the CA stores on the DMZ Server.

Note

The HTTP CDP referenced in any certificate, including imported CA certificates, must be reachable by the DMZ Server.

Note

If the certificates on the DMZ Server and the internal Tachyon servers are from different issuing CAs, then:

- Obtain the certificates (public keys only) for all the intermediate CAs, up to and including the Root CA of the internal Tachyon Server's Web Server Certificate, and add them to the corresponding CA stores on the DMZ Server. If you do not do this, the Switch on the DMZ Server will not be able to start because it won't be able to trust the Core API on the relevant internal server.

Similarly, if the certificates on the DMZ Server and client authentication certificates on external clients are from different issuing CAs, then:

- Obtain the device's intermediate and root CA certificates, and add them to the corresponding CA stores on the DMZ Server.
- Windows devices will need the Tachyon DMZ Server's intermediate and root CA certificates to be added to their CA stores

- Non-windows devices will need the Tachyon DMZ Server's intermediate and root CA certificates to be added to their certificate store (that is either KeyStore or cacert.pem file, depending on the method used to store certificates).

1.4.5.5 The installation process for a Tachyon DMZ Server

1.4.5.5.1 Overview

Tachyon Setup provides a two-stage process to install a new DMZ Server:

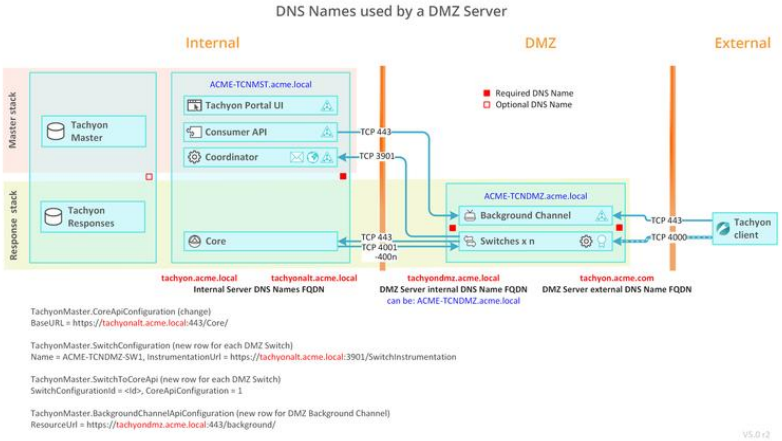
1. Run Setup Maintenance on the Response Stack server (specifically the server that hosts the Core which the DMZ Server will connect to) to prepare the Response server and its database, and store details in an **ini** file.

2. Run Setup to install the DMZ Server using the prepared **ini** file.

The two-stage process and its **ini** file are required because setup is unable to communicate through the DMZ firewall. In previous versions of Tachyon , the first stage required complex manual configuration.

To upgrade a DMZ Server, you only need to run setup on the DMZ Server, you do not require the **ini** file.

To illustrate the following detailed steps we use the ACME network with two servers.



1.4.5.5.2 DNS Names

Use the following table to help map the DNS Names used in your environment with the name used in the steps below.

Server	DNS Name references	DNS Name examples	DNS Names used in your environment
The internal Tachyon Server	Tachyon Server computername FQDN	**ACME-TCNMST.acme.local**	

Server	DNS Name references	DNS Name examples	DNS Names used in your environment
The diagram shows only relevant components of Master Stack and Response Stack			
Tachyon Server DNS Name FQDN	**Tachyon.acme.local**		
Tachyon Server Alternate DNS Name FQDN	**Tachyonalt.acme.local**		
The external Tachyon DMZ Server	DMZ Server computername FQDN	**ACME-TCNDMZ**	
DMZ Server internal DNS Name FQDN	**Tachyondmz.acme.local**		
DMZ Server external DNS Name FQDN (Internet)	**Tachyon.acme.com**		

1.4.5.5.3 Detailed steps

	Location	Detailed steps
1	Internal Tachyon Server (Master and Response Stacks) and internal	Install the internal Tachyon Server, with Master and Response Stacks, and ensure it works by running the tests described in Verifying.

	Location	Detailed steps
	Tachyon client(s).	
2	DMZ Server.	Ensure Preparation steps are complete for the Tachyon DMZ Server. **Note** You must ensure the following before installation of Tachyon on a DMZ Server. • The **Tachyon Master Server** is installed and verified with internal clients. – Ensure the certificate(s) used on the internal server(s) already meet the additional requirements for implementing a DMZ Server. Tachyon Setup does not check these requirements. – The documentation below assumes this has a Master Stack and Response Stack on the same server. – A Response Stack is required in order to provide the Core component that will be used by the remote DMZ Server. Internal clients are not required to use the Switch and Background Channel of this Response Stack. • The **DMZ internal and external firewall** are configured correctly. Please refer to the Communication Ports page for more details. • The **DMZ Server** is provisioned. Although a DMZ Server does not have all Tachyon components, all prerequisites must be met in order for Tachyon Setup to run. In particular, the following must be prepared before installation. For more detail about each requirement, click on the relevant link. – **DNS Names** • The DMZ Server requires two DNS Names, even if the DMZ Server is configured with one network interface. **Two network interfaces** are required to prevent response traffic from clients to server, and from server to Core, using the same network interface. • A **DMZ Server internal DNS Name** so that the internal Tachyon Server can connect to the DMZ Server. The documentation below assumes this DNS Name exists,

but it can alternatively be the server's computer name FQDN.

- A **DMZ Server external DNS Name** so that Internet devices can connect to the DMZ Server, which is the name included in the client configuration for Switch and Background Channel settings (1E Client configuration file). This DNS Name is not necessarily for the actual IP Address(es) of the external network interfaces if DMZ firewall, Network Address Translation (NAT), or other routing is employed.
- Both DNS Names must be included in the Web server certificate. Please see Certificate requirements for more information on certificate DNS Name requirements.
- If DMZ Server is domain-joined, both DNS Names require an HTTP class Service Principal Name (SPN) registered on the DMZ Server's computer$ account. Please refer to Service Principal Names for more details.

– **Network interfaces**

- The DMZ Server should have an internal network interface, and an external network interface for each Switch, in order to keep Core and Switch traffic apart. This recommendation is for performance reasons when supporting over 500 devices.
- If an internal interface is *not* used, then the external interface will use both DNS Names.
- If using two interfaces...
  - The internal interface will use the internal DNS Name, and the external interface(s) will use the external DNS Name. This is the assumption made in the configuration steps below.
  - Internal and external interfaces will typically be on different subnets.
  - Ensure your network routing is configured to route outgoing traffic using the internal interface. You may need to configure a persistent route, for example using the same steps described in Configuring a persistent route for SQL traffic.

Location	Detailed steps

- **Web Server certificate**
  - Each DMZ Server requires its own web server certificate. Please see Certificate requirements below for more information.
- **Windows Server roles and features**
  - IIS to host the Background Channel application.
  - Windows Authentication role if the server is domain joined and has a trust relationship with the domain that Master Stack is configured to use.

- **Test devices** with the client installed.
  - At least one is connected to the internal network; another is connected to the external network.

Expand to see guidance when DMZ Server is using different CA certificates to the internal Tachyon server or clients...

Note

If the certificates on the DMZ Server and the internal Tachyon servers are from different issuing CAs, then:

- Obtain the certificates (public keys only) for all the intermediate CAs, up to and including the Root CA of the internal Tachyon Server's Web Server Certificate, and add them to the corresponding CA stores on the DMZ Server. If you do not do this, the Switch on the DMZ Server will not be able to start because it won't be able to trust the Core API on the relevant internal server.

Similarly, if the certificates on the DMZ Server and client authentication certificates on external clients are from different issuing CAs, then:

- Obtain the device's intermediate and root CA certificates, and add them to the corresponding CA stores on the DMZ Server.
- Windows devices will need the Tachyon DMZ Server's intermediate and root CA certificates to be added to their CA stores
- Non-windows devices will need the Tachyon DMZ Server's intermediate and root CA certificates to be added to their certificate store (that is either KeyStore or cacert.pem file, depending on the method used to store certificates).

3	Internal Tachy	***On the internal Tachyon Server (Response Stack)***

	Location	Detailed steps
	on Server (Response Stack).	Add an alternate HTTPS binding to the Tachyon website. In our example this is **https://Tachyonalt.acme.local:443** You may have already created an alternate HTTPS binding when installing the Response Stack server. The Response Stack server is the server you have already installed that hosts the Core component. This will have been installed when installing a Single-Server with all components, or a dedicated Response Stack server. If you need to add the binding, then use the manual steps below. **Tip** Remember this binding for steps 5, 8 and 21. 1. On the internal Tachyon Server, open **IIS Management Console**. 2. Expand **Sites** and right-click on the **Tachyon** website. 3. Under the Edit Site actions, click on **Bindings...**. 4. Click **Add...**. 5. Select type **https**. 6. Set the **Host name** to the **Tachyon Server Alternate DNS Name** - see table above. 7. Enable **Require Server Name Indication**. 8. Select the **SSL certificate** to be the *same* certificate as the existing HTTPS binding, ensuring it is the certificate with SAN entries for **Tachyon Server DNS Name FQDN** and **Tachyon Server Alternate DNS Name FQDN**. 9. Click **OK** to save, and **Close**.
4	Internal Tachyon Server (Response Stack).	***On the internal Tachyon Server (Response Stack)*** On the server that hosts the Core component - which the DMZ Server will connect to - run Tachyon Setup and go to the **Maintenance** screen, and click on **Add DMZ Server...** This is the first stage of using Tachyon Setup to install a DMZ Server. It prepares the Response server and its database, and stores configuration details in a **<DMZ Server computername>.ini** file in the Setup folder. You will need to copy this file to the DMZ Server.

Location	Detailed steps

When you click on **Ok**, Setup validates the configuration details. Any serious errors will prevent Setup from going ahead, and any warnings will cause a dialog to be presented to ask for confirmation about whether you want to continue. The **ini** file is only saved or updated after a successful validation, or warnings have been accepted.

Note

After this moment, Tachyon will "think" that you have a DMZ Server, even though you have not yet installed it, this means:

- Tachyon will attempt to send instructions to the Switch in the DMZ and will log an error because such Switch is not yet installed. The error is harmless and will not prevent the instruction from being sent to other existing Switches, but you should be prepared to see the error message in the Log without being alarmed.
- You will not be able to upload any new instructions which contain resources. If you try to upload an instruction definition that contains resources, the Consumer API will try to upload the resources to all Background Channels, including the one in the DMZ. This will, of course, fail, and it will cause the Consumer API to revert the changes made to all other Background Channels and return an error result.
- You will not be able to deploy a Policy, because Policies also require one or more files to be uploaded to all Background Channels, which will be reverted when the DMZ Server fails to update.

The **Undo** button will allow you to undo the changes written to the database so that your server will not think anymore that you have a DMZ Switch and Background Channel. This can be useful if you find an error in your configuration or if you need to revert the changes to avoid the errors mentioned above or if you wish to uninstall your DMZ Server. If you need to do this after you have already closed the form, you can re-open it and reload the information by using the **Import** button.

Parameter	Description
DMZ Server computername.	The computername of the DMZ Server. It is used to ensure you are preparing the correct DMZ Server, and prepare the Switch configuration in the TachyonMaster database.

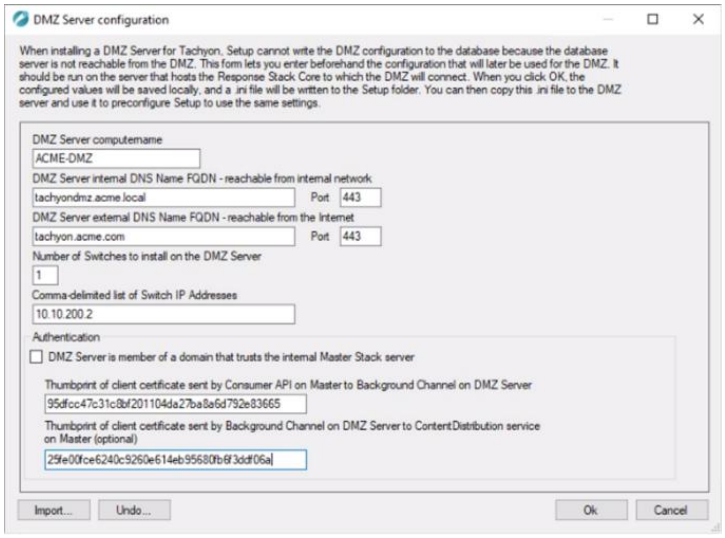
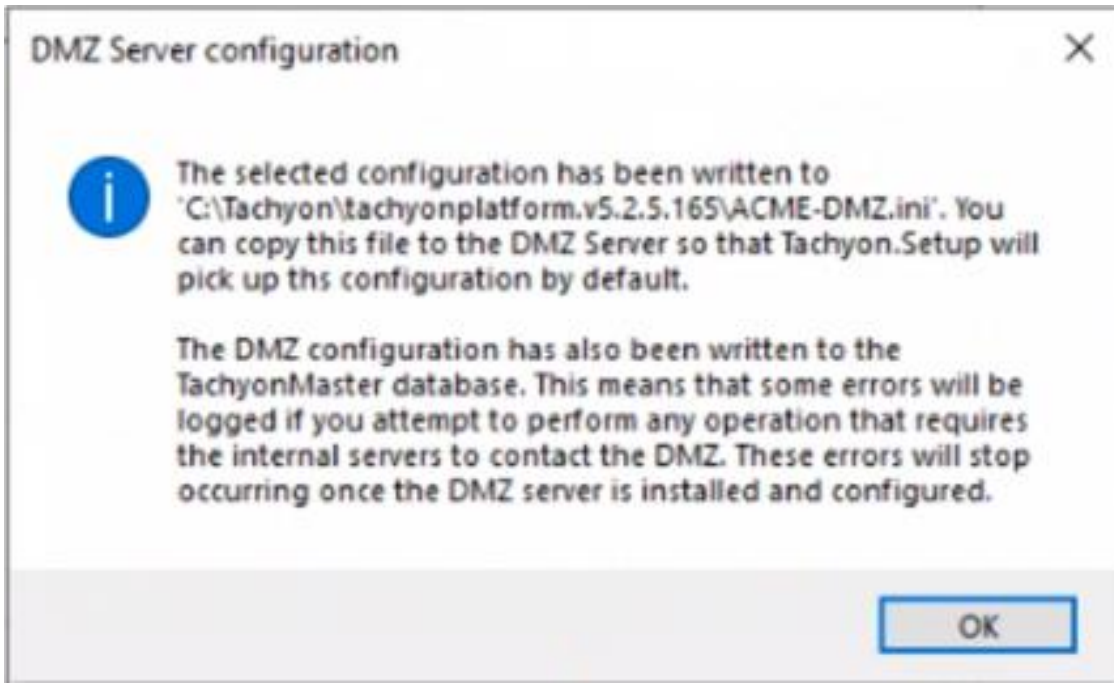
Tip

Location	Detailed steps
	The computername is the value returned when you run the command **cmd /k hostname** on the DMZ Server.
DMZ Server internal DNS Name FQDN - reachable from internal network.	The DNS Name FQDN and port that the internal Tachyon servers will use to connect to the DMZ Server through the DMZ firewall. In our example this is **Tachyondmz.acme.local** and default port **443**. **Tip** In most cases, your DMZ Server will have dual network connections, one for your intranet and another for the Internet. Here, you need to provide a DNS Name that resolves to the IP address of the internal network connection. It will be used by the Consumer API for posting information to the Background Channel in the DMZ, and the Core connecting to the DMZ Switch(es). When you install the DMZ Server, this DNS Name FQDN will be used for the alternate HTTPS binding and exist as a SAN in the binding certificate.
DMZ Server external DNS Name FQDN - reachable from the Internet.	The DNS Name FQDN and port that clients will use to connect to the DMZ Server, and the port used by the Background Channel. In our example this is **Tachyon.acme.com** and default port **443**. This DNS Name FQDN should be the one that the clients on the Internet use for connecting to the DMZ server. The DMZ Tool will save it to the .ini file; when the file is read by Setup in the DMZ, it will be used for pre-configuring the corresponding entry in the Web configuration page. **Note** The Tachyon installer only configures a single address in IIS. If your DMZ server is dual-ported, meaning that it uses a different address for the internal network and the external network, only the latter will be

Location	Detailed steps
	automatically configured in IIS during installation in the DMZ. You will need to manually add the internal address in the IIS configuration. **Tip** In most cases, your DMZ Server will have dual network connections, one for your intranet and another for the Internet. Here, you need to provide a DNS Name FQDN that clients use to connect to the Background Channel using the external network connection. When you install the DMZ Server, this DNS Name FQDN will be used for the main HTTPS binding, and exist as a SAN in the binding certificate.
Number of Switches to install in the DMZ.	The number of Switches you will install on the DMZ Server. By default it will be **1**, but you need to increase the value if you expect to have more than 50,000 clients connecting to this DMZ server. Add one Switch for every 50,000 clients.
Comma-deimited list of Switch IP Addresses.	Enter as many IP Addresses as the number of Switches that you specified above. In our example we have one Switch which has an IP Address **10.10.200.2** **Tip** Each Switch listens for clients on its own network interface with its own IP Address. Each IP Address is for an external connection of the Switch to the Internet. If you are using reverse-NAT in your external router, then this is the IP Address as seen by the DMZ Server, not as seen from the Internet. By default, each Switch listens on port 4000. If you need to change the port, you must do this manually after installation - please contact 1E for guidance.

Location	Detailed steps
	Note When you later run Setup on the DMZ Server to complete Stage 2, the Switch configuration allows you to select the IP Addresses for the Switches, and you must visually verify that the addresses match the ones that you selected here, and in the same order as they appear on the screen. The order is important because each Setup stage independently assigns a numeric name to each Switch, Setup stage 1 stores names in the database, and Setup stage 2 stores the same names in the Switch Host configuration file on the DMZ Server. This information is stored in the SwitchConfiguration table of the TachyonMaster database, and is read by the Switches on the DMZ Server when they start up. Therefore, a Switch will fail to start if the DMZ Server does not actually have a network interface with the expected IP Address.
Authentication - DMZ Server is member of a domain that trust the internal Master Stack server.	Check this checkbox if your DMZ Server will be a "member of a trusted domain" - that is, it will be joined to a domain that has a two-way trust with the domain of your internal Tachyon servers. **Note** If the DMZ Server and internal servers trust each other, then Setup will configure them both to use Windows Authentication for incoming and outgoing connections. If you do not select the option, then Setup will configure the servers to authenticate to each other by means of certificates, and you will need to provide thumbprints below.
Thumbprint of client certificate sent by the Consumer API on Master to Background	This text box is enabled if you did not select "member of a trusted domain". You should enter here the thumbprint of a certificate that is installed in the Master Stack server. It should be enabled for Client Authentication, contain a private key, and be accessible

Location	Detailed steps	
	Channel on DMZ Server.	to the Consumer API. This certificate will be presented by the Consumer API to the Background Channel in the DMZ when the Consumer API sends any changes to the Background Channel. In our example, this is **95dfcc47c31c8bf201104da27ba8a6d792e83665**. **Note** The service account under which the Consumer API is running (by default, NT Authority\Network Service) will need to have read access on the private key of this certificate. The DMZ configuration tool will automatically grant this permission if you are running it on the same machine where the Consumer API is installed. If you are running it in a remote Response Stack, you will need to grant this permission manually at the Master Stack.
	Thumbprint of client certificate sent by Background Channel on DMZ Server to ContentDistribution service.	This text box will only be enabled if you did not select "Member of a trusted domain". This field is optional. You only need to enter this value if you are installing the ContentDistribution service in your internal network, and you want the Background Channel in the DMZ to act as a Proxy so that external clients can reach the internal server. In our example, this is **25fe00fce6240c9260e614eb95680fb6f3ddf06a**. If you are using this feature, then you should enter here the thumbprint of a certificate that is installed in the DMZ server. It should be enabled for Client Authentication, contain a private key, and be accessible to the Background Channel. This certificate will be presented by the Background Channel to the ContentDistribution service in the intranet when its internal Proxy needs to forward any packets to the internal server.

Location	Detailed steps
	 
5 Internal Tachyon Server (Response	On the internal Tachyon Server (Response Stack), restart all Switches and confirm they are working. 1. Restart the **1E Tachyon Switch Host** service. 2. Ensure all internal Switches are running. 3. In Explorer , confirm that at least one internal client is connected.

	Location	Detailed steps
	Stack).	
6	Internal Tachyon Server (Master and Response Stacks) and internal Tachyon client(s).	Ensure that everything is still working by running the tests described in Verifying. **Note** However, remember that Tachyon thinks your DMZ Server is live, although it is not. This means: • Tachyon will attempt to send instructions to the Switch in the DMZ, and will log an error because such Switch is not yet installed. The error is harmless and will not prevent the instruction from being sent to other existing Switches, but you should be prepared to see the error message in the Log without being alarmed. • You will not be able to upload any new instructions which contain resources. If you try to upload an instruction definition that contains resources, the Consumer API will try to upload the resources to all Background Channels, including the one in the DMZ. This will, of course, fail, and it will cause the Consumer API to revert the changes made to all other Background Channels and return an error result. • You will not be able to deploy a Policy, because Policies also require one or more files to be uploaded to all Background Channels, which will be reverted when the DMZ Server fails to update.
7	DMZ Server.	***On the Tachyon DMZ Server* 3**
8	DMZ Server.	Use Services.msc to confirm **Tachyon Switch Host** service is running. If it is stopped then there is an issue with all the Switches. Check the number of Switch log files, and review their contents. There should be one log file for each Switch, plus **Switch.Host.log** Use IIS Manager to confirm the presence of the **Tachyon** website, which contains only the **Background** web application. Check the binding to confirm all the bindings exist that were specified in the Website configuration screen. **Tip** If you wish, you can manually delete the default HTTP binding.

	Location	Detailed steps
9	Internal Tachyon Server (Response Stack) and DMZ Server.	Copy existing **Background Channel** content from the internal Tachyon Server to the Tachyon DMZ Server: 1. Copy the content (minus the web.config file) from each of the following directories on the internal Tachyon Server (Response Stack) to the equivalent directory on the DMZ Server. This is the default location. – **%PROGRAMDATA%\1E\Tachyon\Content** – **%PROGRAMDATA%\1E\Tachyon\Installers** – **%PROGRAMDATA%\1E\Tachyon\PolicyDocuments** – **%PROGRAMDATA%\1E\Tachyon\Updates** **Note** Only the initial copy of the content is required. From this point on, the Consumer API will maintain the content of the Background Channel on the Tachyon DMZ Server. **PolicyDocuments** can be omitted. When you click on the **Deploy** button in Guaranteed State (in step 27), then all policies will be regenerated and automatically copied to all registered Background Channels (see step 7 for registration of DMZ Server). If any source directory is empty then it means you have not tested that feature when verifying the internal Tachyon system in Step 1. This is not critical at this stage, but you should re-check later.
10	Internal Tachyon portal, Tachyon Server (Response Stack) and DMZ	Verify that the internal Tachyon Server can upload content to the Background Channel on the Tachyon DMZ Server: 1. Connect to the Tachyon website and open the Settings application and navigate to **Instruction sets** 2. Delete the **Verification** instructions. 3. Verify that **%PROGRAMDATA%\1E\Tachyon\Content\1E-TachyonPlatform-VerificationStage2** is removed from the internal Response Stack and DMZ servers. 4. Upload the **Verification** Instructions.

	Location	Detailed steps
	Server.	5. Verify that **%PROGRAMDATA%\1E\Tachyon\Content\1E-TachyonPlatform-VerificationStage2** is recreated on the internal Response Stack and DMZ servers.
11	DMZ Server and external Tachyon client(s).	Verify an external client can connect to the Tachyon DMZ Server Switch. Change the client configuration (1E Client configuration file) to point at both the internal Tachyon Server and the Tachyon DMZ Server. This assumes you want client devices to be able to switch between internal and external access. If you prefer, you can simply enter details only for the Tachyon DMZ Server. 1. Edit the **%PROGRAMFILES%\1E\Client\1E.Client.conf** file. 2. Modify the **Switch** configuration property. – In our example this would be: **Switch=tachyon.acme.local:4000;tachyon.acme.com:4000** 3. Modify the **BackgroundChannelUrl** configuration property. – In our example this would be: **BackgroundChannelUrl=https://tachyon.acme.local:443/Background/;https://tachyon.acme.com:443/Background/** 4. Ensure the test device is connected to the external network and not the internal network, then review the **1E.Client.log** to confirm the platform client connects. 5. Browse to the Tachyon website and start the Explorer application, and confirm the external test device is online.
12	Internal Tachyon portal and external client(s).	Run verification steps (Verifying) to verify an external Tachyon client can download content from the Tachyon DMZ Server Background Channel. 1. Browse to the Tachyon website and open the Explorer application. 2. Run the verification stage 1 and 2 and confirm a successful response is received from the external client. **Note** The verification stage 2 Action confirms that content can be downloaded by the platform client.

	Location	Detailed steps
13	Internal Tachyon portal and external client(s).	Verify the external client can receive Policy updates. 1. Open the **Guaranteed State** application in a browser. 2. Click **Administration**, then click **Policies**. 3. Select an existing enabled policy that will affect the client and then click **Disable**. 4. Click **Deploy**. 5. Check the 1E Client log on the external client to verify that it has successfully received a message to fetch new policy, and that the policy download from the Background Channel has been successful. **Note** You do not need any policies defined in Guaranteed State for this step to take effect. Pressing **Deploy** will create an empty policy. This step is required if you are making use of **Tachyon**

1.4.6 Deploying 1E Client

Client features are provided by the 1E Client, which also provides client modules for Nomad, PXE Everywhere Agent, Shopping/WSA, and WakeUp.

For full details, refer to Installing 1E Client.

1.4.7 Uninstalling Tachyon Platform

How to tidy up after uninstalling Tachyon. Follow these recommendations if you want to reinstall Tachyon instead of upgrading.

1.4.7.1 Uninstalling all the Tachyon server components

Use Tachyon Setup to uninstall Tachyon 8.1 instead of Windows Programs and Features (appwiz.cpl), this should not require a reboot.

Click here to see reasons why Tachyon Setup is best for uninstalling server components...

Note

Tachyon Setup is the recommended method of uninstalling all or individual components instead of using the Windows Control Panel.

This is because Tachyon Setup can undo any changes that were done after deploying the components, which would not be undone by the standard application uninstaller. For an example of why this is important, see the information box below.

Before uninstalling, make a backup copy of the installation folder.

The BI (Business Intelligence), SLA (Software Lifecycle Automation) and Catalog components have dependencies and should be uninstalled in the following order:

1. BI
2. SLA
3. Catalog.

Note

The Tachyon Server component can be uninstalled at any point as long as SLA is not installed. SLA has a dependency on Tachyon Server.

If ActiveEfficiency Server is installed (because it was not removed when Tachyon was upgraded), it can be uninstalled at any point.

If you use Tachyon Setup for uninstalling, it will automatically enforce dependencies and uninstall components in the correct order.

1.4.7.1.1 After uninstalling the Tachyon server

Uninstalling leaves behind the following artifacts. Like other Windows installers, uninstalling will leave behind any files, folders, and registry entries created after installation.

Location	Artifacts	Recommendation
Installation folder	You may find web.config files if IIS settings were modified after the previous installation.	Delete or rename the installation folder.
Logs folder	Log files remain.	Delete or rename the logs folder. If it is not deleted, a new installation using the same logs folder will continue to use the old log files.
Registry	Encrypted license details remain in HKLM\SOFTWARE\1E\Tachyon\LicData	The Tachyon registry key can be deleted or left. It is overwritten by the next installation.
SQL Server	TachyonMaster and TachyonResponses databases, as well as any databases used by additional	The databases can be deleted. If not deleted, the

Location	Artifacts	Recommendation
	installed components (Catalog, SLA), will remain at their corresponding SQL instances.	Tachyon Server installer provides an option to drop old databases or use them.

1.4.7.2 Uninstalling 1E Client for Windows

1.4.7.2.1 Manual uninstallation

1E Client can be uninstalled manually by using Windows Apps and Features (appwiz.cpl). A reboot is not normally required.

1.4.7.2.2 Disabling a feature or client module

Please refer to Reconfiguring 1E Client for examples of how to use the **-reconfigure** command-line to reconfigure the 1E Client.

1.4.7.2.3 Uninstallation using the Windows Installer

1E Client can be uninstalled automatically by using a Windows Installer command line, where the {product code} is dependent on the version of the 1E Client. The example below also includes switches that prevent prompting and restart and creates a log file.

```
msiexec /x {BF6F5FA9-64C8-4B72-A6B6-14A582BF96B8} /qn /norestart /l*vx C:\Windo
ws\temp\1EClient-uninstall.log
```

1.4.7.2.4 Tidy up after uninstallation

After uninstallation of 1E Client, the following is left behind. As with other Windows installers, uninstallation will leave behind any files, folders, and registry entries that were created after installation.

Location	Artifacts	Recommendation
Installation folder	None.	
Logs folder	Log files remain. Please refer to Log files for log file locations of 1E Client and its client modules.	The log files can be deleted or renamed. If not deleted, then a new installation that uses the same logs folder will continue to use the old log file.

Location	Artifacts	Recommendation
Client\Persist folder remains.	Leave this folder which contains status information about current instructions. The Persist folder should be deleted only if you do not intend re-installing the 1E Client with Tachyon enabled, or when preparing Sysprep and OS images.	
Tachyon client registry	HKLM\SOFTWARE\1E\Client\Persist	This registry exists if the client feature of the 1E Client is enabled. It is used to keep a record of hash values for its persistent storage files, which includes status information about current instructions. This registry key should be deleted only if you do not intend re-installing the 1E Client with Tachyon enabled, or when preparing Sysprep and OS images.
Nomad Cache	%ALLUSERSPROFILE%\1E\NomadBranch	The folder should be deleted only if you do not intend re-installing the 1E Client with Nomad enabled. Downloaded content is retained so that if Nomad client is re-enabled it will be scanned and re-registered, to make available for peer sharing with other Nomad clients.

Note

HKLM\SOFTWARE\1E\Common and HKLM\SOFTWARE\1E\NightWatchman are used by the 1E NightWatchman Agent, previously part of the 1E Agent.

1.4.7.3 Uninstalling 1E Client for non-Windows

1.4.7.3.1 macOS uninstallation

To uninstall the 1E Client from a macOS device invoke the *uninstall.sh* script from within a sudo bash script. *uninstall.sh* is available within the scripts directory of the Apple Disk Image (dmg) file of the macOS 1E Client.

Alternatively, enter the following commands inside a sudo bash shell:

```
bash$ cd /Library
bash$ pkgutil --only-files --files com.1e.pkg.1E.Client | tr '\n' '\0' | xargs
-n 1 -0 rm
bash$ pkgutil --forget com.1e.pkg.1E.Client
```

1.4.7.3.2 Linux uninstallation

The following command line can be used to uninstall the 1E Client on Linux:

```
sudo rpm -e 1e.client
```

Uninstallation will leave behind files, folders, and registry entries that were created after installation:

Location	Artifacts	Recommendation
Installation folder	None.	
Logs folder	Log files remain.	The log files can be deleted or renamed. If not deleted, then a new installation that uses the same logs folder will continue to use the old log file.
Client\Persist folder remains.	You should keep the **Persist** folder, which contains status information about current instructions, only if you intend to re-install the 1E Client.	

1.4.7.3.3 Solaris uninstallation

Note

1E Client is no longer available for Solaris, but 1E may reintroduce it, if there is sufficient demand.

1.4.8 Tachyon Product Pack Deployment Tool

The Tachyon Product Pack Deployment Tool (PPDT) can be used to upload multiple Classic and Integrated Product Packs into Tachyon.

The PPDT is found in the ProductPacks folder of the Tachyon Platform zip, and with appropriate permissions. Once the zip has been extracted, the tool can be used to upload any Classic and Integrated Product Packs found in its folder structure. Ensure you use the same version of the tool to match the version of Tachyon.

Classic Product Packs

Classic Product Packs contain instructions, for use in Tachyon Explorer and other Tachyon applications.

Classic Product Packs can also be uploaded using the Tachyon portal Settings app→ Instructions → Instruction Sets, described in Instructions Menu, this method does not assign instructions to any instruction set. Settings can also be used to export instructions.

Hyphens

The tool creates an instruction set with the same name as its zip. When creating or updating an instruction set, the tool converts hyphens to spaces. Hyphens can be included in the names of Instruction sets, but they are converted by the tool.

The Settings application keeps hyphens and spaces in the zip name when downloading (exporting) an instruction set. If the tool is then used to re-upload the same pack, the hyphens are lost, creating a new instruction set with a different name from the original.

Individual Product Packs are not versioned, however, each instruction has its version stored in the instruction definition.

Integrated Product Packs

Integrated Product Packs contain policies, rules, and fragments for use by Guaranteed State, and may also include instructions.

If the Product Pack contains instructions associated with the policies, the tool creates an instruction set using the name in its manifest file.

Note

When the tool is used to upload new versions of instructions, then the updated instructions remain in their current instruction set, they are not moved to the new set created by the tool.

Tachyon Product Packs reference provides full details of all the product packs included in the Tachyon Platform zip.

1.4.8.1 Getting started

To run the tool, you need the following:

1.4.8.1.1 Account permissions

The account used to run the **Tachyon.ProductPackDeploymentTool.exe** must:

- Have local administrator rights on the computer it is running on
- Exist as a Tachyon user assigned to either **Installer** or **Full Administrator** role.

1.4.8.1.2 The account used to run the Tachyon.ProductPackDeploymentTool.exe must:

- Have local administrator rights on the computer it is running on
- Exist as a Tachyon user assigned to either **Installer** or **Full Administrator** role.
  - Guaranteed State administrator
  - Instruction Set administrator.

1.4.8.1.3 Locating the Tachyon Product Pack Deployment Tool

The tool is included in the Tachyon Platform zip file under the **ProductPacks** folder.

- **Tachyon.ProductPackDeploymentTool.exe** (and its supporting files) is used to upload Product Packs into Tachyon.
- The tool creates a log file called **Tachyon.ProductPackDeploymentTool.log** in the same folder.

The **ProductPacks** folder contains two directories, **Classic** and **Integrated**.

- The **Classic** directory holds a number of classic Product Packs that contain Tachyon Instructions.
- The **Integrated** directory holds a number of integratedProduct Packs that contain definitions for some Guaranteed State Policies, associated Fragments, and Instructions. In addition, a core utility pack has been provided with common Fragments that you can use to build your own Policies.

Tachyon Product Packs reference provides full details of all the Product Packs included in the Tachyon Platform zip.

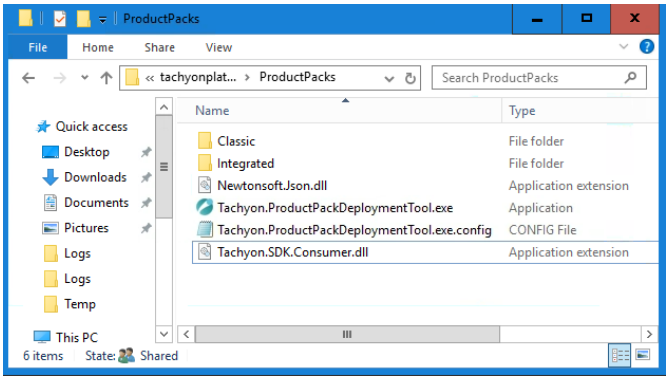
1.4.8.2 Running the Tachyon Product Pack Deployment Tool

Here are the steps for running the tool:

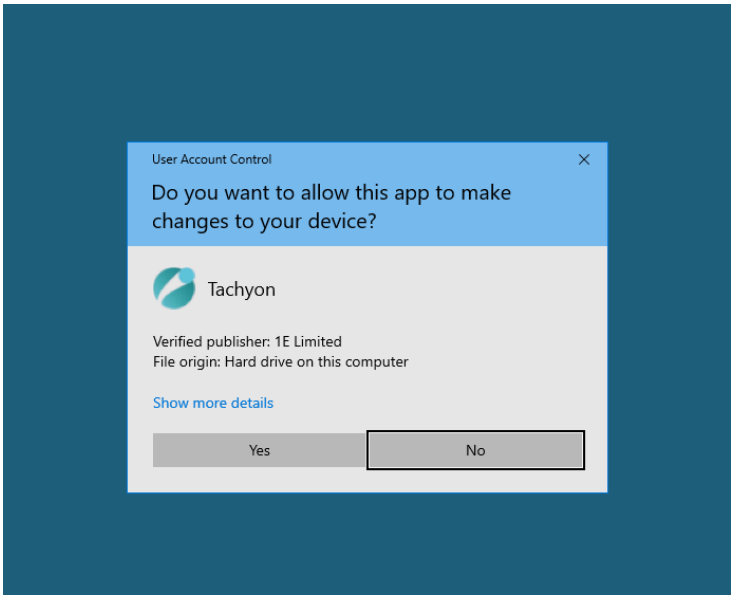
1. Navigate to the directory where the **tachyonproductpacks.<version>.zip** file has been unzipped.
2. You will see two directories: **Classic** and **Integrated** within which are actual Product Pack zips.
3. In this directory you can also see the **Tachyon Product Pack Deployment Tool** files:
   - Newtonsoft.Json.dll
   - Tachyon.ProductPackDeploymentTool.exe

- Tachyon.ProductPackDeploymentTool.exe.config
- Tachyon.SDK.Consumer.dll

4. Double-click on **Tachyon.ProductPackDeploymentTool.exe**.



5. Click on **Yes** if any UAC dialog is displayed.



6. The **Tachyon Product Pack Deployment Tool** dialog will appear.

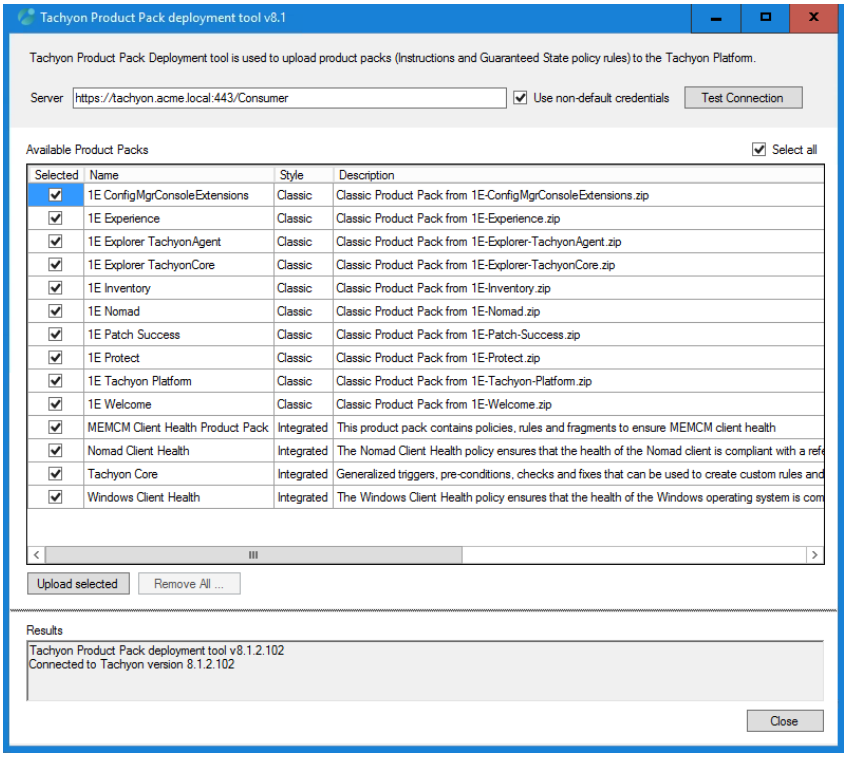
   You must specify the URL of the Tachyon Consumer API in the **Server** field and then click on **Test Connection** to verify that you have entered the correct value.

   Alternatively, you can specify the parameter *-url "<ConsumerAPI>"* on the command line, for example: *-url "https://tachyon.acme.local/Consumer"*. If you run the tool on the Tachyon Server, the tool will automatically prefill the URL.

   The **Style** column of the **Available Product Packs** table indicates whether each **Product Pack** is **Classic** or **Integrated**. The **Available Product Packs** table will be populated with all the zip files encountered in the directory the tool was launched from and all its sub-directories.

   The **Select all** box can be used to select or deselect all the items in the **Available Product Packs** table.

Click **Use non-default credentials** if you need to use alternative credentials. Domain is not required if connecting to a non-domain joined server, or server in an untrusted domain.



1.4.8.2.1 Uploading Product Packs

When you have selected and checked the Tachyon Consumer API location you will then be able to upload the selected **Available Product Packs** by clicking on the **Upload selected** button. The content of the selected packs will then be uploaded to the Tachyon Server. The **Results** field displays the progress of the operation.

> **Warning**
>
> Updating Policies, Rules, Fragments, and Triggers that already exist in the Tachyon database is supported, but you need to be careful to ensure that the new artifacts uploaded are compatible with the existing ones. In particular, any new fragments and trigger templates uploaded need to have the same parameters that are used by the version of the same artifact that already exists in the database. Otherwise, any rules that are passing the previous set of parameters to the fragments will be broken when the new fragments start requiring a different set of parameters to be passed to them.

1.4.8.3 Log files

The log file is called **Tachyon.ProductPackDeploymentTool.log**. It is created in the same folder where the tool executable is located.

The logging level can be changed by adding the parameter **-log <level>** on the command line, for example, **-log DEBUG**. Supported values available:

- TRACE
- DEBUG
- INFO (default)
- WARN
- ERROR

1.4.8.4 Command-line options

-server or -url: Specifies the url for the Consumer API.

-log: Sets the logging level. Supported values available: **Trace**, **Debug**, **Info**, **Warn**, **Error**

-domain, **-user** and **-password**: These options allow you to override the default behavior of using the currently logged-in Windows user. A domain is not required if connecting to a non-domain joined server. This option is useful when you need to upload Product Packs to a Tachyon platform running in the cloud, or from a computer that is not joined to the same domain.

Example

```
Tachyon.ProductPackDeploymentTool -server https://tachyon.acme.local/Consumer -log debug -user administrator -password notasecret
```

1.5 Upgrading Tachyon Platform

Guidance for upgrading Tachyon, SLA, and ActiveEfficiency platforms to Tachyon Platform.

Before you attempt an upgrade, please ensure you thoroughly read all sections that apply to you. Combine the steps if your system matches multiple upgrade scenarios. If you cannot find a complete match, please contact 1E.

- In-place upgrade of Tachyon
- In-place upgrade of ActiveEfficiency Server for Nomad
- Side-by-side upgrade of ActiveEfficiency Server for Nomad
- In-place upgrade of ActiveEfficiency Server for Shopping

Tachyon Setup will upgrade ActiveEfficiency Server to Content Distribution if it detects the ActiveEfficiency website is installed on the server.

- ActiveEfficiency Server is now deprecated, and is not required by the latest versions of products that previously used it: Nomad 7.1 & 8.x, AppClarity 7.0, 7.1 & 8.x, nor Shopping 6.1
- ActiveEfficiency Version 1.10.100 was released on March 2020 and is used by Nomad 7.0 and Shopping 6.0 which are still in support
- ActiveEfficiency Version 1.10 was released in November 2018 and was required by older versions of Nomad, Shopping, and AppClarity which are now out of support.

Tachyon Setup does not upgrade the following 1E server products:

- PXE Everywhere Central - please refer to Upgrading PXE Everywhere
- Shopping (Central or Receiver) - please refer to Shopping - Upgrading to Shopping
- NightWatchman Management Center - please refer to NightWatchman Enterprise - Upgrading NightWatchman Enterprise
- WakeUp Server - please refer to NightWatchman Enterprise - Upgrading NightWatchman Enterprise
- ActiveEfficiency Scout.

For upgrading clients, please read below first, then refer to Upgrading 1E Client.

Note

When upgrading to Tachyon Platform 8.1, you will need a new license. Please contact your 1E Sales account manager for license inquiries.

If you are upgrading from SLA Platform 3.3, Tachyon 3.3, or Tachyon 4.x, you must first upgrade to Tachyon 5.2.

1.5.1 Preparing for upgrade

1.5.1.1 SQL Server AlwaysOn Availability Group

If you are using an Availability Group (AG) then you must temporarily remove the Tachyon databases from the AG during the upgrade.

Please refer to high availability options for SQL Server:

- Upgrade Tachyon with an existing Availability Group.
- Upgrade Tachyon with a new Availability Group.

1.5.1.2 Backup first

Note

Before doing a re-installation or upgrade of the Tachyon Platform, make a backup of the following (but first see the note below about automatic backups):

- Tachyon Master database

  Note

  Backing up the Tachyon Responses database is **not** usually needed, unless there are instruction responses that you need to keep. Tachyon responses are not permanently held data and will naturally expire according to the settings specified when an instruction was run, typically in hours or possibly days. If in doubt, there is no harm in backing up the Tachyon Responses database as well.

- Tachyon Server installation directory.
  - including the config files, which may have been manually updated in the previous installation.

  - Switch certificate files.
- Earlier versions of Product Packs that have been modified.

Note

Tachyon Setup will automatically perform a backup of the following items:

- Tachyon Server installation directory. This is backed up to a subfolder named Tachyon.bak under the root installation folder for Tachyon . All files, including the .config files and certificate files, will be copied.
- IIS configuration. This is done by taking a copy of the applicationhost.config file from the Windows system folders. The backup file is placed at the same location and is named like the original file with a suffix that indicates the date and time when the copy was taken.
- The following databases are backed up to the default location for backups that is configured in the database server. By default, this points to a subfolder named "Backups" under the folder where the executable for SQL Server is installed. Unless you are installing a small lab or proof-of-concept, this is usually *not* a good location for the backups, so make sure that you configure the backup location in SQL Server to an adequate folder before starting the Tachyon upgrade:
  - 1ECatalog
  - ContentDistribution (optional, required by Nomad)
  - SLA-Data
  - SLA-Shared
  - SLA-Integrate
  - TachyonMaster
  - TachyonResponses
  - TachyonExperience (optional, required for Experience).

  The Product packs are not copied by themselves, but they are kept in a table within the TachyonMaster database, which *is* backed up.

1.5.2 In-place upgrade of Tachyon

This scenario is for upgrading from an older version of Tachyon.

If your current Tachyon server already has ActiveEfficiency Server installed then please also read the following according to what it is currently used for.

- In-place upgrade of ActiveEfficiency Server for Nomad
- In-place upgrade of ActiveEfficiency Server for Shopping

Tachyon Setup is used to upgrade the following versions of Tachyon and its applications.

Version	Features
Tachyon Platform 5.2, 8.0	Real-time and inventory features. Applications: Explorer, Guaranteed State, Patch Success, Application Migration, AppClarity, Experience, and Nomad.
Tachyon Platform 5.0, 5.1	Real-time and inventory features. Applications: Explorer, Guaranteed State, Patch Success, Application Migration, AppClarity, Experience, and ActiveEfficiency.

Tachyon 8.1 includes real-time and inventory features. Applications: Guaranteed State, Patch Success, Application Migration, AppClarity, Experience, and Nomad.

Tachyon Setup assumes you will keep existing applications when upgrading and optionally install additional applications. However, your Tachyon license ultimately determines which applications you can install and what you are able to use when you connect to the portal.

Upgrading from older versions

When upgrading to Tachyon Platform 8.1, you will need a new license. Please contact your 1E Sales account manager for license inquiries.

If you are upgrading from SLA Platform 3.3, Tachyon 3.3, or 4.x, you must first upgrade to Tachyon Platform 5.2. There are additional notes, which can be found in the Tachyon Platform 5.2 - Upgrading to Tachyon Platform pages.

1.5.2.1 Steps for in-place upgrade of Tachyon Platform

1. Upgrade server hardware as required - please refer to urn:resource:component:614830.
2. Run Tachyon Setup on the Tachyon Master Stack server to upgrade to Tachyon Platform.
3. Run Tachyon Setup on remote Tachyon Response Stack servers (if used).
4. Verify existing clients.
5. Run Tachyon Setup on remote Tachyon DMZ Server (if used).
6. Verify existing Internet based clients.
7. Upgrade existing Product Packs, and install new ones.
8. Deploy new 1E Client to devices (with Tachyon enabled) and verify.
9. Review Role name changes and rationalize your existing roles if necessary.

1.5.2.2 Changing the Platform configuration when reinstalling or upgrading

1.5.2.2.1 Keep the DNS Names

Each server that has Tachyon platform components installed requires its own DNS Name. A DNS Name can be a DNS alias, CNAME or Host (A) record.

Master Stack	The Master Stack is used by the following, therefore it helps users if it has a recognizable and convenient DNS Name such as **tachyon** - this is specified during installation of the Tachyon Server using Tachyon Setup. • Tachyon users, approvers and administrators connecting to the Tachyon Portal and Consumer API • Remote tools and Consumer applications connecting to the Consumer API • Remote Response Stacks and DMZ Server connecting to the Coordinator service Platform services also reside on the Master Stack, which non-Tachyon clients connect to, for example: • Application Migration, used by Windows Self-Service task sequences • AppClarity, used by AppClarity Software Reclaimer
DMZ Server	The DMZ Server is a type of Response Stack used to provide Tachyon Real-time and Inventory services to Internet-based clients. It requires an external DNS Name - for example **tachyonext** - this is specified during installation of the DMZ Server using Tachyon Setup. The DNS Name is shared between the Switch network interfaces and Background Channel on the DMZ Server, and specified during installation of Tachyon clients, and stored in their configuration file.
Response Stack	A Response Stack is used to provide Tachyon Real-time and Inventory services to clients on the internal (corporate) network. The choice of DNS Name is discussed in the table below. The DNS Name is shared between the Switch network interfaces and Background Channel on the Response Stack, and specified during installation of Tachyon clients, and stored in their configuration file.

The number of DNS Names used by a system depend on the location of Tachyon and other Platform services. The table below describes options.

Single DNS Name	A Tachyon system can have a single DNS Name if all components are installed on the same server, for example **tachyon** - this is specified during installation of the Tachyon Server using Tachyon Setup. If the server has multiple Switches, and therefore multiple network interfaces, then the same DNS Name can be shared by all Switches, the Background Channel and Master Stack.

Multiple client-facing DNS Names

The following client-facing components can each have their own DNS Name:

- Tachyon Switch and Background Channel on Response Stack servers, including DMZ Server
- Tachyon Platform services on the Master Stack, used by clients of A pplication Migration and/or AppClarity software reclaim
- Tachyon Portal, and Consumer API, on the Master Stack, used by administrators.

Note

Master and Response Stacks must have different DNS Names if they exist on different servers:

- The Master Stack has its own DNS Name, for example, **tachyon**
- Each Response Stack can have its own client-facing DNS Name, or they can share a common client-facing DNS Name, for example **tachyonrs**.

When a Response Stack is installed on the same server as Master Stack, it will normally share the same DNS Name as Master Stack as described under #UUIDba4ce843708df87c3577ca1f7920f3d8_id_PreparationSingleDNSName. However, if you have multiple Response Stacks and want them to share the *same* DNS Name, then the Master Stack must use a *different* DNS Name. This approach of all Response Stacks sharing the same DNS Name simplifies adding further Response Stacks at a later date.

During installation - using Website configuration - you need to consider the following:

HTTP binding	Required for installation, but can be manually removed later - please refer to Removing the HTTP binding from the Tachyon website. This binding is not used by Tachyon clients or administrators, but can optionally be used for Application Migration and/or AppClarity reclaim clients. Example name **acme-tcn01**.
HTTPS binding	Required. This is the main binding. On a Master Stack server (that has no Response Stack components) it is used by administrators to connect to the Tachyon Portal. It can optionally be used for Application Migration and/or AppClarity reclaim clients. Example name **tachyon** .

	On a Response Stack server, it is used by clients to connect to Switches and/or Background Channel. Example name **tachyon** or **tachyonrs**. See panel above about making the right choice. On a DMZ Server, it is used by Internet-based clients to connect to Switches and/or Background Channel. Example name **tachyonext**. See below.
Alternate HTTPS binding	Required, except in the simplest (single server) configurations, described above. It is typically used by other Tachyon Platform servers to connect to each other, but there are other scenarios. • Required on a Response Stack server if it will have a DMZ Server connected to it. Example name **tachyonalt**. • Required on a DMZ Server - used by internal servers to connect to the DMZ Server - see below. Example name **tachyondmz**. See below. • Required on a Master Stack if you have local and remote Response Stack(s) - used for inter-server communications. Example name **tachyonalt**. • Required on a Master Stack if the main HTTPS binding is used by client-facing components, and you want a different name for the Portal. Used by administrators to connect to the Tachyon Portal. Example name **tachyon**. • Required on a Master Stack if you need a different **HTTPS port** for Application Migration and/or AppClarity reclaim clients. This can be by choice, or if you have upgraded from an original SLA Platform installation that used different ports.
Manual bindings	You can manually add further HTTP and HTTPS bindings after installation, to help differentiate the services which client devices and administrators connect to.

If you are upgrading ActiveEfficiency to Tachyon Platform then you might have had a HTTPS binding described as **aeserver** in previous documentation.

If Master and Response Stacks are on the same server and you want them to have different DNS Names, then use the main binding for client connections to the Response Stack (because it is client-facing) and use the Alternate binding for other connections to the Master Stack. A simpler option is to put the Response Stack on its own server. Remote Response Stacks are recommended if the Master Stack is also hosting services AppClarity Software Reclaimer or Application Migration.

If you want to configure Switches on the same server to use multiple DNS Names, you will need to seek guidance from 1E. In most cases this is not required or recommended.

Internal DNS Names

A DMZ Server is a special example of a Response Stack. The DMZ Server itself requires two DNS Names:

- A client (external) facing DNS Name - for example **tachyonext** - which is shared between the Switch network interfaces and Background Channel on the DMZ Server - this is specified during Tachyon Setup as the main HTTPS binding
- An internal facing DNS Name for the internal network - for example **tachyondmz** - this is specified during Tachyon Setup as the alternate main HTTPS binding.

Note

Both DNS Names must be included in the web server certificate. You can manually replace the external/client facing certificate after installation, to comply with best practice not to expose internal names in an external facing certificate.

The internal Response Stack also requires an additional DNS Name - for example **tachyonalt** - for internal communications with the DMZ Server.

Please refer to Implementing a Tachyon DMZ Server for more detail about DMZ Servers.

Note

Tachyon Setup supports installation of one HTTP and up to two HTTPS bindings, but you can manually add more bindings after installation.

Tachyon Setup currently supports only one Web server certificate, which must contain all the DNS Names used by the HTTPS bindings on that server. Each DNS Name must be included as a DNS Name in the **Subject Alternate Name (SAN)** entry of the web server certificate.

You can manually add more certificates, and change bindings. Please refer to Certificate requirements . Please note that Tachyon Setup helps maintain the main and alternate HTTPS bindings using one certificate.

1.5.2.2.2 Moving Server

Agents use the DNS Name FQDN to connect to the Switch and Background Channel. Provided the DNS Name FQDN remains the same, the server can be renamed or moved without having to re-configure clients.

If the server hosting a Tachyon Server is renamed or moved, then it will need a new certificate and Tachyon Server must be re-installed. The database can be kept. There is also a known issue where new website URLs do not get updated in the database tables.

Please contact 1E for advice if a new configuration is required when re-installing or upgrading a server.

1.5.3 Upgrading to Tachyon Platform

Note

Partial Upgrades

You may still be asked at some intermediate steps about configuration information for the components that will not be installed. You should still provide it, because it may be relevant for Tachyon Setup at the time of configuring other components that *are* being installed so that they can interact with the components that are *not* being installed but are already present in the system.

Use the following process when upgrading Tachyon to Tachyon Platform, and keep the same configuration and the TachyonMaster database. Keeping the same configuration means using the same installer properties as the previous installation.

If changing the configuration, please refer to Changing the Platform configuration when reinstalling or upgrading.

Ref	Step	Notes
1	Ensure you have prerequisites ready for installation of the new version. • Tachyon Server installer properties • Server installation account • Backup the Switch certificate files, these	Preparation for an in-place upgrade is not as complex compared to a new installation, provided the configuration remains the same. If changing the configuration, please refer below to Changing the Platform configuration when reinstalling or upgrading . Determine if you will re-use the existing Web certificate or a new one. If re-using the certificate and upgrading from a version of prior to 5.0 then ensure you make a copy of the certificate files in the Switch SSL folder. If using a new certificate, then follow the guidance in Server Provisioning. If you are upgrading from Tachyon 5.x, the certificates will

Ref	Step	Notes
	are required during the upgrade • License file for new version of Tachyon Review Known issues.	already be in the local Windows Computer Certificate Store so there is no need to backup. If in doubt about your configuration, review each of the configurations in the Tachyon installation folder. A later step in this process asks you to make a backup copy of the installation folder. This allows you to review configuration settings and also retain a backup of the Switch certificate files. 1E recommends using the same server installation account as the original installation, but this is not mandatory provided the account is an existing Tachyon administrator user. You can check which is the original installation account by looking in the Permissions page and finding the user which does not have an edit or delete icon. **Note** When upgrading to Tachyon Platform 8.1, you will need a new license. Please contact your 1E Sales account manager for license inquiries. If you are upgrading from SLA Platform 3.3, Tachyon 3.3, or Tachyon 4.x, you must first upgrade to Tachyon 5.2.
2	Inform Tachyon users when you plan to upgrade the system.	You should notify Tachyon users about the impending upgrade. This includes users of external consumers such as the extension described in Using Tachyon in Configuration Manager. To help identify the users of the Tachyon system, you can review the Tachyon Permissions. You can also review the Tachyon Consumers in order to remind yourself of any 3rd party systems that will be affected by the upgrade. Any instructions that are running or pending approval prior to the Platform and Agent upgrade will not be affected, other than be delayed by services being temporarily down.
3	Shutdown the existing Tachyon system.	If you want to keep any instruction responses, review the notes in the next step before shutting down the system.

Ref	Step	Notes
	1. Stop or uninstall external or third-party Consumers (if any) 2. Stop the Tachyon services – 1E Tachyon Switch Host – 1E Tachyon Coordinator	Shutting down the system gracefully ensures there are no instructions in process and prevents access. The installer will internally shut down the services if you do not stop them manually. Stopping them manually gives you greater control over when they are stopped. The services will be restarted automatically after the upgrade. **Note** Both the Tachyon Switch Host and the Coordinator can take some time to stop their services. No other services for the applications associated with Tachyon need to be stopped. **Warning** Do not stop or disable the Tachyon website or application pools. The installer needs them to be active in order to complete all installation tasks.

4	Close all active connections to the Tachyon databases.	To avoid Known issues when upgrading, you must ensure there are no active connections to the databases.
		You can use the following SQL script to identify which programs have active connections to the Tachyon databases.
		`SELECT DB_NAME(dbid) as [database], loginame, hostname, program_name`
		`FROM sys.sysprocesses`
		`WHERE DB_NAME(dbid) LIKE 'Tachyon%' AND program_name LIKE 'Tachyon%'`
		`ORDER BY DB_NAME(dbid), loginame, hostname, program_name;`
		With the Tachyon services stopped, any open connections to the database, such as Tachyon Consumer and Tachyon Portal, should not cause the upgrade to fail and can be safely ignored.

5	Backup the databases.	If you use Tachyon Setup to perform the upgrade, it backs up the following databases: • TachyonMaster.

Ref	Step	Notes
		• TachyonExperience (if installed). • SLA-Data. • SLA-Shared. • SLA-Integrate. • ContentDistribution (if installed). • 1ECatalog. The following notes apply to the Responses database and whether you would need to create a backup of that database too: **Note** Backing up the Tachyon Responses database is **not** usually needed, unless there are instruction responses that you need to keep. Tachyon responses are not permanently held data and will naturally expire according to the settings specified when an instruction was run, typically in hours or possibly days. If in doubt, there is no harm in backing up the Tachyon Responses database as well.
6	Make a copy of the Tachyon Server installation folder.	The installation folder contains the following non-default files: • Switch certificate files in the SSL folder, these are required during the upgrade and should be copied to the directory with the TachyonServer.msi. • Configuration files for the website, web applications, services and Switch (*.config files). • Other customizations. • Content in the Background folders (these are the **Content** and **Updates** folder in %ALLUSERSPROFILE%\1E\Tachyon).
7	Install Tachyon Server.	Install Tachyon Server using the same configuration as before. Do not drop the databases.

Ref	Step	Notes
		Please refer to Tachyon Setup for more details.
8	Post-install tasks.	Repeat any Tachyon Server post-installation tasks that are relevant for an upgrade installation and are not performed automatically by Tachyon Setup.
9	Customizations.	Re-instate non-default settings. • Configuration files for the website, web applications, services and Switch (*.config files) **Note** Tachyon Setup will automatically backup and restore any entries in the .config files that it modifies during installation. Do not simply replace config files. Instead, compare the old and new versions and consider which changes can or need to be re-instated. In some cases, new versions may contain fixes for workarounds included in the old files. Please contact 1E if you have any difficulties. • Other customizations **Note** The Tachyon Setup installer will backup and restore customized mail headers. • Content in the Background folders (these are the **Content** and **Updates** folder in %ALLUSERSPROFILE%\1E\Tachyon)
10	Verify.	See Verifying page.

1.5.4 After upgrading to Tachyon Platform

1.5.4.1 All versions

- Verify the installation - see Verifying page.
- Upgrading and updating Instructions.
- After upgrading, you should perform a sync for all configured Connectors, followed by the Basic Inventory Consolidation report.

1.5.4.2 After upgrading from Tachyon Platform 8.0 or earlier

Tachyon Platform 8.1 (and later) no longer requires SQL Analysis Services (SSAS) for Tachyon Experience.

The following points should be considered if you have upgraded from Tachyon 8.0 or earlier version, and you previously used Tachyon Experience.

- You can delete the **TachyonExperience** database from your SSAS instance
- If you are not using Patch Success, you can decommission your SSAS instance - Patch Success uses the **SLA-BI** database on the SSAS instance
- Please review Device Deduplication page. Deduplication is basically the same as before, but has some minor changes because the Experience Cube no longer exists.

1.5.4.3 After upgrading from Tachyon Platform 5.0 or earlier

Tachyon Platform 5.1 (and later) uses UTC for Schedules.

The following points should be considered if you have upgraded from Tachyon 5.0 or earlier version.

- If you have previously configured any Schedules for Instructions, these will be converted to using UTC time. You will need to revisit these to ensure the time you want the Schedules to run is still correctly configured
- If you have previously configured any Schedules for Tachyon or Configuration Manager Connector syncs, these will need to be deleted and re-created - as the sync process for both of these types of connector has been redefined. Please refer to Tachyon connector and System Center Configuration Manager connector for more details.

1.5.4.4 Upgrading and updating Instructions

Tachyon Instructions are designed as far as possible to be backwards compatible, but as a general rule we recommend that you update your Tachyon Product Packs to the latest version so that you can gain the benefit of newer features.

When upgrading you should be able to safely keep your existing Instructions. We recommend that newer versions of Instructions are verified in a test environment to ensure that they still behave as expected before updating in your production environment.

> **Note**
>
> An instruction is not upgraded if it is the same version, or is currently *in use*. You will be notified if any instructions are not upgraded because they are in use. You can upload the product pack again later, after the instruction has completed, or cancelled.

Your license should retain any code signing certificates you may have registered. This means your custom instructions should continue to be licensed as normal following an upgrade of Tachyon. You may want to check the /document/preview/736743#UUID-33c212b3-863e-21bc-bc5d-52e41a0492b3 in the TachyonSDK pages to check for any changes to the SCALE language.

1.5.5 In-place upgrade of ActiveEfficiency Server for Nomad

This scenario is for upgrading a server that has ActiveEfficiency Server installed and used by Nomad. If ActiveEfficiency is also being used for Shopping then please also read In-place upgrade of ActiveEfficiency Server for Shopping.

Tachyon Setup will do the following automatically, but only if your Tachyon license includes Nomad, *and* you choose to install Nomad, *and* a local installation of ActiveEfficiency Server is detected.

- replace ActiveEfficiency Server with Content Distribution to support to new Nomad clients
- create a virtual directory in the Tachyon website and use **HTTP redirection** to support legacy Nomad clients
- rename the ActiveEfficiency database as ContentDistribution if it exists on the SQL Server instance you selected for the ContentDistribution database (the database is renamed, but the database mdf and ldf filenames are not changed)

The last point means ActiveEfficiency data will be retained in the ContentDistribution database, to provide the following:

- Existing pre-cache jobs, and paused collections, are migrated so they are shared by old and new Nomad clients, and can be managed by upgraded installations of the Nomad Configuration Manager Console Extensions
- Locations and Single-site content registrations are not migrated, but retained in legacy database tables so they continue to be used by legacy Nomad clients - content registrations for new Nomad clients are created in new database tables, so that legacy and new clients function independently.

The ActiveEfficiency database will be retained, and no data migrated, if it is on a different SQL Server instance than the one you specified for your ContentDistribution database. To automatically migrate data during upgrade, you will need to copy the ActiveEfficiency database to the new location, and reconfigure ActiveEfficiency Server to use the copied database. Alternatively, you can Manually migrate data as described in the link.

If the installation of Content Distribution fails for whatever reason, the database changes are rolled back.

Although ActiveEfficiency Server is replaced by Content Distribution, the Nomad client in 1E Client 5.2 (and later) does not connect directly to it. Instead, it connects to the same Tachyon Switch and Background Channel as the Tachyon client - the 5.2 and later versions of the Background Channel contain a reverse proxy which forwards API requests to Content Distribution. The Tachyon Switch and Background Channel may be on the same server as the Tachyon Master stack, or on a remote Response Stack. This means any remote Tachyon Response Stacks or DMZ Server (if used) must be upgraded also, before your Tachyon infrastructure can support new Nomad clients.

When upgrading Nomad clients, the new Nomad clients will no longer require an HTTP connection to the server that previously hosted ActiveEfficiency Server. However, if you are upgrading from a Tachyon or SLA server, then other 1E software (Application Migration and AppClarity Software Reclaimer) may still use HTTP to connect to SLA services on the server.

> **Note**
>
> If you are currently using Nomad with ActiveEfficiency, you must upgrade both Nomad clients *and* ActiveEfficiency. You should only upgrade to Tachyon Platform 8.1 if you are

prepared to upgrade Nomad clients to 1E Client 8.1 (with Tachyon and Nomad clients enabled) and replace ActiveEfficiency with Nomad and Content Distribution on Tachyon Platform.

1.5.5.1 Steps for in-place upgrade of ActiveEfficiency

1. Review your requirements to determine which features you need of 1E Client and Tachyon Platform, please refer to Planning for Tachyon Platform pages
2. Upgrade your server hardware as required- please refer to Server sizing requirements
3. Reconfigure Shopping Central (if used)
4. Uninstall ActiveEfficiency Scout (if used) and disable associated Windows Task Scheduler job(s)
5. Run Tachyon Setup on the ActiveEfficiency server to upgrade it to Tachyon Platform - please refer to Tachyon Setup
6. Run Tachyon Setup on remote Tachyon Response Stack servers (if used) - please refer to Tachyon Setup
7. Verify existing clients, to confirm Tachyon continues to function as before, with Nomad clients using **HTTP redirection** as described above
8. Run Tachyon Setup on remote Tachyon DMZ Server (if used) - please refer to Implementing a Tachyon DMZ Server
9. Verify existing Internet based clients
10. Deploy new 1E Client to some test devices (with Tachyon and Nomad client enabled)
11. Verify the test devices
12. Upgrade Nomad tools - please refer to Upgrading Nomad
    a. Upgrade Nomad Admin Tools and server components
    b. Update OS Deployment Task Sequence actions to use the Tachyon Platform
    c. Review Automatically migrated data and configure Nomad Sites
13. Deploy new 1E Client to remaining devices.

Warning

Do not reinstall ActiveEfficiency on the Tachyon Platform server.

1.5.5.2 Automatically migrated data

As stated above, the upgrade of ActiveEfficiency Server to Tachyon Platform automatically migrates details of pre-cache jobs, and paused collections, so they can be managed by upgraded installations of the Nomad Configuration Manager Console Extensions. You can review these in the Nomad app.

Locations, Single-site data, and content registrations are not migrated, but are retained in legacy database tables so they continue to be used by legacy Nomad clients. This data is not shared with new clients, so that legacy and new clients function independently. New clients will re-register their content automatically up to 24 hours later, or can be forced by using the NomadBranch command-line parameter **-cdssync** as described in NomadBranch.exe command-line switches. Old and new clients will perform master elections and peer-share content if they are the same subnet, but they will only use SSD with their own set of clients.

You will continue to maintain Nomad Sites (previously known as Locations) using one of the new versions of the example PowerShell scripts provided with the Nomad Admin Tools. Alternatively, you can use the examples to modify your existing script to use Content Distribution instead of ActiveEfficiency.

1.5.6 Side-by-side upgrade of ActiveEfficiency Server for Nomad

This scenario is for an existing Nomad and ActiveEfficiency installation, where Tachyon Platform is on a different server, either newly installed or upgraded from on earlier version of SLA Platform or Tachyon. The old ActiveEfficiency Server is eventually decommissioned. There is no requirement for **HTTP redirection** on the Tachyon server, because old Nomad clients will continue to use the ActiveEfficiency server, and new Nomad clients will use Content Distribution on the upgraded Tachyon Platform. Each set of clients functions independently. Some data is manually migrated from the ActiveEfficiency server, as described below.

If your Tachyon license includes Nomad, *and* you choose to install Nomad, *and* a local installation of ActiveEfficiency Server is detected, then you are doing an In-place upgrade of ActiveEfficiency Server for Nomad.

If a local installation of ActiveEfficiency Server is not detected, the ActiveEfficiency database is retained even if it is on the same SQL instance you specified for the ContentDistribution database.

1.5.6.1 Steps for side-by-side upgrade of ActiveEfficiency

1. Review your requirements to determine which features you need of 1E Client and Tachyon Platform, please refer to Planning for Tachyon Platform pages
2. Upgrade your server hardware as required- please refer to Server sizing requirements
3. Run Tachyon Setup on the existing SLA Platform or Tachyon server to upgrade it to Tachyon Platform - please refer to Tachyon Setup
4. Run Tachyon Setup on remote Tachyon Response Stack servers (if used) - please refer to Tachyon Setup
5. Verify existing clients (if upgrading SLA Platform or Tachyon)
6. Run Tachyon Setup on remote Tachyon DMZ Server (if used) - please refer to Implementing a Tachyon DMZ Server
7. Verify existing Internet based clients (if upgrading Tachyon)
8. Deploy new 1E Client to some test devices (with Tachyon and Nomad client enabled)
9. Verify the test devices
10. Upgrade Nomad Admin Tools and server components - please refer to Upgrading Nomad

a. Upgrade Nomad Admin Tools and server components

b. Update OS Deployment Task Sequence actions to use the Tachyon Platform

c. Manually migrate data from ActiveEfficiency Server

d. Configure Nomad Sites.

11. Deploy new 1E Client to remaining devices

12. When all Nomad clients have been upgraded, then you can decommission the old ActiveEfficiency Server (unless you need to retain it for Shopping).

1.5.6.2 Manually migrate data

Use the following migration scripts to manually migrate sites, pre-cache jobs, and paused collections, from ActiveEfficiency, so they can be managed by upgraded installations of the Nomad Configuration Manager Console Extensions. After migration, you can review these in the Nomad app.

Locations, Single-site data, and content registrations are not migrated, but are copied to legacy database tables for reference only. This data is not shared with new clients, so that legacy and new clients function independently. New clients will re-register their content automatically up to 24 hours later, or can be forced by using the NomadBranch command-line parameter **-cdssync** as described in NomadBranch.exe command-line switches. Old and new clients will perform master elections and peer-share content if they are the same subnet, but they will only use SSD with their own set of clients.

You will maintain Nomad Sites (previously known as Locations) using the one of the new versions of the example PowerShell scripts provided with the Nomad Admin Tools. Alternatively, you can use the examples to modify your existing script to use Content Distribution instead of ActiveEfficiency.

You may continue to maintain Locations in ActiveEfficiency as before, to continue supporting old clients.

Click here to download - AE-CD Data Migration Scripts.zip

Note

1. **ExportData.ps1** - run on any computer that has read access to the ActiveEfficiency database
2. **CreateTables.sql** - run on the SQL Server instance that hosts the ContentDistribution database created by Tachyon Setup
3. **ImportData.ps1** - run on any computer that has write access to the ContentDistribution database.

1.5.6.2.1 Prerequisites

- The ability to run PowerShell scripts and SQL script
- A SQL Login on each SQL Server instance for the user running the scripts
- db_datareader rights on the ActiveEfficiency database
- db_datawriter rights on the ContentDistribution database

Before running the scripts you will need to prevent clients, administrators, and scheduled jobs from updating ActiveEfficiency and Nomad.

1. Stop IIS on the Tachyon Master Stack server (where Content Distribution is installed)
    a. Open command prompt in administrator mode and run **iisreset /stop**
2. Stop IIS on the server where ActiveEfficiency Server is installed
    a. Open command prompt in administrator mode and run **iisreset /stop**
3. Temporarily disable any Task Scheduler jobs related to ActiveEfficiency
    a. From the Start screen, start typing Task Scheduler then click on **Task Scheduler** in the search results
    b. Expand **Task Scheduler Library** → **ActiveEfficiency**
    c. Right-click on each job and select **Disable**
4. If you have any custom jobs to run import scripts for **Sites and Subnets** then also disable these temporarily.

1.5.6.2.2 Create Tables

Open SQL Management Studio and connect to ContentDistribution database. Execute SQL script **CreateTables.sql**. This will create all the required legacy tables in the ContentDistribution database.

> **Note**
>
> This script only needs to be executed once.

1.5.6.2.3 Export Data

Run the **ExportData.ps1** script in a PowerShell admin command prompt using a command line similar to below.

```
.\ExportData.ps1 -AEServerName "AEServer" -AEDBName "ActiveEfficiency" -CDServe
rName "CDServer" -CDDBName "ContentDistribution" -folderPath "C:\migration" -lo
gsPath "C:\migration\logs"
```

This command will create a series of CSV files that we will later import into the ContentDistribution database.

1.5.6.2.4 Import Data

Run the **ImportData.ps1** script in a PowerShell admin command prompt using a command line similar to below.

```
.\importData.ps1 -CDServerName "CDServer" -CDDBName "ContentDistribution" -fold
erPath "C:\migration" -logsPath "C:\migration\logs"
```

This command will populate the tables from the CSV files exported earlier.

1.5.6.2.5 Restart IIS

1. Restart IIS on the ActiveEfficiency Server and Tachyon Master Stack server (where Content Distribution is installed)

    a. Open command prompt in administrator mode and run **iisreset /start**

2. Enable the Task Scheduler jobs again on the ActievEfficiency Server

1.5.6.2.6 Script parameters

Parameter	Description
AEServerName	Name of the SQL Server hosting ActiveEfficiency database. If the server is not running on the default instance, enter the server name and instance name separated by backslash, for example **DBServer\DB**
AEDBName	Name of the ActiveEfficiency database.
CDServerName	Name of the server hosting ContentDistribution database. If the sever is not running on the default instance, enter the server name and instance name separated by backslash, for example **DBServer\DB**
CDDBName	Name of the ContentDistribution database.
folderPath	Folder location to save CSV files. If the path doesn't exist, it will be created by the script.
logsPath	Folder location to save log files. If the path doesn't exist, it will be created by the script.

1.5.7 In-place upgrade of ActiveEfficiency Server for Shopping

This scenario is for upgrading a server that has ActiveEfficiency Server installed and used by 1E Shopping versions prior to Shopping 6.1. If ActiveEfficiency is also being used for Nomad then please also read In-place upgrade of ActiveEfficiency Server for Nomad.

If your installation of ActiveEfficiency is being used by 1E Shopping, then before you replace ActiveEfficiency with Content Distribution, you will need to do ***one*** of the following:

- upgrade to Shopping 6.1 - this version does not use ActiveEfficiency
- reconfigure your existing Shopping 6.0 server to synchronize directly with Configuration Manager - this method of synchronization is provided out-of-the-box in Shopping 6.1 onwards - to do this, please refer to the steps below
- install another instance of ActiveEfficiency Server and Scout, and reconfigure your existing Shopping server to use that - this process is not described here

Shopping is not a Tachyon Platform application, and has no direct dependency on it, therefore it is not affected by Tachyon Setup, other than ActiveEfficiency being removed. Whilst Shopping has no direct dependency on Tachyon Platform, it can optionally integrate with Introducing Application Migration which is a Tachyon application. The Shopping/WSA client is a module of the 1E Client. If this is interesting to you please refer to Shopping - Integrating with Application Migration.

1.5.7.1 Reconfigure Shopping to synchronize directly with Configuration Manager

The process is for Shopping 6.0 only.

Execute the following SQL script on the Shopping database, then restart the Shopping Central service. A few minutes later, the Central service will perform its usual synchronization processes with AD, and also synchronize with CM. You can monitor this process in
C:\ProgramData\1E\ShoppingCentral\ShoppingCentral.log

The script changes preference settings for Shopping 6.0 - Shopping Admin Console settings: Central Service as shown in the table opposite. It changes the description of the sync interval, it does not change its value, which is 1 day by default. If you change the value later it should be set to longer than the time it takes to complete all the syncs. You should not need to change the value of the sync interval because the SCCM sync should be approximately the same as your current ActiveEfficiency Scout sync.

Click here to download - ReplaceActiveEfficiencySyncWithConfigMgrSync.sql

Note

Click **Read more...** to view source for ReplaceActiveEfficiencySyncWithConfigMgrSync.sql

```
-- Disclaimer:
-- Your use of this script is at your sole risk. This script is provided "as-is
", without any warranty,
-- whether express or implied, of accuracy, completeness, fitness for a particu
lar purpose, title or
-- non-infringement, and is not supported or guaranteed by 1E. 1E shall not be
liable for any damages
-- you may sustain by using this script, whether direct, indirect, special, inc
idental or consequential,
-- even if it has been advised of the possibility of such damages.

UPDATE dbo.tb_Preference
SET
Description = 'Sets the interval for synchronizing the members in Computer Cate
gory groups held in the Shopping database with Active
Directory. Also used for the ConfigMgr, Intune Machine sync and the ConfigMgr,
Intune user sync. The value for the interval uses the units defined in the
Active Directory Sync Units parameter.'
WHERE
preferencename = 'Users and Machines, AD Sync Interval'
GO

UPDATE dbo.tb_Preference
```

```
SET
Description = 'The unit is used by the AD, ConfigMgr, Intune Machine and User S
ync Interval setting. This may be set to one of the
following values: Days, Hours or Minutes.'
WHERE
preferencename = 'Users and Machines, AD Sync Units'
GO

UPDATE dbo.tb_Preference
SET
PreferenceValue = 'False'
WHERE
preferencename = 'Sync Machines and Users From Active
Efficiency'
GO

UPDATE dbo.tb_Preference
SET
Hidden = 1
WHERE
preferencename = 'Sync Machines From Old Sccm'
GO

UPDATE dbo.tb_Preference
SET
Hidden = 1
WHERE
preferencename = 'ActiveEfficiency ServerName'
GO
```

Preference name	Change made by the SQL script
Users and Machines, AD Sync Interval	Change description
Users and Machines, AD Sync Units	Change description
Sync Machines and Users From Active Efficiency	Set to 'False' (enables sync from SCCM instead)
Sync Machines From Old Sccm	Hide as no longer required
ActiveEfficiency ServerName	Hide as no longer required

1.5.8 Upgrading 1E Client

Guidance for upgrading Tachyon and other legacy 1E agents to 1E Client. This page contains detailed steps for upgrading Tachyon Agent and a summary of considerations for upgrading other

legacy agents. The 1E Client contains clients for 1E products and solutions, and their upgrade documentation should be consulted before upgrading their clients and agents.

When upgrading a 1E product or solution, you should upgrade its server infrastructure first. For more information, please refer to the following:

- Upgrading Nomad - from 7.1 onwards you will be replacing ActiveEfficiency Server with Tachyon Platform, which includes Content Distribution
- Upgrading PXE Everywhere
- NightWatchman Enterprise - Upgrading NightWatchman Enterprise
- Shopping - Upgrading to Shopping
- Upgrading Tachyon Platform.

Note

Upgrading from earlier versions of 1E Client to 8.1 simply requires deploying the new version, using the same or different configuration settings.

Please refer to:

- Deploying 1E Client on Windows
- Deploying 1E Client on macOS
- Deploying 1E Client on Linux
- Deploying 1E Client on Solaris

If you are upgrading any legacy 1E agents then please read sections below.

Please refer to Reconfiguring 1E Client for how to reconfigure the 1E Client after it has been deployed.

1.5.9 Role name changes

Role names were changed in Tachyon Platform 8.0. You will notice these changes if you are upgrading from version 5.2 or earlier.

For a full list of role names, please refer to:

- Roles and Securables reference page, which contains a copy of the notes below, details about renamed roles, and roles that are recommended to replace the ones that have been retired
- Roles page, which contains guidance on how to configure custom roles.

The upgrade process makes the following changes:

1. New roles are created, if they do not exist already:

   New system roles

   – Group Administrator

- Guaranteed State Policy Assigner
- Installer
- Tachyon System

New Custom roles

- Experience Administrator
- Experience Engagement Assigner
- Patch Success Administrator

2. The Tachyon user doing the upgrade is automatically assigned to the **Installer** role. The user is also *unassigned* from the following roles, if assigned before the upgrade:
   - Applications Administrators
   - Consumer Administrators
   - Event Subscription Administrators
   - Instruction Set Administrators
   - Permissions Administrators
3. Tachyon users associated with the NT AUTHORITY/NETWORK SERVICE and machine accounts, are assigned to the **Tachyon System** role. These users will also be *unassigned* from the following roles, if assigned before the upgrade:
   - Applications Administrators
   - Consumer Viewers
   - Engagement Administrator
   - Management Group Sync Initiators
   - Offloaders
   - Permissions Viewers
   - Survey Administrators
4. Several old roles are renamed
   a. Some are renamed from plural to singular, for example if the **Nomad Administrators**role exists it is renamed to**Nomad Administrator**
   b. An exception is in the unlikely event that the **Nomad Admins** role exists, it is renamed to **Nomad Administrator** unless that role already exists, in which case it is renamed to **Nomad Administrators** instead

c. **Global Questioner**, **Global Actioner**, **Global Viewer**, and **Global Approver** roles have been renamed with **Global...** replaced by **All instructions...**

d. **Inventory Viewers**, **Experience Viewers**, **Patch Success Viewers**, have been renamed with **...Viewers** changed to **...User**

System roles renamed from

- Global Actioners
- Global Administrators
- Global Approvers
- Global Questioners
- Global Viewers
- Guaranteed State Administrators
- Guaranteed State Viewers
- Inventory Administrators
- Inventory Viewers
- Survey Administrators
- Survey Viewers

System roles renamed to

- All Instructions Actioner
- Full Administrator
- All Instructions Approver
- All Instructions Questioner
- All Instructions Viewer
- Guaranteed State Administrator
- Guaranteed State User
- Inventory Administrator
- Inventory User
- Experience Engagement Administrator *
- Experience Engagement Viewer *

Note

* These roles are retired, and will only be kept if a user or group is assigned to it.

Custom roles renamed from

- AppClarity Administrators
- Application Migration Administrators
- Compliance Administrators

Custom roles renamed to

- AppClarity Administrator
- Application Migration Administrator
- Compliance Administrator
- Compliance Viewer
- Entitlement Administrator

- Compliance Viewers
- Entitlement Administrators
- Experience Viewers
- Nomad Administrators
- Patch Success Viewers
- Reclaim Administrators
- Reclaim Viewers
- Experience Viewer
- Nomad Administrator
- Patch Success User
- Reclaim Administrator
- Reclaim Viewer

5. Other system and custom roles are deleted. A role is kept only if it is **(a)** on the list of roles to be kept, or **(b)** the role has a user or group assigned to it

System roles that are kept

- All Instructions Actioner
- All Instructions Approver
- All Instructions Questioner
- All Instructions Viewer
- Full Administrator
- Group Administrator
- Guaranteed State Administrator
- Guaranteed State Policy Assigner
- Guaranteed State User
- Installer
- Inventory Administrator
- Inventory User

System roles that have been retired

- 1E Client Deployment Administrators
- 1E Client Installer Administrators
- Applications Administrators
- Component Administrators
- Connector Administrators
- Consumer Administrators
- Consumer Viewers
- Custom Properties Administrators
- Event Subscription Administrators
- Event Subscription Viewers
- Infrastructure Administrators
- Instruction Set Administrators
- Log Viewers
- Management Group Administrators

- Tachyon System

Custom roles that are kept

- 1E ITSM Connect Actioner
- AppClarity Administrator
- Application Migration Administrator
- Compliance Administrator
- Compliance Viewer
- Entitlement Administrator
- Experience Administrator
- Experience Engagement Assigner
- Experience User
- Nomad Administrator
- Patch Success Administrator
- Patch Success User
- Reclaim Administrator
- Reclaim Viewer
- Management Group Sync Initiators
- Offloaders
- Permissions Administrators
- Permissions Viewers
- Policy Administrators
- Provider Configuration Administrators
- Schedule Administrators
- Survey Administrators (Experience Engagement Administrator)
- Survey Viewers (Experience Engagement Viewer)
- VDI Administrators

Custom roles that have been retired

- Any custom role created by Tachyon administrators

Tip

A retired role is kept if it has a user or group assigned to it.

Role names

Tachyon Platform 5.2 onwards no longer allows the use of dots in role names, for example Questioners.Core, and roles will no longer work after an upgrade. Therefore, please review your custom role names before upgrading.

1.6 Using consumer applications

All consumer applications can be accessed from the Tachyon portal using the following URL, and then clicking the application icon.

https://<platform DNS Name FQDN>/Tachyon

where <platform DNS Name FQDN> is the FQDN of your platform server, set up during the preparation phase, as described under the heading DNS Names.

1.6.1 Included applications

The following are applications built-into the platform:

Inventory	*https://<platform DNS Name FQDN>/Tachyon/App/#/inventory/*
Settings	*https://<platform DNS Name FQDN>/Tachyon/App/#/platform/*

1.6.2 Optional applications that require a license

AppClarity	*https://<platform DNS Name FQDN>/Tachyon/App/#/appclarity/*
Application Migration	*https://<platform DNS Name FQDN>/Tachyon/App/#/applicationmigration/*
Guaranteed State	*https://<platform DNS Name FQDN>/Tachyon/App/#/guaranteedstate/*
Content Distribution	*https://<platform DNS Name FQDN>/Tachyon/App/#/nomad/*
Patch Success	*https://<platform DNS Name FQDN>/Tachyon/App/#/patchsuccess/*
Experience	*https://<platform DNS Name FQDN>/Tachyon/App/#/experience/*
Explorer	*https://<platform DNS Name FQDN>/Tachyon/App/#/explorer/*
Dashboards	*n/a*

1.7 Using Settings

How to use the **Settings** application to configure your platform and application settings.

1.7.1 Settings features

The Settings application lets you configure the Tachyon system and application settings. For more information please refer to the Using Settings section of this documentation.

1.7.1.1 Settings features

1.7.1.1.1 Instructions, Product Packs, Instruction sets, and permissions

Tachyon lets you investigate your network using questions and actions, which are collectively known as Instructions.

You can load Instructions into Tachyon, either individually or with a Product Pack, which is essentially a zip file containing one or more Instructions. Tachyon comes with a range of pre-framed questions and actions in the form of Product Packs, providing extensive out-of-the-box capabilities that can be extended as new and updated Product Packs are made available.

Tachyon permissions for the Instructions are handled using Instruction sets. You create Instruction sets, then define roles that specify particular permissions on those sets, and then assign the roles to users. Each Instruction is only allowed to reside in one Instruction Set, which associates it with a role and thereby the users that have that role and can run the Instruction. The roles have associated Management groups that determine the devices that users with the role have access.

When Instructions are loaded into Tachyon they are placed in the default **Unassigned** Instruction Set, so you must move them into previously created Instruction sets before they can be run.

For more information on uploading product packs into Tachyon and managing Instruction sets, please refer to Instruction sets page.

1.7.1.1.2 Server software

Category	Product	Notes
Server OS	• Windows Server 2022 • Windows Server 2019 • Windows Server 2016	For more detail about configuration of servers, please refer to Windows Server requirements. Only 64-bit server OS are supported. The server must be domain-joined. This version of Tachyon requires the server OS to be **English** because of a Known issues with certain regional settings. If TLS 1.0 is disabled, then please ensure you follow the steps in If TLS1.0 is disabled to add registry entries, for the 1E Catalog Update Service to successfully connect to the 1E Cloud Catalog. **Note** This list shows only those OS versions in

Category	Product	Notes
		mainstream support by Microsoft, and therefore supported by Tachyon, and by 1E Client 8.1. Please refer to Constraints of Legacy OS regarding the end of mainstream support. For Microsoft product lifecycle details, please refer to https://support.microsoft.com/en-us/lifecycle/search. Refer to Support for Microsoft Rapid-Release Cycle on https://support.1e.com/ for details of which Current Branch versions are supported by 1E products, and known issues regarding specific versions.
SQL Server and SQL Server Analysis Services (SSAS)	• SQL Server 2019 • SQL Server 2017 • SQL Server 2016 SP3	For more detail, please refer to SQL Server requirements. Standard and Enterprise editions of these versions of SQL Server and SQL Server Analysis Services (SSAS) are supported. SQL Server 2016 RTM is not supported due to some issues, which are resolved by SP3. **Note** Tachyon only supports AlwaysOn Availability Groups on **SQL Server Enterprise Edition**. Please refer to High

Category	Product	Notes
		Availability options for SQL Server for HA options and their requirements. **Note** If you intend to integrate with third-party business intelligence products such as Power BI, you must install the **Enterprise edition of SSAS** as per their requirements. A SQL Server database instance is required for the following databases: • **1ECatalog** • **ContentDistribution** (optional - required for Nomad) • **SLA-BI** (optional - required for Patch Success) • **SLA-Data** • **SLA-Integrate** • **SLA-Shared** • **TachyonExperience** (optional - required for Tachyon Experience) • **TachyonMaster** • **TachyonResponses** **SLA Inventory databases** Tachyon Setup can install the above databases on separate SQL Server instances, however SLA-Data, SLA-Integrate, and

Category	Product	Notes
		SLA-Shared must exist on the same instance. A SQL Server Analysis Services (SSAS) instance installed in **Multidimensional** mode is required for SLA Business Intelligence. **SLA Business Intelligence** SLA Business Intelligence (BI) is only required for the Patch Success application. Together, the SLA Platform and BI installers create the following: • A database called **SLA-BI** on the SQL Server database instance. • A MOLAP cube called **SLA-BI** on the SSAS instance. • A linked server for the SLA databases to get data from the SLA-BI database and then from the SLA-BI cube. • A linked server for the SLA-BI database to get data from the SLA databases. • A datasource definition used by the SLA-BI cube to connect to the BI database. If the SLA databases, BI database, or SSAS instance for BI, are on *different* SQL Servers then the BI installer enforces

Category	Product	Notes
		the use of a SQL login on each instance. If they are on the *same* SQL Server then the installer gives you a choice of using integrated security (domain user account) or a SQL login. However, if you are installing all the components using Tachyon Setup instead of their individual installers, then you are not given the choice. Tachyon Setup always uses integrated security. Contact your 1E Account Team if your scenario requires the above-mentioned databases to be on *different* SQL Servers. This affects different servers, not different instances. All SQL Server instances *must* be configured with the following: • A case-insensitive, accent-sensitive collation which is **SQL_Latin1_General_CP1_CI_AS** by default, • **Allow remote connections to this server** enabled. All SQL Servers should be configured with the **SQL Server Browser service** running in order for the BI installer to select from a list of instances. **SQL Server Management Studio** is required to review the

Category	Product	Notes
		configuration and edit settings in 1E database tables. If installing SQL Server locally, note: • SQL Server 2016 and 2017 require .NET Framework 4.6 or later • SQL Server setup requires PowerShell 2.0. For the latest information about SQL Server prerequisites, please refer to http://go.microsoft.com/fwlink/?LinkId=622999.
Microsoft Endpoint Configuration Manager	• MECM CB 2303 • MECM CB 2211 • MECM CB 2207 • MECM CB 2203 • MECM CB 2111 • MECM CB 2107	Tachyon uses Configuration Manager for the following optional apps and features: • Reclaiming a product using SCCM Uninstall • Introducing Application Migration • Introducing Inventory captures data using the System Center Configuration Manager connector • Tachyon extensions for the Configuration Manager Console. - installed on Configuration Manager consoles using the 1E Tachyon Toolkit installer • Introducing Nomad requires 1E Client with Nomad client features enabled.

Category	Product	Notes
		Nomad provides the following Content Distribution features for Configuration Manager: • Nomad app overview provides visibility of content distribution activity • Single Site Download (SSD) (SSD). • Task sequence actions to augment OS Deployment: – Peer Backup Assistant - PBA – High Availability PBA (HAPBA) – Get Migration Settings to manage computer associations. • Nomad Pre-caching • Nomad Download Pause. Nomad requires the Content Distribution web service to synchronize with the Configuration Manager database. For standalone primary site environments, permissions are automatically assigned to the service account of Content Distribution's web application pool service (by default Network Service) using the **ConfigMgr_DViewAccess** localgroup native to Configuration Manager. For a CAS, this group is not created natively therefore additional steps are required to allow access. Please refer to Preparation: Microsoft

Category	Product	Notes
		Endpoint Configuration Manager preparation.
Web Server	• IIS 10	See Windows Server roles and features for details about required Web Server roles and features.
Runtime libraries	• Visual C++ 2013 Redistributable • Visual C++ 2015-2019 Redistributable • ASP.NET Core Framework 3.1 • .NET Framework 4.8	See Windows Server roles and features for details about required .NET Framework roles and features. To know supported combinations of OS and .NET Framework, please refer to: https://docs.microsoft.com/en-us/dotnet/framework/migration-guide/versions-and-dependencies. • Windows Server 2022 has .NET Framework 4.8 installed by default. • Windows Server 2019 has .NET Framework 4.7.2 installed by default. • Windows Server 2016 has .NET Framework 4.6.2 installed by default. **ASP.NET Core Hosting Bundle** is required only for the Nomad. It is not included with the Operating System, and must be downloaded and installed separately. If it not already installed, Tachyon Setup will attempt to automatically download version **3.1.11** and install it. Alternatively you can download it, or a later version, and install it yourself. For more detail please refer to ASP.NET Core Hosting Bundle. Installers include and automatically installs the redistributable packages

Category	Product	Notes
		for **Visual C++ 2013** and **Visual C++ 2015-2019**. The Coordinator (licensing module on the Master Stack), and Switch (on Response Stack) are written in C++ using Visual Studio 2013 and 2019, therefore require the **runtime (x64)** versions of these packages. Other server components use .NET Framework. **SQL BCP** is required by the **Export All** feature described in Exporting data from Explorer, and must be installed on each Tachyon Response Stack server (specifically the servers which have the Tachyon Core installed). BCP uses ODBC, which requires **Microsoft ODBC Driver versions 13.1 and 17** and **Visual C++ 2017 Redistributable** to be installed first. Please refer toP SQL BCP for more detail.
Other software	• PowerShell	PowerShell is required by Tachyon installer during installation.
Browsers	Latest version of: • Google Chrome • Microsoft Edge (Chromium) • Mozilla Firefox	A browser is not a prerequisite for installation of Tachyon servers but is required to use and administer the Tachyon platform. The administration is performed via the Tachyon portal and can be on a remote computer. These browsers are supported on all OS platforms which the browser vendor supports. The Portal and any API should be added as a trusted site. This is especially important when running

Category	Product	Notes
		scripts that may produce unexpected errors. Please review Known Issues Using Tachyon. **Note** **Microsoft legacy browsers** Support has been withdrawn for **Internet Explorer 11** and **legacy Microsoft Edge** (non-Chromium version) because Microsoft no longer supported them since 2021. We recommend you use Google Chrome, Firefox, or Microsoft Edge Chromium browser.

1.7.1.1.3 Connectors

Connectors are used to connect to other 1E and third party systems and populate repositories. When more than one connector to different data sources is used, the information from those different data sources is de-duplicated and normalized into a single cohesive view that is then stored in a repository. In this way, you can use the data from different sources to augment each other and build a better picture of "what's out there?".

For example, you can sync inventory data from Configuration Manager into an inventory repository, which will fetch information about your Windows devices. You could then augment that with inventory data synced from Tachyon which could include information about non-Windows devices where the client has been installed.

Note

For more information on connectors, please refer to:

- Connectors page

The following connectors are supported:

- BigFix connector — Connects to a BigFix Inventory database server.
- BigFixInv connector — Connects to a BigFix Inventory database.
- File Upload connector — Uploads inventory data from a folder containing tab (TSV) and comma (CSV) separated value file(s).

- Intune connector — Connects to an Intune application and collects inventory and usage data.
- Microsoft Office 365 connector — Connects to an Office 365 application in InTune and pulls in inventory and usage data.
- OpenLM connector — Connects to an OpenLM database server.
- Oracle LMS connector — Connects to Oracle LMS and queries it for inventory information.
- ServiceNow connector — Connects to a ServiceNow instance to import basic inventory data into SLA Platform.
- System Center Configuration Manager connector — Connects to a Configuration Manager database and pulls in inventory and usage data.
- Tachyon connector — Connects the Tachyon and SLA components to support the Management group and Tachyon Powered Inventory features. The Tachyon Powered Inventory feature uses instructions to fetch inventory data from clients, and is a prerequisite for Patch Success.
- vCenter connector — Connects to a vCenter server and pulls in inventory data.
- Windows Server Update Services connector — Connects to a WSUS database and pulls in patch data.

1.7.1.1.4 Repositories

Repositories are used by applications to process and store information. For example, the Patch Success application uses both an inventory and a BI repository to process the information needed to report on how successful patching is in your enterprise. Normally a connector is used to connect a data source to an appropriate repository.

Tip

Repositories are also useful when you want to segregate different types of data. For example, you could have one inventory repository for Configuration Manager inventory data, and another one for BigFix data. Alternatively, you can have connectors to different inventory sources pushing data into one repository. Any Management Groups that you create will span all the repositories you have.

Note

For more information on managing repositories, please refer to:

- Repositories page.

1.7.1.1.5 Device Tags

Device Tags are generally associated with Explorer and can be used when setting coverage to target Instructions to particular devices, but they can also be used to define Management Groups optionally used by all applications.

Device Tags must be defined by a **Full Administrator** before they can be used to tag devices or used to set the coverage of Instructions.

This is done from the **Settings**→**Configuration**→**Custom properties**→ **Device Tags** page, which can be viewed by users with the **Full Administrator** role.

Note

For more information on managing and using Device Tags, please refer to:

- Device Tags page
- Adding properties - tutorial
- Actions to set tags - tutorial
- Using tags to set the coverage for a question - tutorial.

1.7.1.1.6 Software Tags

Using Software Tags allows you to create custom labels and associate them with the software titles you have deployed in your estate.

You can do this from the **Settings**→**Configuration**→**Custom properties**→**Software Tags** page, which can be viewed by users with the **Full Administrator** role.

Using Software Tags allows you to create custom labels and associate them with the software titles you have deployed in your estate. An administrator with either the **Full Administrator** or **Group Administrator** role can set Software Tags in their environment, they can also create Management Groups based on the tag name and value. For details about configuring Tachyon users, Roles, and Management Groups refer to the Permissions Menu pages.

In short, you can work with Software tags by:

1. Creating your Software Tag.
2. Associating the new tag with a software title.
3. Creating a Management Group based on the Software Tag name and Tag value rules (This step can be run anytime before evaluation).
4. Evaluating the new Management Group by running a Basic Inventory Consolidation.

If an administrator adds or modifies Software Tags or associations, they will have to run the Management Group evaluation report again to see the updated devices reflected in Inventory.

1.7.1.1.7 Schedules

Schedules can be created to execute specific operations on repositories in Tachyon so that they are kept up to date with their data sources and processing. These operations include:

- Syncing data sources to repositories using connectors
- Processing the BI data cube.

Repository schedules are different from Instruction schedules that can be set in Explorer.

Note

For more information on setting schedules, please refer to:

- Schedules page.

1.7.1.1.8 Consumers, Applications, Components, and Providers

There are pages in the Settings application for each of these. They are described in the following table:

Configuration objects	Description
Consumers	These can access Tachyon using the Tachyon Consumer API. To enhance the security of the Tachyon system, only consumers that have been registered on the **Settings→Configuration→Consumers** page will be allowed to access Tachyon.
Applications	Features of Tachyon that is hosted in the Tachyon portal. Applications are generally Consumers as they need to interact with Tachyon using the Tachyon API. These are available on the **Switch App** menu.
Components	These form part of SLA and cannot be changed or altered by a user. These can be viewed using the **Settings→Configuration→Components** page.
Providers	These are components that can be configured to provide a particular operation in SLA. These can be viewed and configured using the **Settings→Configuration→Provider configuration** page.

Note

For more information on Consumers, Components, and Providers, please refer to:

- Consumers page
- Components page
- Provider configuration page.

1.7.1.1.9 Information pages

Information on your Tachyon license is available, as well as the ability to, reactivate it following an update.

You can view information on the Tachyon system information for the Consumer, Coordinator, Background channel, Core and Switch.

Note

For more information please refer to:

- License information page

- System information page.

1.7.1.1.10 Monitoring log files

The monitoring pages let you view how Tachyon is performing its tasks. Four key log pages are provided:

Page	Description
Process log	Whenever you execute a sync or process a repository the steps are displayed here. This page is updated in real-time and shows the status of each step as it happens.
Sync log	The results of performing a sync are displayed here.
Infrastructure log	Information on the Tachyon infrastructure is displayed here, such as license status and instruction workflow.
Audit information log	This page displays information on the Instructions that have been run in Explorer. This includes the instruction text and the user that requested it.

Note

For more information on monitoring please refer to:

- Process log page
- Sync log page
- Infrastructure log page
- Audit information log page.

1.7.1.1.11 Defining users and roles

Tachyon users or groups can be added from AD. They can be assigned roles that determine what aspects of Tachyon they can access. Custom roles can be created that let you associate particular permissions on particular Instruction sets for particular management groups.

Note

For more information on users and roles please refer to:

- Users and Groups page
- Roles page
- Configuring Access Rights - tutorial.

1.7.1.1.12 Management groups

Management groups use inventory-based rules to define groups of particular devices, they are implemented in SLA and then made available to Tachyon applications and other consumers. After

a management group is defined, each time the inventory is updated the device membership of the groups is re-evaluated by applying the management group's rules to the new inventory.

Custom roles can be created that tie particular Instruction sets to particular management groups. This means you can not only set the permissions for users to access the Instructions in specific Instructions sets, but you can also determine which devices they can target using those Instructions.

Once defined, management groups can then be used to set the coverage for Instructions in Explorer and also which devices can be targeted by particular users. Management groups are also used by the Patch Success and Guaranteed State applications to determine which devices are being targeted.

Note

For more information on management groups, please refer to:

- Management Groups page
- Management Groups - tutorial.

1.7.1.1.13 Uploading Instructions into Tachyon and creating Instruction sets

You determine the capabilities of Explorer by uploading Instructions from product packs into Tachyon. Product Packs are either provided with the release or downloaded from the 1E Exchange. Once the Instructions have been uploaded into Tachyon you then need to put them into Instruction sets. The Instruction sets can then be associated with custom roles to determine the permissions applied to the Instructions. The custom roles are then applied to users to determine which Instructions each user has access to.

Note

For more information on uploading product packs into Tachyon and managing Instruction sets, please refer to:

- Instruction sets page.

1.7.2 Configuration Menu

General configuration options for Tachyon.

1.7.2.1 Connectors page

Connectors are used to connect to other 1E and third party systems, retrieve their data and populate repositories. Tachyonprovides the following inventory connectors to populate the Tachyon Repositories page:

- BigFix connector — Connects to a BigFix Inventory database server.
- BigFixInv connector — Connects to a BigFix Inventory database.
- File Upload connector — Uploads inventory data from a folder containing tab (TSV) and comma (CSV) separated value file(s).
- Intune connector — Connects to an Intune application and collects inventory and usage data.

- Microsoft Office 365 connector — Connects to an Office 365 application in InTune and pulls in inventory and usage data.
- OpenLM connector — Connects to an OpenLM database server.
- Oracle LMS connector — Connects to Oracle LMS and queries it for inventory information.
- ServiceNow connector — Connects to a ServiceNow instance to import basic inventory data into SLA Platform.
- System Center Configuration Manager connector — Connects to a Configuration Manager database and pulls in inventory and usage data.
- Tachyon connector — Connects the Tachyon and SLA components to support Management group and Tachyon Powered Inventory features. The Tachyon Powered Inventory feature uses instructions to fetch inventory data from clients, and is a prerequisite for 1E Patch Success.
- vCenter connector — Connects to a vCenter server and pulls in inventory data.
- Windows Server Update Services connector — Connects to a WSUS database and pulls in patch data.

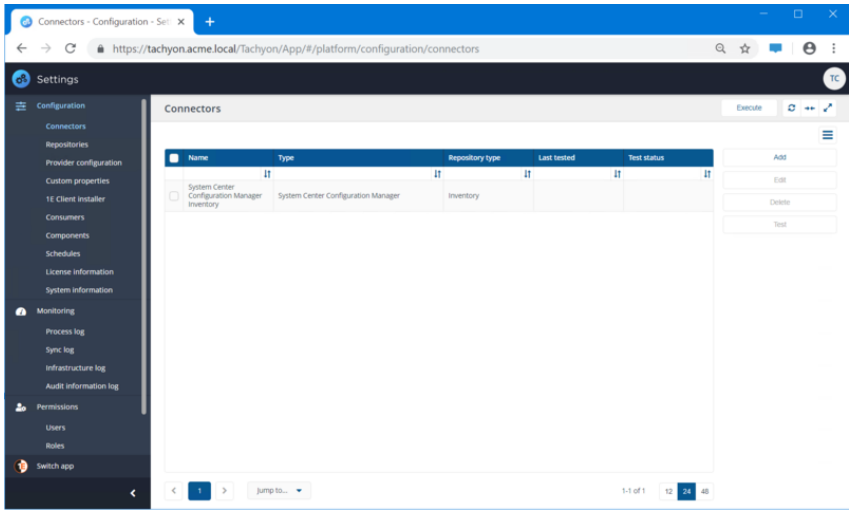
Use the links above to find more information about each type of connector. Please refer to Introducing Inventory for more information about viewing and exporting inventory repositories.

Additional connectors may exist for add-on Consumer applications that have been installed. For example, AppClarity has the following connectors to populate its entitlement repository:

- AppClarity v5.2 connector — Exports entitlements from an AppClarity 5.2 database into a TSV file, which can then be reviewed and imported into .
- Entitlement .tsv connector — Uploads entitlements from a folder containing one or more tab or comma separated value file(s).

Note

Consumer applications may add additional connectors to populate their repositories.



Please refer to Third party data sources below for supported versions of software used by these connectors, and other prerequisites.

1.7.2.1.1 Add a new connector

1. Navigate to **Settings→Configuration→Connectors**.
2. Click the **Add** button.
3. In the **Add Connector** popup select the required **Connector type** from the list of connector types.
4. Once you've made a selection the **Add connector** popup will show fields appropriate to the selected **Connector type**.
5. Enter the relevant connector configuration details including **Connector name**.

   Tip

   You should use a naming convention for connector names:

   <connector type> <scope> <RCR>

   Scope describes where data is coming from or what it's being used for. For example Demo, Test, Lab, Q2 Audit.

   Include **RCR** in the name if you have enabled **Run Consolidation Reports**.

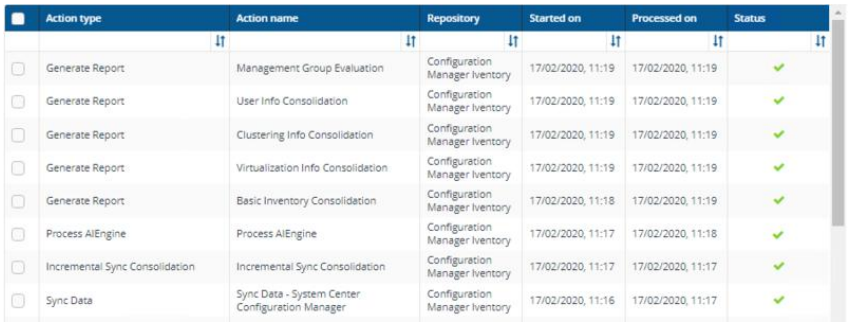
   For more information about what details are required, please refer to the corresponding documentation page for the connector type you are configuring.
6. When you have entered relevant details, click **Add**.
7. A new connector will be added with the selected details.

Note

Inventory connectors use consolidation actions to consolidate, normalize and store data in Inventory repositories.

Check the **Run Consolidation Reports** checkbox if you want consolidation actions to be processed each time the **Sync Data** action is executed for the connector.

This can lead to unnecessary processing if you enable this on more than one connector. The recommended method of processing consolidation actions is to schedule the action **Generate Report - Basic Inventory Consolidation** to execute after the **Sync Data** actions have run for all connectors. This will execute the remaining consolidation actions. Alternatively check the **Run Consolidation Reports** checkbox on one of your connectors. You can view action processes in **Settings→Process log**.



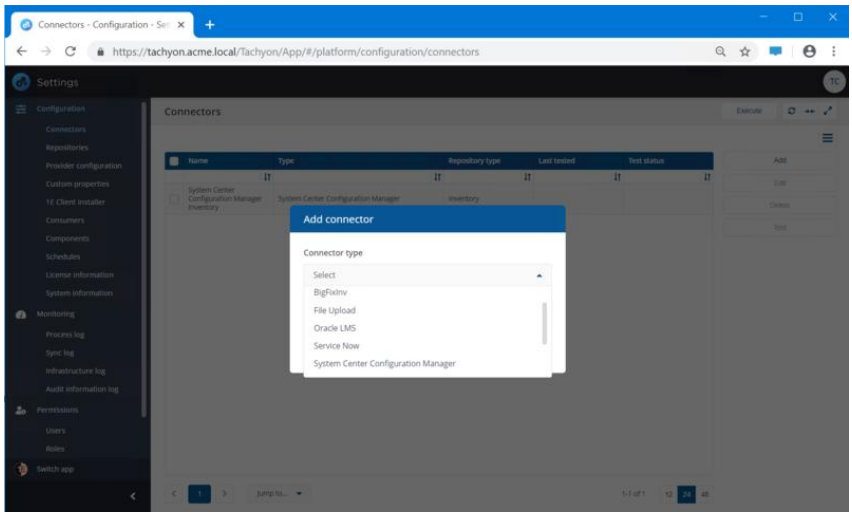
Action type	Action name	Repository	Started on	Processed on	Status
Generate Report	Management Group Evaluation	Configuration Manager Inventory	17/02/2020, 11:19	17/02/2020, 11:19	✓
Generate Report	User Info Consolidation	Configuration Manager Inventory	17/02/2020, 11:19	17/02/2020, 11:19	✓
Generate Report	Clustering Info Consolidation	Configuration Manager Inventory	17/02/2020, 11:19	17/02/2020, 11:19	✓
Generate Report	Virtualization Info Consolidation	Configuration Manager Inventory	17/02/2020, 11:19	17/02/2020, 11:19	✓
Generate Report	Basic Inventory Consolidation	Configuration Manager Inventory	17/02/2020, 11:18	17/02/2020, 11:19	✓
Process AIEngine	Process AIEngine	Configuration Manager Inventory	17/02/2020, 11:17	17/02/2020, 11:18	✓
Incremental Sync Consolidation	Incremental Sync Consolidation	Configuration Manager Inventory	17/02/2020, 11:17	17/02/2020, 11:17	✓
Sync Data	Sync Data - System Center Configuration Manager	Configuration Manager Inventory	17/02/2020, 11:16	17/02/2020, 11:17	✓

Note

When the new connector is saved then a new action is defined in Tachyon. This new action will have a name of the form: **Sync Data - <ConnectorName>**.

In order to sync the data from the connector's data source to a selected repository you will need to either:

1. To execute a manual sync action, please refer to Execute a connector sync action action below.
2. To schedule a sync action, please refer to Schedules page.



The following inventory connectors are provided by Tachyon out-of-the-box.

- BigFix connector — Connects to a BigFix Inventory database server.
- BigFixInv connector — Connects to a BigFix Inventory database.
- File Upload connector — Uploads inventory data from a folder containing tab (TSV) and comma (CSV) separated value file(s).
- Intune connector — Connects to an Intune application and collects inventory and usage data.
- Microsoft Office 365 connector — Connects to an Office 365 application in InTune and pulls in inventory and usage data.
- OpenLM connector — Connects to an OpenLM database server.
- Oracle LMS connector — Connects to Oracle LMS and queries it for inventory information.
- ServiceNow connector — Connects to a ServiceNow instance to import basic inventory data into SLA Platform.
- System Center Configuration Manager connector — Connects to a Configuration Manager database and pulls in inventory and usage data.
- Tachyon connector — Connects the Tachyon and SLA components to support Management group and Tachyon Powered Inventory features. The Tachyon Powered Inventory feature uses instructions to fetch inventory data from Tachyon clients, and is a prerequisite for Patch Success.

- vCenter connector — Connects to a vCenter server and pulls in inventory data.
- Windows Server Update Services connector — Connects to a WSUS database and pulls in patch data.

Additional connectors may exist for add-on Consumer applications that have been installed. For example, AppClarity has the following connectors to populate its entitlement repository:

- AppClarity v5.2 connector — Exports entitlements from an AppClarity 5.2 database into a TSV file, which can then be reviewed and imported into .
- Entitlement .tsv connector — Uploads entitlements from a folder containing one or more tab or comma separated value file(s).

1.7.2.1.2 Delete a connector

To delete a connector:

1. Select the connector you want to delete from the list of **Connectors** bychecking the box at the left-hand end of the connector's row.
2. Click the **Delete** button.
3. In the **Delete connector** popup you will be asked if you want to proceed and delete the selected connector.
4. To delete, click the **Yes, delete connector** button.

1.7.2.1.3 Test a connector

Once a new connector has been added the next step is normally to test that the details you have entered enable you to connect to the specified data source.

1. Select the connector you want to test from the list of **Connectors** by checking the box at the left-hand end of the connector's row.
2. Click the **Test** button.
3. The **Test status** column for the connector will display a clock icon

   indicating that the test has been queued for executing.
4. If the test succeeds **Test status** will display a check icon

   and the **Last tested** column will display the date and time the test succeeded.
5. If the test fails the **Test status** will display a failed icon

   and you'll need to check the details you entered for the connector.

Tip

If you have access to the Process log you can see an entry for the Test action.

1.7.2.1.4 Execute a connector sync action

The **Execute** button allows you to *manually* run an action. To *schedule* an action, please refer to Schedules page.

1. Click the **Execute** button.
2. In the **Execute action** popup subsequently displayed, use the **Repository** menu to select the inventory repository you want to populate.
3. Once the repository has been selected you can then select the action to run. In the case of inventory repositories the actions will be restricted to inventory related actions. For a connector you will be looking for an action with the form **Sync Data - <connector name>**.
4. For inventory syncs (where you sync a connector) you have additional options to check as shown in the example picture opposite:

   Warning

   Clean Sync causes deletion of existing data previously imported by the selected combination of **action** and **repository**. Data imported by any other connector actions is left intact and consolidated with new data. To clear all data from a repository, please refer to Repositories page.

   If **Clean Sync** checkbox is not checked then an incremental sync occurs, consolidating new data with old. An incremental sync is quicker than a clean sync.

   Clean Sync will prevent the Management Groups feature and applications such as Patch Success from working until the sync is complete and new data has been consolidated. This operation should only be performed if you need a clean sync or are experiencing problems with sync times taking too long.

   Note

   Run AI action will cause the AI action to run, this is only available if AI Powered Auto-curation has been enabled. The **Run AI action** checkbox is also available if the selected Action is **Generate Report - Basic Inventory Consolidation**. For detail on how to enable AI Powered Auto-curation the information is on the AI Powered Auto-curation page.

   Note

   Data to Sync allows you to select some or all categories of data supported by the connector.
5. Click the **Execute** button in the **Execute action** popup to start the sync.
6. A popup appears momentarily informing you that the Sync has started and you can monitor progress in the **Process log**.
7. When the sync starts a number of actions are queued to be performed on the selected repository. To check the progress of the sync actions:

a. Navigate to the **Monitoring→Process log** page.

b. Here you can see the sequence of actions that have been queued for the selected repository related to the **Sync Data** action selected.

c. When each action has finished running you'll see a check icon

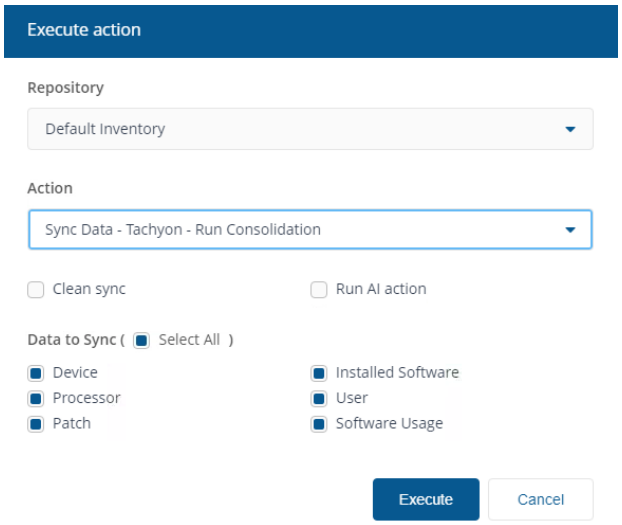
appear in the **Status** column if it succeeds or a failed icon

if it fails.

8. Once all the actions have succeeded you can check the results. To do this:

a. Navigate to the **Monitoring→Sync log** page.

b. This displays the items that have been added to the selected repository as a result of running the sync.



Note

The **Execute** button is also available on the Process log page.

1.7.2.1.5 Third party data sources

The following table shows the supported versions of software used by the Tachyon out-of-box connectors.

Connector	Product	Notes
BigFix	• BigFix	Please refer to the BigFix connector for prerequisites.

Connector	Product	Notes
Intune	• Intune	Please refer to the Intune connector page for prerequisites.
Microsoft Office 365	• Azure	Please refer to the Microsoft Office 365 connector page for prerequisites.
OpenLM	• OpenLM Server version 21.12	Please refer to the OpenLM connector page for prerequisites.
Oracle LMS	• Oracle LMS	Please refer to the Oracle LMS connector page for prerequisites.
ServiceNow	• ServiceNow Jakarta release	Please refer to the ServiceNow connector page for prerequisites.
System Center Configuration Manager (SCCM)	• SCCM CB 2203 • SCCM CB 2111 • SCCM CB	Please refer to the System Center Configuration Manager connector page for prerequisites.

Connector	Product	Notes
	2107 • SCCM CB 2103 • SCCM CB 2010	
Tachyon	• Tachyon 8.1	Please refer to the Tachyon connector page for prerequisites.
vCenter	• VMware PowerCLI 11.1.0	VMware PowerCLI 11.1.0 (code.vmware.com/web/dp/tool/vmware-powercli/11.1.0) must be installed on the Tachyon Master server (where the SLA Integrate Services Agent service is hosted) before you can configure and use the vCenter connector. Earlier or later versions of PowerCLI are not supported and may cause errors. VMware PowerCLI is freeware and was previously known as vSphere PowerCLI. VMware PowerCLI supports multiple versions of VMware vCenter Server. For details, please refer to the VMware compatibility matrix using the following link: https://www.vmware.com/resources/compatibility/sim/interop_matrix.php#interop&2=&106= Please refer to the vCenter connector page for configuration details.
WSUS (Windows Server Update Services)	• WSUS	Please refer to the Windows Server Update Services connector page for configuration details.

1.7.2.1.6 BigFix connector

Connects to a BigFix Inventory database server.

Before adding a new BigFix connector, you will need the following:

- domain user account or SQL Login to connect to the BigFix database
- access rights configured in the BigFix database.

1.7.2.1.6.1 BigFix connector configuration

To add the connector:

1. In **Connector name**, enter a logical name for this connector.

   Tip

   You should use a naming convention for connector names:

   <connector type> <scope> <RCR>

   Scope describes where data is coming from or what it's being used for. For example Demo, Test, Lab, Q2 Audit.

   Include **RCR** in the name if you have enabled **Run Consolidation Reports**.

2. In **BigFix Database Server**, enter the name of the server where the inventory database is hosted. If there is a database instance, then append it to the server name, for example *Server_Name\Instance*. Use the location of the inventory database server rather than the server itself. For example, if your application server is located on device A and its database is located on device B, use the location (hostname or IP address) for device B.
3. In **BigFix Database**, enter the name of the database you want to connect to.
4. If you are authenticating with Windows:
   a. Ensure **Use Windows Authentication** is checked.
   b. You do not need to populate the BigFix SQL Server User and BigFix SQL Server Password fields.
5. If you are using an SQL account:
   a. Ensure **Use Windows Authentication** is unchecked.
   b. In **BigFix SQL Server User**, enter the name for the account you want to use to connect to the database.
   c. In **BigFix SQL Server Password**, enter the password for this account.
6. Check the **Run Consolidation Reports** checkbox if you want consolidation actions to be processed each time the **Sync Data** action is executed for the connector.

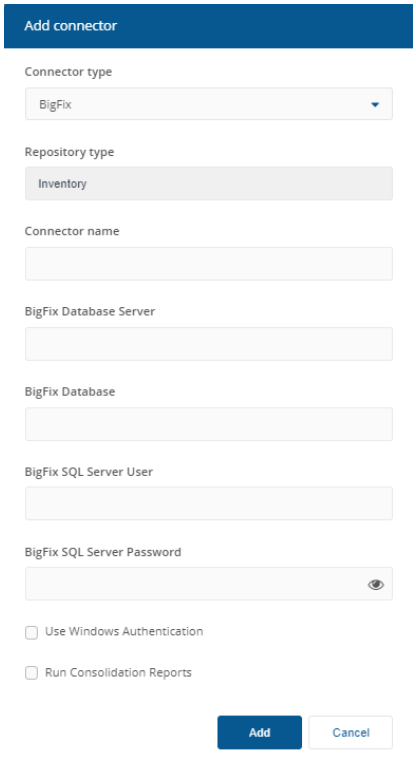
   This can lead to unnecessary processing if you enable this on more than one connector. The recommended method of processing consolidation actions is to schedule the action **Generate Report - Basic Inventory Consolidation** to execute after the **Sync Data** actions have run for all connectors. This will execute the remaining consolidation actions. Alternatively check the

Run Consolidation Reports checkbox on one of your connectors. You can view action processes in **Settings→Process log**.

7. Click **Add**.

After adding the connector, please refer to:

- Connectors page: Test a connector - to test the connector configuration
- Connectors page: Execute a connector sync action - to actually sync data into a repository
- Connectors page: Delete a connector



1.7.2.1.7 BigFixInv connector

Connects to a BigFix Inventory database.

Before adding a new BigFixInv connector, you will need the following:

- domain user account or SQL Login to connect to the BigFix Inventory database
- access rights configured in the BigFix Inventory database.

1.7.2.1.7.1 BigFixInv connector configuration

To add the connector:

1. In **Connector name**, enter a logical name for this connector.

   Tip

You should use a naming convention for connector names:

<connector type> <scope> <RCR>

Scope describes where data is coming from or what it's being used for. For example Demo, Test, Lab, Q2 Audit.

Include **RCR** in the name if you have enabled **Run Consolidation Reports**.

2. In **BigFix Inventory Database Server**, enter the name of the server where the inventory database is hosted. If there is a database instance, then append it to the server name, for example *Server_Name\Instance*. Use the location of the inventory database server rather than the server itself. For example, if your application server is located on device A and its database is located on device B, use the location (hostname or IP address) for device B.

3. In **BigFix Inventory Database**, enter the name of the database you want to connect to.

4. If you are authenticating with Windows:

    a. Ensure **Use Windows Authentication** is checked.

    b. You do not need to populate the BigFix Inventory SQL Server User or BigFix Inventory SQL Server Password fields.

5. If you are using an SQL account:

    a. Ensure **Use Windows Authentication** is unchecked.

    b. In **BigFix Inventory SQL Server User**, enter the name for the account you want to use to connect to the database.

    c. In **BigFix Inventory SQL Server Password**, enter the password for this account.

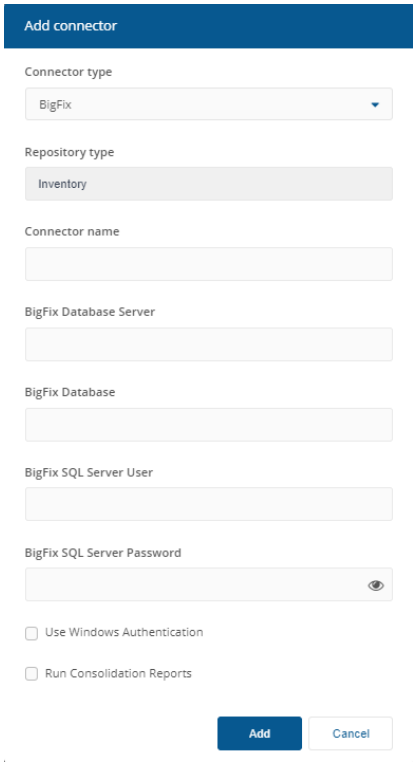
6. Check the **Run Consolidation Reports** checkbox if you want consolidation actions to be processed each time the **Sync Data** action is executed for the connector.

    This can lead to unnecessary processing if you enable this on more than one connector. The recommended method of processing consolidation actions is to schedule the action **Generate Report - Basic Inventory Consolidation** to execute after the **Sync Data** actions have run for all connectors. This will execute the remaining consolidation actions. Alternatively check the **Run Consolidation Reports** checkbox on one of your connectors. You can view action processes in **Settings→Process log**.

7. Click **Add**.

After adding the connector, please refer to:

- Connectors page: Test a connector - to test the connector configuration
- Connectors page: Execute a connector sync action - to actually sync data into a repository
- Connectors page: Delete a connector



1.7.2.1.8 File Upload connector

Uploads inventory data from a folder containing tab (TSV) and comma (CSV) separated value file(s).

Before adding a new **File Upload** connector, you will need the following:

- inventory files with the correct column structure
- folder location with at least **read access** for the **SLA Platform service account**.

1.7.2.1.8.1 File Upload connector configuration

To add the connector:

1. In **Connector name**, enter a logical name for this connector

   Tip

   You should use a naming convention for connector names:

   <connector type> <scope> <RCR>

   Scope describes where data is coming from or what it's being used for. For example Demo, Test, Lab, Q2 Audit.

   Include **RCR** in the name if you have enabled **Run Consolidation Reports**.

2. In **Folder Location**, enter the location for your inventory TSV/CSV file(s)
3. Check the **Run Consolidation Reports** checkbox if you want consolidation actions to be processed each time the **Sync Data** action is executed for the connector.

This can lead to unnecessary processing if you enable this on more than one connector. The recommended method of processing consolidation actions is to schedule the action **Generate Report - Basic Inventory Consolidation** to execute after the **Sync Data** actions have run for all connectors. This will execute the remaining consolidation actions. Alternatively check the **Run Consolidation Reports** checkbox on one of your connectors. You can view action processes in **Settings→Process log**.

4. Click **Add**

Note

The **No incremental sync** checkbox is reserved for future use.

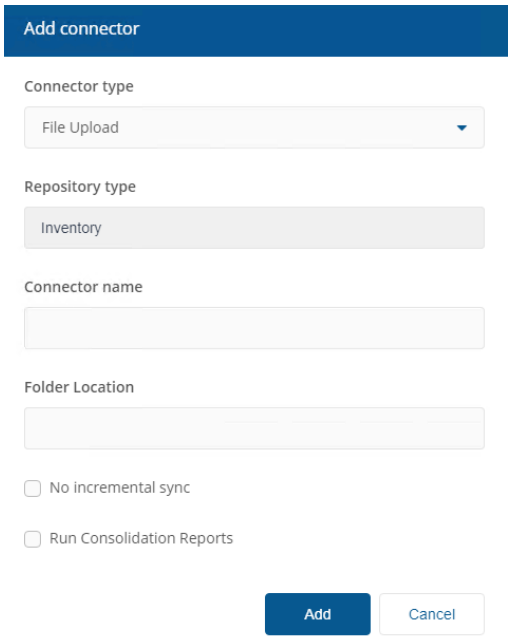
After adding the connector, please refer to:

- Connectors page: Test a connector - to test the connector configuration
- Connectors page: Execute a connector sync action - to actually sync data into a repository
- Connectors page: Delete a connector

Tip

All files in the folder location will be uploaded, including sub-directories.

Test will confirm whether the service account has read access to the folder location.



1.7.2.1.9 Intune connector

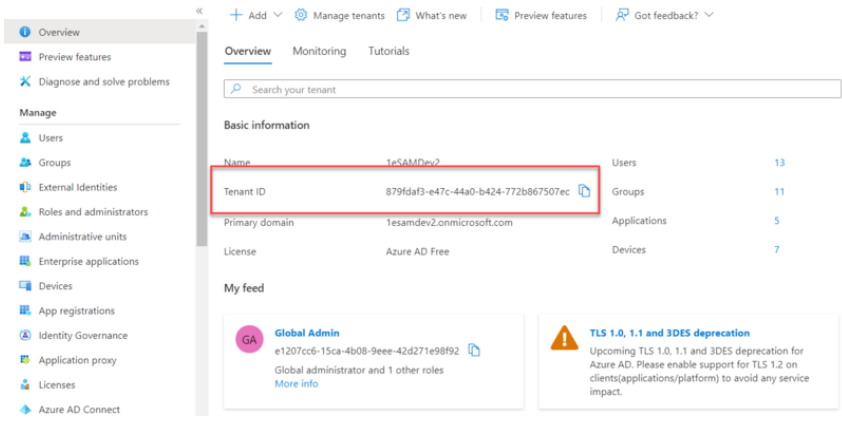
Connects to an Intune application and collects inventory and usage data. For information on the type of data collected by the Intune connector, please refer to the Intune column of the table on Management groups rules page.

The below configuration procedure assumes you already have an Intune subscription, and are able to populate the connector with information available in an Enterprise Application in your Azure Active Directory (AAD) Console.

1.7.2.1.9.1 Prerequisites

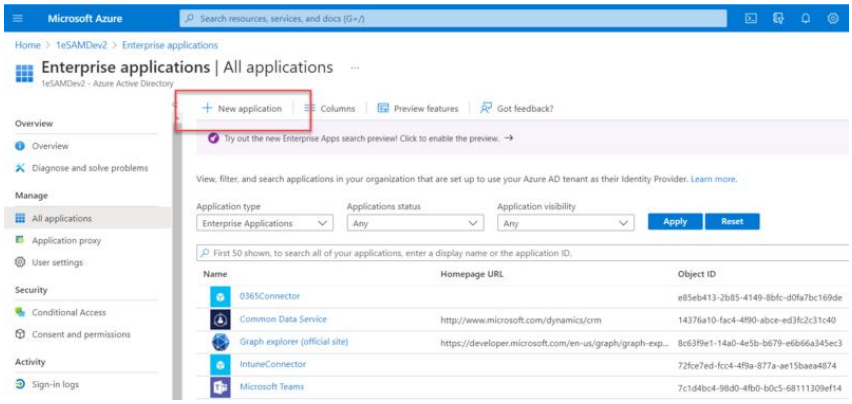
Before adding a new Intune connector, you will need the following information from an Enterprise Application created in your AAD console:

- Azure cloud instance URL (optional) if this is not supplied then **AzurePublic** is used as a default
- Azure **Tenant ID**, available in the **Overview** node of your AAD console (see opposite)
- The registered application clientID (a string representing a GUID)
- A client secret value that has been created for your chosen Enterprise Application.



1.7.2.1.9.1.1 Prepare an AAD application

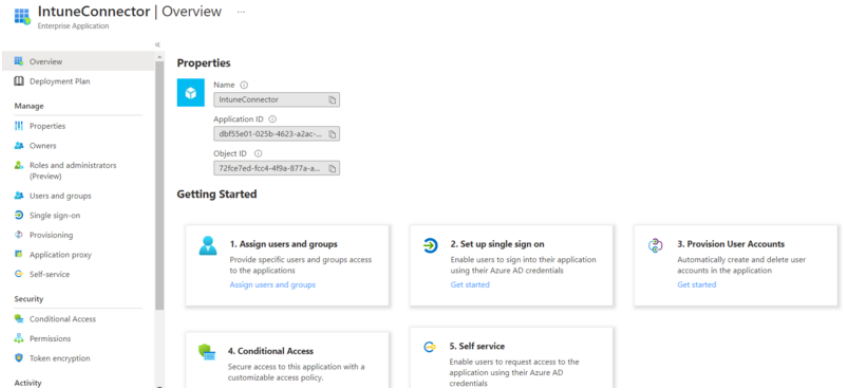
In your Azure Active Directory console, go to the **Enterprise applications** node and click **New application**.



You need to create a non-gallery application, in the version of AAD we're using this is done by clicking the **Create your own application** button.

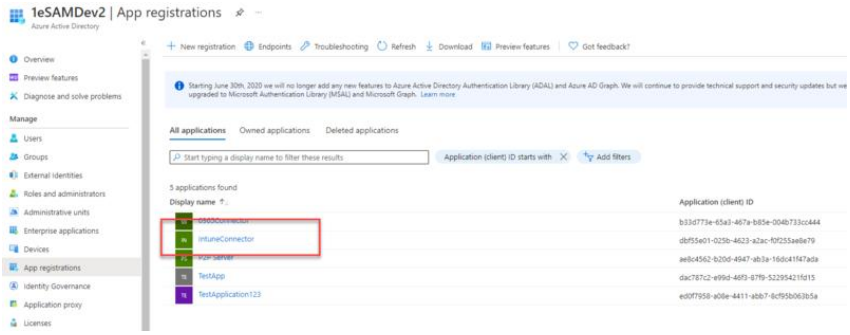
Provide a name for the application. The application name is not important but should suggest the application relates to platform connector. For example **Tachyon Intune Connector**, click **Add** in the bottom left of the screen.

In the **Overview**tab, copy the**Object ID** (called **Client Id** in Tachyon) and the **Application ID** (called **Tenant Id** in Tachyon) values as these will be required for the connector.



Click the **App registrations** node of AAD. Click on the application name for the application(s) listed, you will need to navigate back to the AAD blade.

> **Note**
>
> You may need to change the tab to **All Applications** to see the new application.



1.7.2.1.9.1.2 Add permissions

1. Click on the **API permissions** node under the **Manage** node, then click **Add a permission**.
2. Click on the **Microsoft Graph** tile, then click on **Application permissions**.
3. Scroll through the list of API permissions, and check as appropriate using the following, then click **Add permissions**.

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (3)				
DeviceManagementApps.Read.A	Application	Read Microsoft Intune apps	Yes	Granted for
DeviceManagementManagedDe	Application	Read Microsoft Intune devices	Yes	Granted for
User.Read.All	Application	Read all users' full profiles	Yes	Granted for

4. Click **Grant admin consent for <organization>**, where <organization> is the **Organization** you set when you created your Intune instance.

   This means that as an administrator for your organization, you're consenting that the users of the application would want to use these permissions.

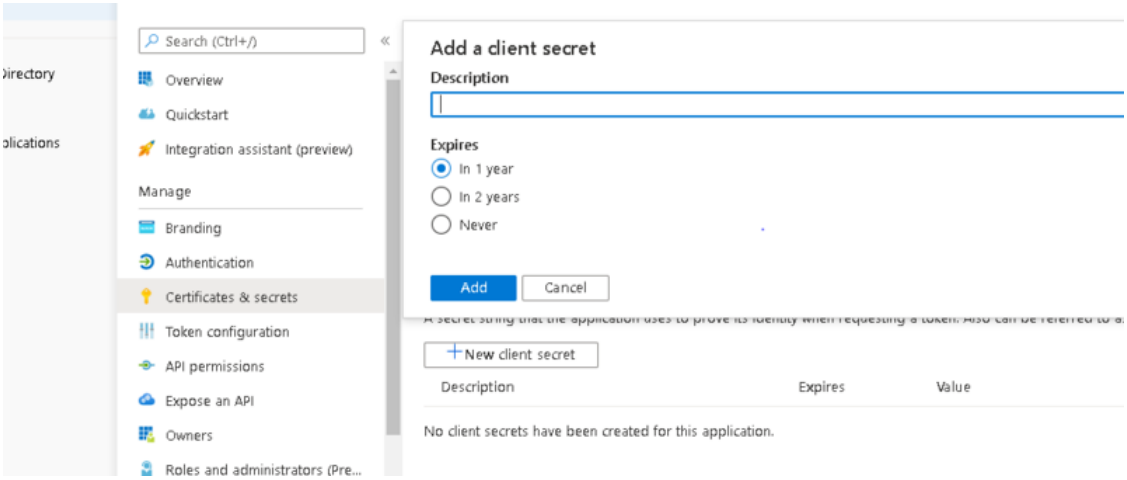
1.7.2.1.9.1.3 Add a client secret

Click on the **Certificates & secrets** node and then click on the **New client secret** button.

The **Add a client secret** form will open, add a **Description** and select an expiry from the **Expires** radio buttons and then click **Add**.

Copy the new client secret value and save it, as you won't be able to retrieve it after you perform another operation or leave this blade.

> **Warning**
>
> If you do not copy the **Value** at this point, when you navigate away from the **Certificates & secrets** screen you will be unable to copy it again. This means that you will have to delete the **Secret** and recreate it.



1.7.2.1.9.2 Configuring the Intune connector

These instructions show how to create an Intune connector in the **Settings** application.

1.7.2.1.9.2.1 Adding, testing and running an Intune connector

These are the steps to add, test and run an Intune connector.

1.7.2.1.9.2.1.1 Adding an Intune connector

1. In the Tachyon portal portal, navigate to **Settings**→**Configuration**→**Connectors**.
2. Click on the **Add** button.
3. In the **Add connector** popup, select the **Intune** type.
4. In **Connector name**, enter a logical name for this connector. In our example we choose the name **Intune Inventory**.
5. **Azure Cloud Instance** can be set to the URL for your Intune implementation. If you leave this field blank **AzurePublic** is used as a default, for the **AzureCloudInstance** reference see https://learn.microsoft.com/en-us/dotnet/api/microsoft.identity.client.azurecloudinstance?view=msal-dotnet-latest
6. In Azure **Tenant Id**, enter your Azure tenant ID, available in the **Overview**node of your AAD console.

7. **Client Id** this should be set to your registered application clientID.
8. **Client Secret** this should be set to the specific client secret value that has been created for your chosen Enterprise Application
9. **Run Consolidation Reports** - check this checkbox if you want the consolidation reports running automatically after this connector has been synchronized.
10. Click **Add**.

The new connector has now been added and a new action that can be used to run the connector has been created in the background, called **Sync Data - Intune Inventory**.

1.7.2.1.9.2.1.2 Testing an Intune connector

1. Select the Intune connector by checking the box at the left-hand end of its entry in the **Connectors** table.
2. Click the **Test** button.
    a. The **Test status** column for the connector will display a clock icon

    indicating that the test has been queued for executing.
    b. If the test succeeds, **Test status** will display a check icon

    and the **Last tested** column will display the date and time the test succeeded.
    c. If the test fails, the **Test status** will display a failed icon

    and you'll need to check the details you entered for the connector.
3. If the test succeeds, you can proceed to run the connector to populate an inventory repository.

1.7.2.1.9.2.1.3 Running an Intune connector

1. Click the **Execute** button.
2. In the **Execute action** popup subsequently displayed, use the **Repository** menu to select the inventory repository you want to populate.
3. Once the repository has been selected, you can then select the action to run. In the case of inventory repositories, the actions will be restricted to inventory related actions. For a connector, you will be looking for an action with the form **Sync Data - <connector name>**.
4. Select whether you want to clear any existing data in the repository by checking the **Clean sync** checkbox.
5. Click **Execute** button in the **Execute action** popup to start the sync.

6. When the sync starts, a number of actions are queued to be performed on the selected repository. To check the progress of the sync actions:

    a. Navigate to the **Monitoring→Process log** page.

    b. Here, you can see the sequence of actions that have been queued for the selected repository related to the **Sync Data** action selected.

    c. When each action has finished running, you'll see a check icon

    appear in the **Status** column if it succeeds or a failed icon

    if it fails.

7. Once all the actions have succeeded, you can check the results. To do this:

    a. Navigate to the **Monitoring→Sync log** page.

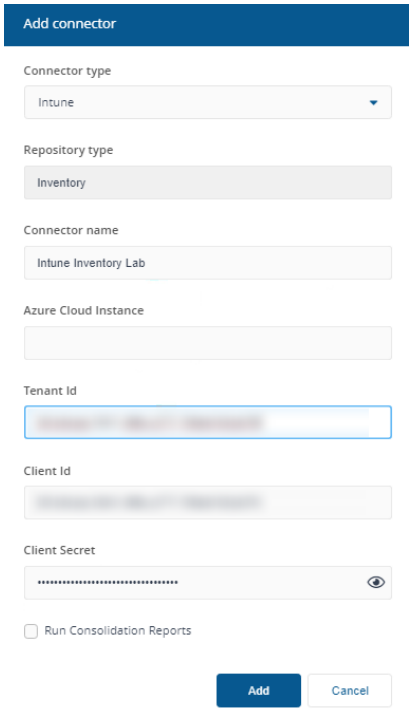
    b. This displays the items that have been added to the selected repository as a result of running the sync.

1.7.2.1.9.2.2 The Intune connector parameters

The following fields are available in the **Add connector** and **Edit connector** popups when the **Intune Connector type** is selected, as shown in the picture opposite:

Field	Description
Connector type	Shows the connector type: **Intune**.
Repository type	Shows which type of repository the connector works with. For the **Intune Connector type** this is always **Inventory**.
Connector name	Here you set the logical name for the connector. **Tip** You should use a naming convention for connector names: **<connector type> <scope> <RCR>** **Scope** describes where data is coming from or what it's being used for. For example Demo, Test, Lab, Q2 Audit. Include **RCR** in the name if you have enabled **Run Consolidation Reports**.

Field	Description
Azure Cloud Instance	Azure cloud instance URL (optional) if this is not supplied the **AzurePublic** is used as a default.
Tenant Id	Azure tenant ID, available in the **Overview** node of your AAD console.
Client Id	The registered application clientID.
Client Secret	A client secret value that has been created for your chosen Enterprise Application.
Run Consolidation Reports	Check the **Run Consolidation Reports** checkbox if you want consolidation actions to be processed each time the **Sync Data** action is executed for the connector. This can lead to unnecessary processing if you enable this on more than one connector. The recommended method of processing consolidation actions is to schedule the action **Generate Report - Basic Inventory Consolidation** to execute after the **Sync Data** actions have run for all connectors. This will execute the remaining consolidation actions. Alternatively check the **Run Consolidation Reports** checkbox on one of your connectors. You can view action processes in **Settings→Process log**.



1.7.2.1.10 Microsoft Office 365 connector

Connects to an Office 365 application in InTune and pulls in inventory and usage data. The following steps assume you have an InTune and Microsoft Office 365 subscription, and can populate the connector with details from an Enterprise Application in your AAD Console.

1.7.2.1.10.1 Prerequisites

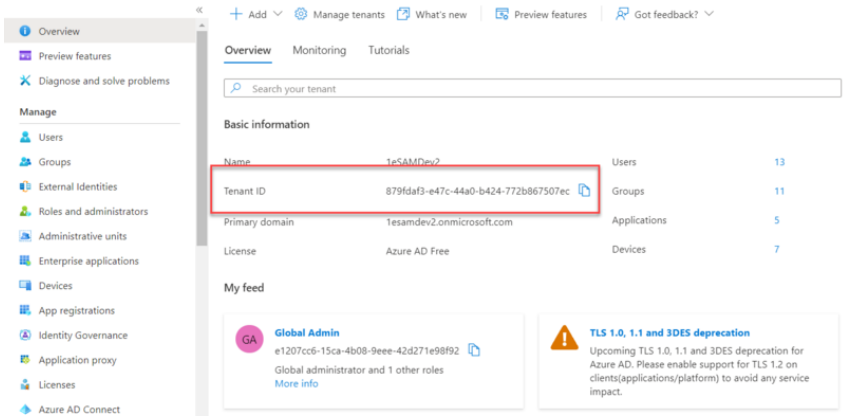
Before adding a new **Microsoft Office 365** connector, you will need to complete the following steps:

- Enable PowerShell to connect to Azure using MSOL
- Prepare an AAD application
- Add permissions
- Add a client secret
- Add a user with the necessary permissions to run the PowerShell scripts.

You will need the following information from an Enterprise Application created in your AAD console:

- Azure cloud instance URL (optional) if this is not supplied then **AzurePublic** is used as a default
- Azure **Tenant ID**, available in the **Overview** node of your AAD console
- The registered application clientID (a string representing a GUID)
- A client secret value that has been created for your chosen Enterprise Application

- SingleSignIn enabled Service Account with global reader permissions for running PowerShell cmdlets.



1.7.2.1.10.1.1 Enable PowerShell to connect to Azure using MSOL

On the Tachyon server where the **Microsoft Office 365** connector will be executed, PowerShell needs to connect to Azure using MSOL, which requires the following two modules installed:

Install-Modules for Microsoft Office 365

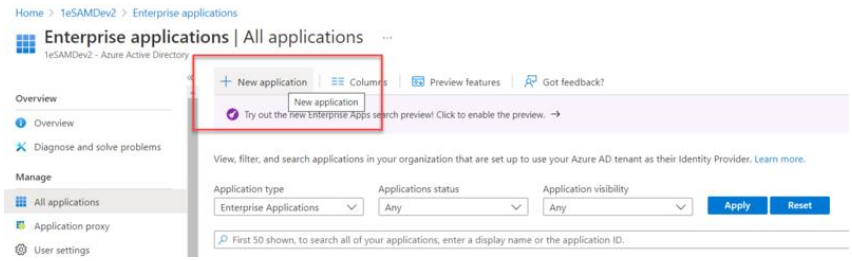
```
Install-Module -Name AzureAD
Install-Module -Name MsOnline
```

> **Note**
>
> If you see the following warnings when installing a module, you will need to run the following command first:
>
> WARNING: Unable to download from URI 'https://go.microsoft.com/fwlink/?LinkID=627338&clcid=0x409' to ''.
>
> WARNING: Unable to download the list of available providers. Check your internet connection.

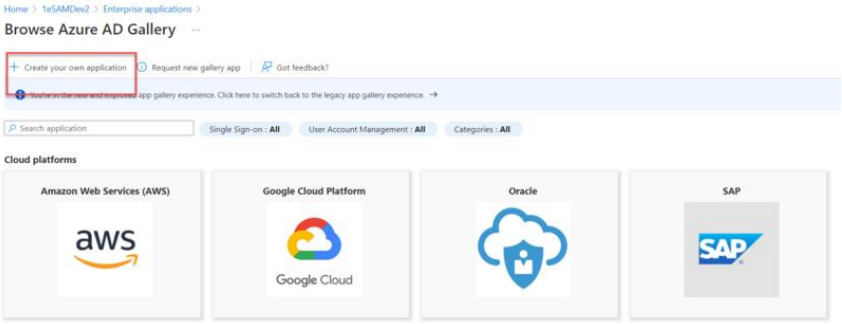
```
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
```

1.7.2.1.10.1.2 Prepare an AAD application

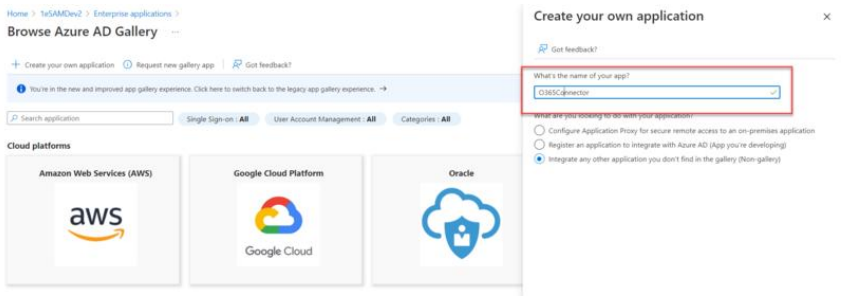
In your Azure Active Directory console, go to the **Enterprise applications** node and click **New application**.



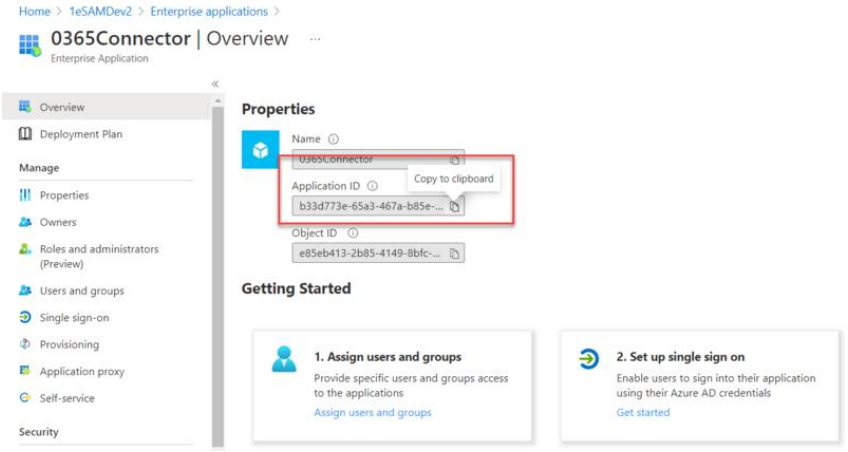
You need to create a non-gallery application, in the version of AAD we're using this is done by clicking the **Create your own application** button.



Provide a name for the application. The name of application should suggest the application is related to the Office 365 connector, for example: **Tachyon O365 Connector**. In this version of AAD we select the **Integrate any other application you don't find in the gallery (Non-gallery)** option and then click**Create**in the bottom left of the panel.



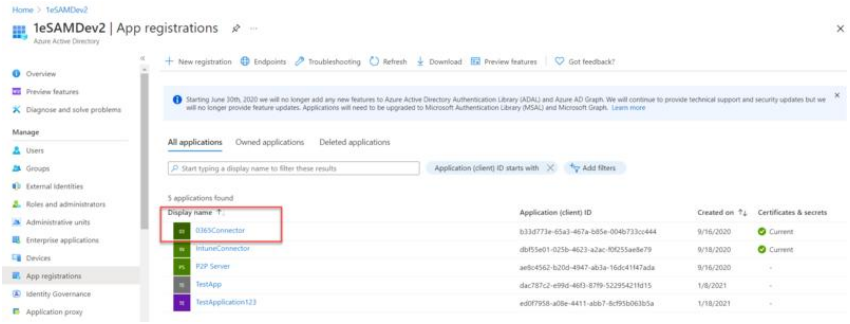
In the **Overview** tab for the new application, copy the **Application ID** value as this will be required for the connector.



Navigate back to the AAD blade and click the **App registrations** node of AAD.

> **Note**
>
> You may need to change the tab to **All applications** to see the new application.

Click on the application name for the new application.



1.7.2.1.10.1.3 Add permissions

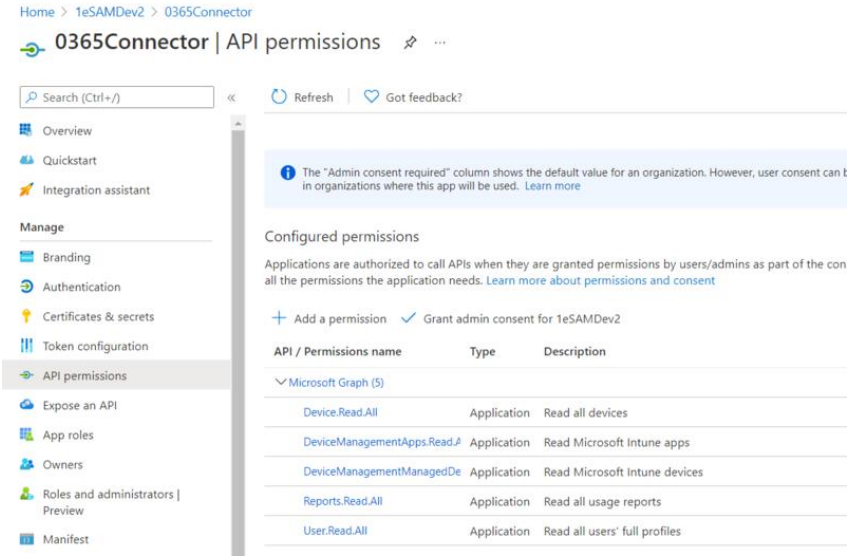
Click on the **API permissions** node under the **Manage** section, then click **Add a permission**.

Click on the **Microsoft Graph** tile and then click on **Application permissions**.

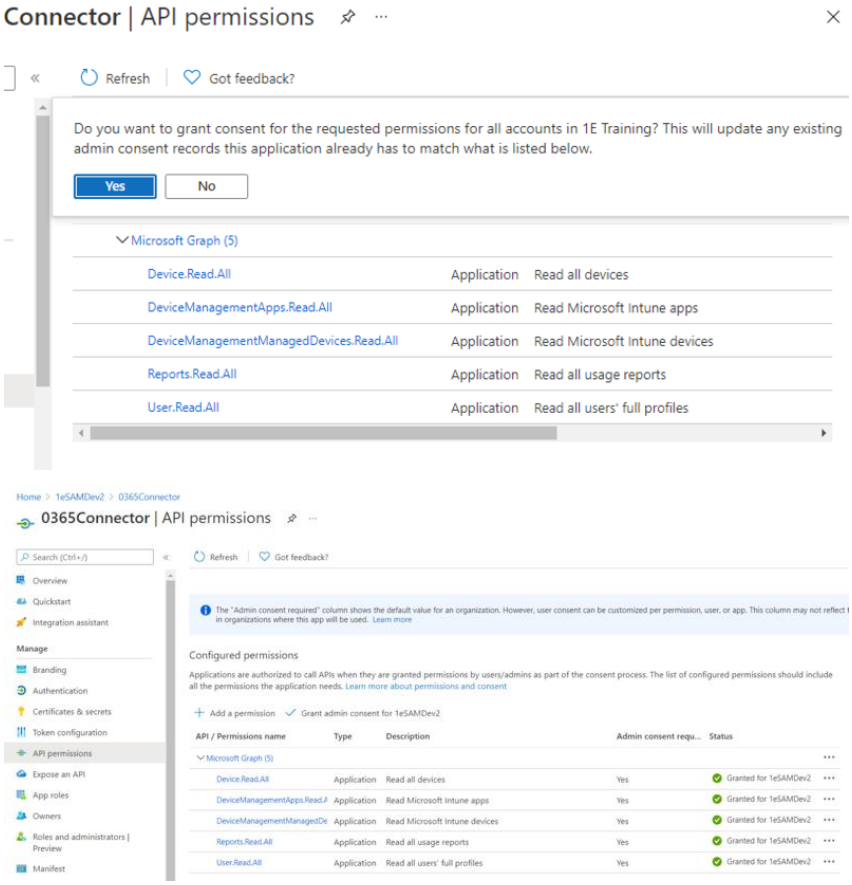
You will see a long list of API permissions, scroll through them and check as appropriate using the following table as a guide.

Group	Permission
Device	Read.All
DeviceManagementApps	Read.All
DeviceManagementManagedDevices	Read.All
Reports	Read.All
User	Read.All

When you have selected the correct permissions, click **Add permissions**. After they've been added, the permissions should like the picture shown opposite.



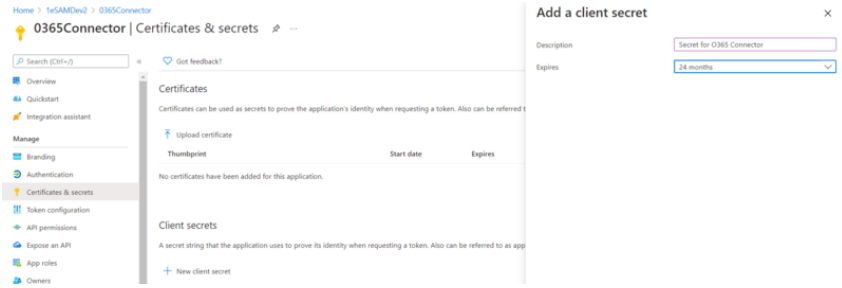
Click **Grant admin consent for <organization>**, where <organization> is the **Organization** you set when your InTune instance was created. This means that as an administrator for your organization, you're consenting that the users of the application can use these permissions. Click **Yes** to confirm.



1.7.2.1.10.1.4 Add a client secret

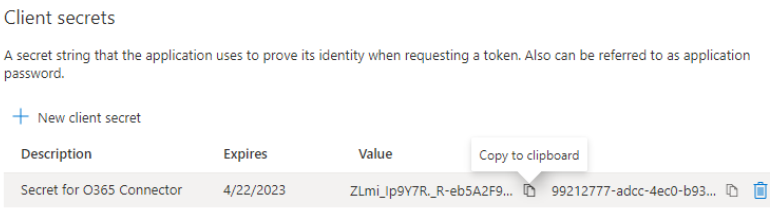
Click on the **Certificates & secrets**node, and then click on **New client secret** button

The **Add a client secret** form will open, add a **description** and select an expiry from the **Expires** options and then click **Add**.



Copy the new client secret **Value** and save it. It is important you save the client secret **Value**, as you won't be able to retrieve it after you perform another operation or leave this blade.

> **Warning**
>
> If you do not copy the **Value** at this point, when you navigate away from the **Certificates & secrets** screen you will be unable to copy it again. This means that you will have to delete the **Secret** and recreate it.



1.7.2.1.10.1.5 Add a user with the necessary permissions to run the PowerShell scripts

An AAD user with Reports Reader permissions must be made available in your organization's blade. The credentials for this user will be set in the Microsoft Office 365 connector when it is created in Tachyon.

1.7.2.1.10.2 Configuring the Microsoft Office 365 connector

These instructions show how to create a Microsoft Office 365 connector in the Settings application.

1.7.2.1.10.2.1 Adding, testing and running a Microsoft Office 365 connector

These are the steps to add, test and run a Microsoft Office 365 connector.

1.7.2.1.10.2.1.1 Adding a Microsoft Office 365 connector

1. In the Tachyon portal portal, navigate to **Settings→Configuration→Connectors**.
2. Click on the **Add** button.
3. In the **Add connector** popup select the **Microsoft Office 365** type.
4. In **Connector name**, enter a logical name for this connector. In our example we choose the name **Microsoft Office 365 Inventory**.

5. **Azure Cloud Instance** can be set to the URL for your InTune implementation. If you leave this field blank **AzurePublic** is used as a default.
6. In Azure **Tenant Id**, enter your Azure tenant ID, available in the **Overview**node of your AAD console.
7. **Client Id** this should be set to your registered application clientID.
8. **Client Secret** this should be set to the specific client secret value created for your chosen Enterprise Application.
9. **Login Email** - set this to the permissioned user.
10. **Login Password** - set this to the password for the permissioned user.
11. Click **Add**.

The new connector has now been added and a new action to run the connector has been created in the background, called:

Sync Data - Microsoft Office 365 Inventory

1.7.2.1.10.2.1.2 Testing a Microsoft Office 365 connector

1. Select the Microsoft Office 365 connector by checking the box at the left-hand end of its entry in the **Connectors** table.
2. Click the **Test** button.
    a. The **Test status** column for the connector will display a clock icon

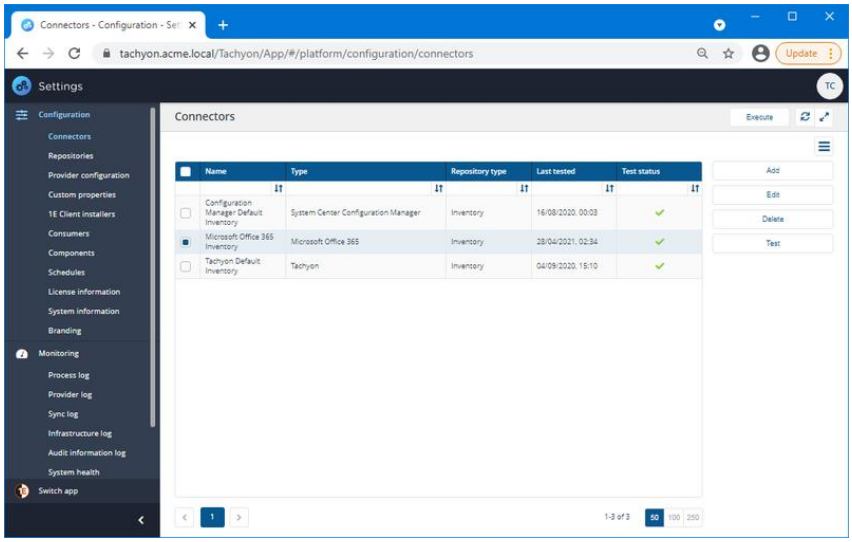
    indicating that the test has been queued for executing.

    b. If the test succeeds **Test status** will display a check icon

    , and the **Last tested** column will display the date and time the test succeeded.

    c. If the test fails the **Test status** will display a failed icon

    , and you'll need to check the details you entered for the connector.
3. If the test succeeds, you can proceed to run the connector to populate an inventory repository.

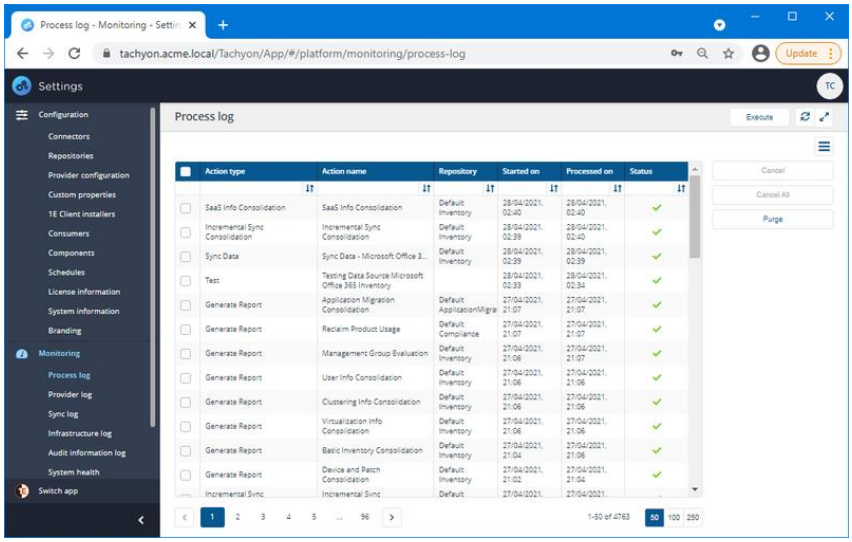


1.7.2.1.10.2.1.3 Running a Microsoft Office 365 connector

1. Click the **Execute** button.
2. In the **Execute action** popup subsequently displayed, use the **Repository** menu to select the inventory repository you want to populate.
3. Once the repository has been selected, you can then select the action to run. In the case of inventory repositories the actions will be restricted to inventory related actions. For a connector you will be looking for an action with the form **Sync Data - <connector name>**.
4. Select whether you want to clear any existing data in the repository by checking the **Clean sync** checkbox.
5. Click **Execute** button in the **Execute action** popup to start the sync.
6. When the sync starts, a number of actions are queued to be performed on the selected repository. To check the progress of the sync actions:
    a. Navigate to the **Monitoring→Process log** page.
    b. Here you can see the sequence of actions queued for the selected repository related to the **Sync Data** action selected.
    c. When each action has finished running you'll see a check icon

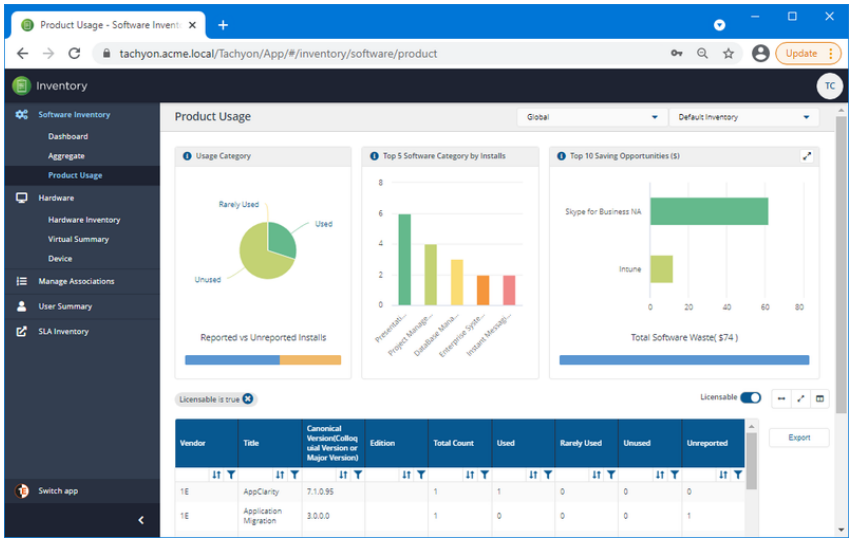
    appear in the **Status** column if it succeeds or a failed icon

    if it fails.



1.7.2.1.10.2.2 Viewing Microsoft Office 365 information in the Inventory application

1. Use the **Switch app** menu to open the **Inventory** application.
2. Navigate to **Software Inventory**→**Product Usage** page.
3. On this page you should see software items from your AAD environment.



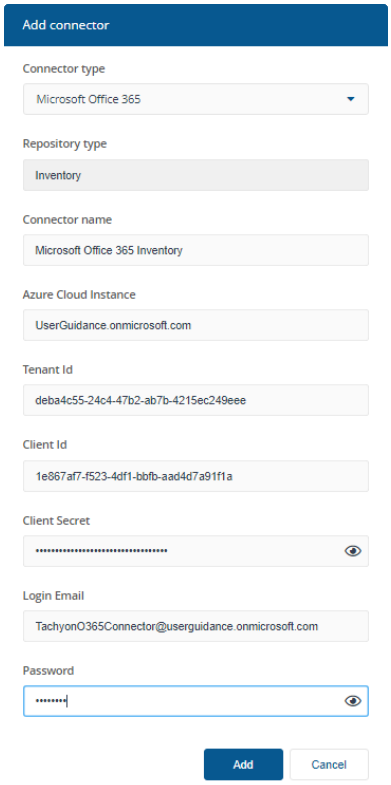
1.7.2.1.10.2.3 The Microsoft Office 365 connector parameters

The following fields are available in the **Add connector** and **Edit connector** popups when the **Microsoft Office 365 Connector type** is selected, as shown in the picture opposite:

Field	Description
Connector type	Shows the connector type: **Microsoft Office 365**.

Field	Description
Repository type	Shows which type of repository the connector works with. For the **Microsoft Office 365 Connector type** this is always **Inventory**.
Connector name	Here you set the logical name for the connector. **Tip** You should use a naming convention for connector names: **<connector type> <scope> <RCR>** **Scope** describes where data is coming from or what it's being used for. For example Demo, Test, Lab, Q2 Audit. Include **RCR** in the name if you have enabled **Run Consolidation Reports**.
Azure Cloud Instance	Azure cloud instance URL (optional) if this is not supplied, the **AzurePublic** is used as a default.
Tenant Id	Azure tenant ID, available in the **Overview** node of your AAD console.
Client Id	The registered application clientID.
Client Secret	A client secret value that has been created for your chosen Enterprise Application.
Login Email	The user login name for the permissioned user.
Password	The password for the permissioned user.
Run Consolidation Reports	Check the **Run Consolidation Reports** checkbox if you want consolidation actions to be processed each time the **Sync Data** action is executed for the connector. This can lead to unnecessary processing if you enable this on more than one connector. The recommended method of processing consolidation actions is to schedule the action **Generate Report - Basic Inventory Consolidation** to execute after the **Sync Data** actions have run for all connectors. This will execute the remaining consolidation actions. Alternatively check the

Field	Description
	Run Consolidation Reports checkbox on one of your connectors. You can view action processes in **Settings→Process log**.



1.7.2.1.11 OpenLM connector

Connects to an OpenLM database server.

Warning

Note

Please contact your 1E Account Team if you need more information about using this feature.

The OpenLM connector is a preview feature to demonstrate how Tachyon can collect license data from OpenLM. Currently, the collected data can be viewed only by using SQL queries, and cannot be viewed in the TachyonPortal or its Consumer applications. License data from OpenLM is not merged with entitlement data used by AppClarity.

The connector will be updated in future versions of Tachyonto support ongoing changes by OpenLM as they migrate from their XML-based API to their new REST-based API.

1.7.2.1.11.1 Prerequisites

Before adding a new OpenLM connector, you will need the following:

- OpenLM Server version 21.12
- OpenLM identity service enabled
- User name and password that provides access to OpenLM - refer to OpenLM security configuration
- Client ID and secret pair.

1.7.2.1.11.2 OpenLM connector configuration

To add the OpenLM connector:

1. In **Connector name**, enter a logical name for this connector.

   Tip

   You should use a naming convention for connector names:

   <connector type> <scope> <RCR>

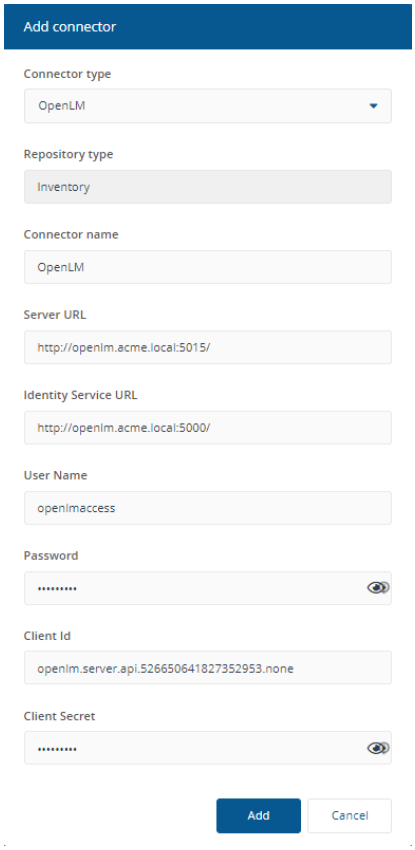
   Scope describes where data is coming from or what it's being used for. For example Demo, Test, Lab, Q2 Audit.

   Include **RCR** in the name if you have enabled **Run Consolidation Reports**.
2. In **Server URL**, enter the URL of the OpenLM Server, including port, for example **http://openlm.acme.local:5015/**
3. In **Identity Service URL**, enter the URL of the OpenLM Identity Service, including port, for example **http://openlm.acme.local:5000/**
4. In **User Name**, enter an OpenLM user name that already exists in your OpenLM system
5. In **Password**, enter the password for the OpenLM user
6. In **Client Id**, enter the Client Id
7. In **Client Secret**, enter the Client Secret
8. Click **Add**.

Tachyonsaves details encrypted.

After adding the connector, please refer to:

- Test a connector - to test the connector configuration
- Execute a connector sync action - to actually sync data into a repository
- Delete a connector



1.7.2.1.12 Oracle LMS connector

Connects to Oracle LMS and queries it for inventory information.

Before adding a new **Oracle LMS** connector, you will need the following:

- Location of Oracle LMS
- At least **read access** for the **SLA Platform service account**.

1.7.2.1.12.1 Oracle LMS connector configuration

To add the connector:

1. In **Connector name**, enter a logical name for this connector.

   Tip

   You should use a naming convention for connector names:

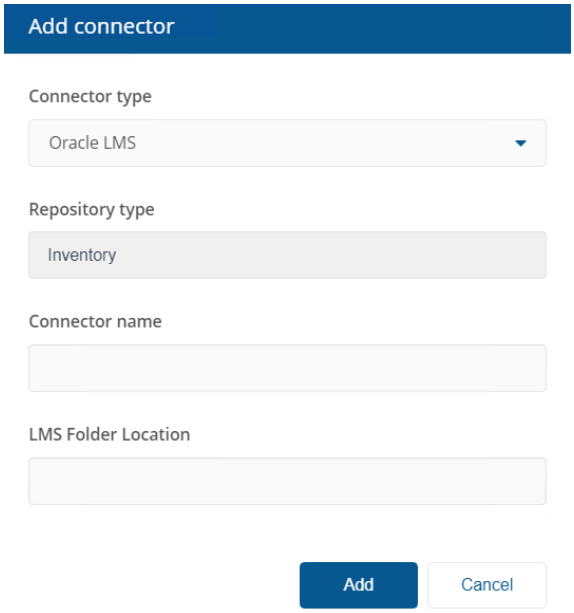
   <connector type> <scope> <RCR>

   Scope describes where data is coming from or what it's being used for. For example Demo, Test, Lab, Q2 Audit.

   Include **RCR** in the name if you have enabled **Run Consolidation Reports**.
2. In **LMS Folder Location** enter the location for the file.
3. Click **Add**

After adding the connector, please refer to:

- Test a connector - to test the connector configuration
- Execute a connector sync action - to actually sync data into a repository
- Delete a connector



1.7.2.1.13 ServiceNow connector

Connects to a ServiceNow instance to import basic inventory data into SLA Platform.

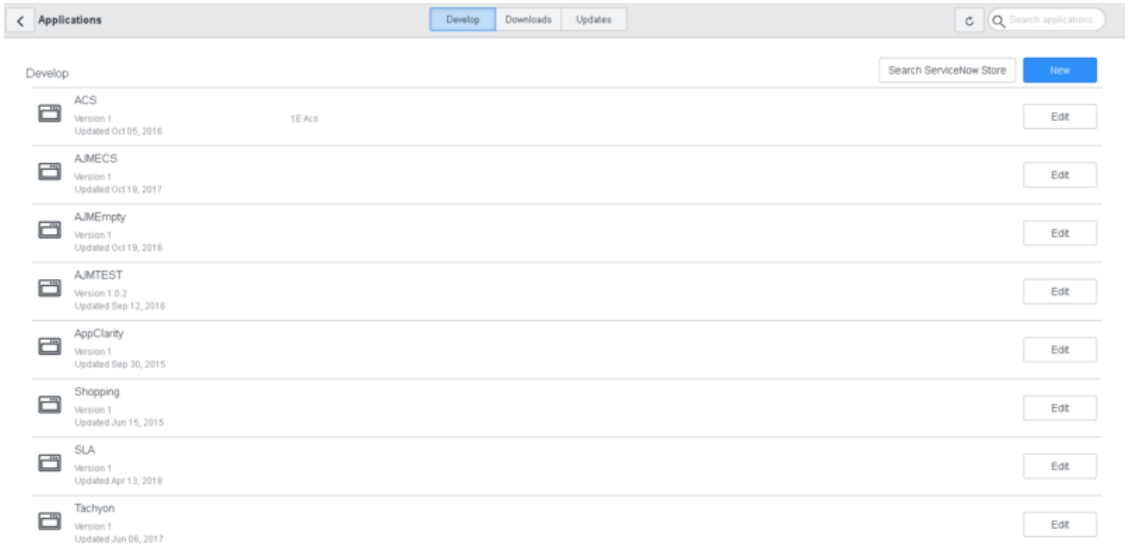
The SLA Platform ServiceNow connector is compatible with the ServiceNow Jakarta release.

Before adding a new ServiceNow connector, you will need the following:

- A ServiceNow application, with defined tables populated with data
- A ServiceNow user with read rights on application scope.

1.7.2.1.13.1 Create an application in your ServiceNow instance

1. Create a new application in ServiceNow, and configure the application scope.
2. Under the new application, create tables with fields using the schema shown below under: Table fields
3. Map / populate inventory data in these table fields.



1.7.2.1.13.2 ServiceNow connector configuration

To add the connector:

1. In **Connector name**, enter a unique name for this connector.

   Tip

   You should use a naming convention for connector names:

   <connector type> <scope> <RCR>

   Scope describes where data is coming from or what it's being used for. For example Demo, Test, Lab, Q2 Audit.

   Include **RCR** in the name if you have enabled **Run Consolidation Reports**.

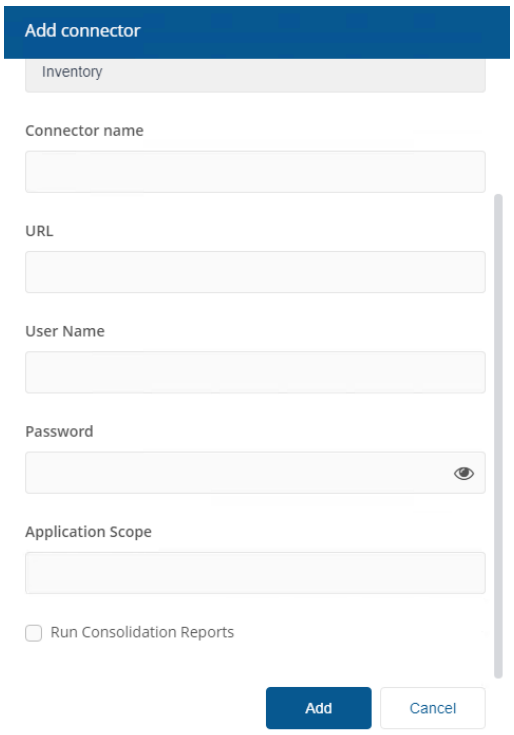
2. In **URL**, enter location of ServiceNow.
3. In **User Name**, enter the name of the account you want to use to connect to ServiceNow.
4. In **Password**, enter the password for this account.
5. In **Application Scope**, enter the scope being used in ServiceNow
6. Check the **Run Consolidation Reports** checkbox if you want consolidation actions to be processed each time the **Sync Data** action is executed for the connector.

   This can lead to unnecessary processing if you enable this on more than one connector. The recommended method of processing consolidation actions is to schedule the action **Generate Report - Basic Inventory Consolidation** to execute after the **Sync Data** actions have run for all connectors. This will execute the remaining consolidation actions. Alternatively check the **Run Consolidation Reports** checkbox on one of your connectors. You can view action processes in **Settings→Process log**.

7. Click **Add**.

After adding the connector, please refer to:

- Test a connector - to test the connector configuration
- Execute a connector sync action - to actually sync data into a repository
- Delete a connector



1.7.2.1.13.3 ServiceNow Terms Glossary

Application Scope | Application Menu | Field types | Instance | Portal

Term	Definition
Application Scope	An application scope is a logical boundary in ServiceNow which allows restricted access to services inside ServiceNow portal. Anything that you work upon must come under an application scope in ServiceNow. Every instance of ServiceNow comes with a default application scope called “Global” scope. So, any item e.g. incident, request item, variable set etc. that you create will come under the scope of “Global” application scope. For more information, please refer to: https://docs.servicenow.com/bundle/kingston-application-development/page/build/applications/concept/c_ApplicationScope.html.
Application Menu	The application menu forms the main navigational flow of the website. Every top level node in left navigation pane is an application menu e.g. Self-Service, Benchmarks, Guided Setup etc. For more information, please refer to:

Term	Definition
	https://docs.servicenow.com/bundle/kingston-platform-user-interface/page/use/navigation/concept/c_ApplicationNavigation.html.
Field types	ServiceNow database fields support a range of data types. For more information, please refer to: https://docs.servicenow.com/bundle/kingston-platform-administration/page/administer/reference-pages/reference/r_DatabaseFieldTypes.html
Instance	ServiceNow offer cloud instances to its customers, technology partners (vendors) and community developers. You can correlate it to SQL Server database instances which is the core of entire product. Vendor instance is a licensed product which is fully featured instance of ServiceNow having all the capabilities. Developer instances are trial kind of instances with few limitations e.g. they get reclaimed if the instance remains unused for 10 consecutive days.
Portal	Each instance of ServiceNow is managed, configured and controlled through a website (navigation page). The portal can also be used to create self-service requests as well.

1.7.2.1.13.4 Table fields

1.7.2.1.13.4.1 Device

DeviceIdent	String
ComputerName	String
Vendor	String
Model	String
Serial	String
SocketCount	Int
IsVirtual	Boolean
IsClustered	Boolean
InventoryDate	DateTime
PurchaseDate	DateTime

LastLogonDate	DateTime
DomainName	String
ADSiteName	String
NetbiosName	String
NetbiosDomainName	String

1.7.2.1.13.4.2 DeviceClassification

DeviceIdent	String
Classification	String

1.7.2.1.13.4.3 DeviceVirtual

DeviceIdent	String
HostDeviceIdent	String
Technology	String
VMLabel	String
IsHostAffinityEnabled	Boolean
IsCPUAffinityEnabled	Boolean
MaxAssignedCores	Int
CPUPoolName	String
CPUPoolSize	Int

1.7.2.1.13.4.4 File

FileIdent	String
Name	String
Version	String

Size	Int
Hash	String

1.7.2.1.13.4.5 MapDeviceFile

DeviceIdent	String
FileIdent	String
LastUsedDate	DateTime
Path	String

1.7.2.1.13.4.6 MapDeviceOU

DeviceIdent	String
OUIdent	String

1.7.2.1.13.4.7 MapDeviceSoftware

DeviceIdent	String
SoftwareIdent	String
InstallDate	DateTime
InstanceName	String
IsClustered	Boolean
Path	String
PurchaseDate	DateTime
IsUsed	Boolean
IsPublicFacing	Boolean
LastUsedDate	DateTime

1.7.2.1.13.4.8 MapDeviceSoftwareUser

DeviceIdent	String
SoftwareIdent	String
UserIdent	String
InstanceName	String
LastLogin	DateTime
IsEnabled	Boolean
InventoryDate	DateTime

1.7.2.1.13.4.9 MapDeviceUser

DeviceIdent	String
UserIdent	String
LastLogin	DateTime
IsEnabled	Boolean
InventoryDate	DateTime
IsTopConsoleUser	Boolean

1.7.2.1.13.4.10 MapSoftwareOU

SoftwareIdent	String
OUIdent	String
InstanceName	String

1.7.2.1.13.4.11 OU

OUIdent	String
Name	String

ParentOUIdent	String
IsExternal	Boolean
Location	String
Department	String

1.7.2.1.13.4.12 Processor

DeviceIdent	String
Vendor	String
Family	String
Model	String
Name	String
CoreCount	Int
ThreadsPerCore	Int
SpeedMHz	Decimal
InventoryDate	DateTime

1.7.2.1.13.4.13 Software

SoftwareIdent	String
Vendor	String
Title	String
Version	String
ColloquialVersion	String
Edition	String

1.7.2.1.13.4.14 User

UserIdent	String
UserName	String
Email	String
FirstName	String
LastName	String
IsExternal	Boolean

1.7.2.1.14 System Center Configuration Manager connector

Connects to a Configuration Manager database and pulls in inventory and usage data.

Before adding a new System Center Configuration Manager (SCCM) connector, you will need the following:

- Configuration Manager client settings are enabled
- Configuration Manager database access for one of the following and given database rights as described below:
  - Tachyon Server's Network Service (computer$) account
  - a SQL Login that already exists in the Configuration Manager database

Tip

This connector supports both System Center Configuration Manager (SCCM) and Microsoft Endpoint Configuration Manager (MECM).

1.7.2.1.14.1 System Center Configuration Manager connector configuration

1.7.2.1.14.1.1 Adding, testing and running a Configuration Manager connector

To demonstrate how to add, test and run a Configuration Manager connector, we will use our example ACME environment. The following steps are also shown in the video opposite.

1.7.2.1.14.1.1.1 Adding a Configuration Manager connector

1. Navigate to **Settings**→**Configuration**→**Connectors**.
2. Click on the **Add** button.
3. In the **Add connector** popup, select the **System Center Configuration Manager Connector** type.
4. In **Connector name**, enter a logical name for this connector. In our example, we choose the name **System Center Configuration Manager Inventory** .

5. In **SCCM Database Server**, enter the name of the SQL Server instance where the Configuration Manager database is hosted, including custom port if used. In our example this is **ACME-SQL01**.

6. In **SCCM Database**, enter the name of the Configuration Manager database you want to connect to. In our example, this is called **CM_CM1**.

7. In our example, we will be using the **SLA Integrate Services Agent** service account to access the database. So we do the following:

    a. Skip the **SCCM SQL Server User** and **SCCM SQL Server Password** fields.

    b. Ensure **Use Windows Authentication** is checked.

8. Check the **Run Consolidation Reports** checkbox if you want consolidation actions to be processed each time the **Sync Data** action is executed for the connector.

    This can lead to unnecessary processing if you enable this on more than one connector. The recommended method of processing consolidation actions is to schedule the action **Generate Report - Basic Inventory Consolidation** to execute after the **Sync Data** actions have run for all connectors. This will execute the remaining consolidation actions. Alternatively check the **Run Consolidation Reports** checkbox on one of your connectors. You can view action processes in **Settings→Process log**.

9. Click **Add**.

The new connector has now been added and a new action that can be used to run the connector has been created in the background, called
Sync Data - System Center Configuration Manager Inventory.

1.7.2.1.14.1.1.2 Testing a Configuration Manager connector

1. Select the Configuration Manager connector by checking the box at the left-hand end of its entry in the **Connectors** table.

2. Click the **Test** button.

    a. The **Test status** column for the connector will display a clock icon

    indicating that the test has been queued for executing.

    b. If the test succeeds, **Test status** will display a check icon

    and the **Last tested** column will display the date and time the test succeeded.

    c. If the test fails, the **Test status** will display a failed icon

    and you'll need to check the details you entered for the connector.

3. In our example the test succeeds, so we can now continue to run the connector to populate an inventory repository.

1.7.2.1.14.1.1.3 Running a Configuration Manager connector

1. Click the **Execute** button.
2. In the **Execute action** popup subsequently displayed, use the **Repository** menu to select the inventory repository you want to populate. In our example, this is a repository called **Configuration Manager inventory**.
3. Once the repository has been selected you can then select the action to run. In the case of inventory repositories, the actions will be restricted to inventory related actions. For a connector, you will be looking for an action with the form **Sync Data - <connector name>**. In our example this is **Sync Data - System Center Configuration Manager Inventory**, which includes the name that was set earlier in the Adding a Configuration Manager connector steps.
4. In our example, we also select to clear any existing data in the repository by checking the **Clean sync** checkbox.
5. Click **Execute** button in the **Execute action** popup to start the sync.
6. When the sync starts, a number of actions are queued to be performed on the selected repository. To check the progress of the sync actions:
   a. Navigate to the **Monitoring→Process log** page.
   b. Here you can see the sequence of actions that have been queued for the selected repository related to the **Sync Data** action selected. In the video, we speed up the process of synchronizing the data.
   c. When each action has finished running you'll see a check icon

      appear in the **Status** column if it succeeds or a failed icon

      if it fails . In our example, all the actions succeed.
7. Once all the actions have succeeded, you can check the results. To do this:
   a. Navigate to the **Monitoring→Sync log** page.
   b. This displays the items that have been added to the selected repository as a result of running the sync. In our example, you can see a number of additions have been made to the **Configuration Manager inventory** repository.

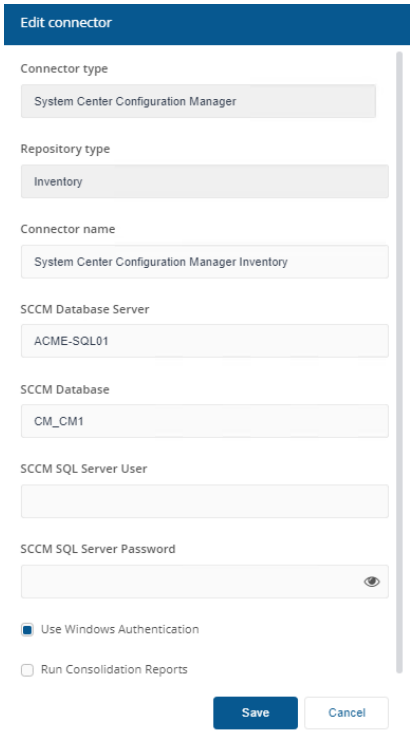
In the video we demonstrated the process of adding, testing and running a Configuration Manager connector and then monitored the progress of the sync and verified the results.

1.7.2.1.14.1.2 The Configuration Manager connector parameters

The following fields are available in the **Add connector** and **Edit connector** popups when the **System Center Configuration Manager Connector type** is selected, as shown in the picture opposite:

Field	Description
Connector type	Shows the connector type: **System Center Configuration Manager**.
Repository type	Shows which type of repository the connector works with. For the **System Center Configuration Manager Connector type** this is always **Inventory**.
Connector name	Here you set the logical name for the connector. **Tip** You should use a naming convention for connector names: **<connector type> <scope> <RCR>** **Scope** describes where data is coming from or what it's being used for. For example Demo, Test, Lab, Q2 Audit. Include **RCR** in the name if you have enabled **Run Consolidation Reports**.
SCCM Database Server	The name of the SQL Server instance where the Configuration Manager database is installed. For example **ACME-SQL01**. The SQL Server instance should be specified using one of the following formats: • **<Server Name>** • **<Server Name>\<Instance>** - for a named instance • **<Server Name>\<Instance>,Port** - for a custom port
SCCM Database	The name of the Configuration Manager database. For example **CM_CM1**.
SCCM SQL Server User	The name of an SQL login account. This is ignored if the **Use Windows Authentication** checkbox is checked.
SCCM SQL Server Password	The password for the SQL login account. This is ignored if the **Use Windows Authentication** checkbox is checked.
Use Windows Authentication	Check this box if you want to use the **Tachyon server's computer$ account** instead of a SQL login specfied above. When the connector is configured to use **Windows Authentication**, the connector is actually using the **SLA Platform Integrate Agent** service account.

Field	Description
	Tachyon Setup configures this service to use **Network Service** which translates as the **Tachyon server's computer$ account** on a remote server.
Run Consolidation Reports	Check the **Run Consolidation Reports** checkbox if you want consolidation actions to be processed each time the **Sync Data** action is executed for the connector. This can lead to unnecessary processing if you enable this on more than one connector. The recommended method of processing consolidation actions is to schedule the action **Generate Report - Basic Inventory Consolidation** to execute after the **Sync Data** actions have run for all connectors. This will execute the remaining consolidation actions. Alternatively check the **Run Consolidation Reports** checkbox on one of your connectors. You can view action processes in **Settings→Process log**.



1.7.2.1.14.2 Configuration Manager site configuration

The following **Client Settings** must be configured to gather inventory and usage data from clients, and applied to relevant Collections containing in-scope devices:

- Software metering (metering rules are not necessary)
- Software inventory
- Hardware inventory

The following **Discovery Methods** must be configured to gather Active Directory data about clients, and applied to relevant Domains and OUs containing in-scope devices:

- Active Directory System Group Discovery (default attributes are sufficient)

1.7.2.1.15 Tachyon connector

Connects the Tachyon and SLA components to support **Management group** and **Tachyon Powered Inventory** features. The **Tachyon Powered Inventory** feature uses instructions to fetch inventory data from clients and is a prerequisite for **Patch Success**.

This configuration procedure assumes you will always use this Connector to synchronize **Management groups**, and optionally import data for the **Tachyon Powered Inventory** feature.

The following steps are always required:

- Create a Tachyon user, in our examples this user is **ACME\SLATACHYON**
- Add the **Tachyon Connector** and configure it to use the above user and password, and the correct Consumer URL
- Test the connector
- Schedule the Tachyon Connector Sync Data action to run every 24 hours using the **Default Inventory** repository.

The following steps are additionally required if intending to use the **Tachyon Powered Inventory** feature:

- Assign the above Tachyon user to the **All Instructions Questioner** role
- Create an instruction set called **1E Inventory**, and upload its instructions
- Create a custom role called **1E Inventory Questioners**, assign questioner permission on the instruction set, assign it to All Devices, and add the Tachyon user as a role member.

To understand synchronization, please refer to How Management Group Synchronization works. For information about how to configure and use Management Groups please refer to Management Groups page.

Tachyon Powered Inventory is used to populate an inventory repository with inventory and usage data by using instructions that collect data from clients. It is required by the Patch Success application. For details of how these instructions are used, please refer to How Tachyon Powered Inventory works.

1.7.2.1.15.1 Prerequisites

Before adding the Tachyon connector, you will need the following:

- A **domain user account** dedicated for use by the Tachyon connector, that will be configured as a Tachyon user
  - This is effectively like a service account. In our examples, this is **ACME\SLATACHYON**
  - The account will be assigned to the Role **All Instructions Questioner**

- A user with **Full Administrator** role permissions, to configure the connector and related tasks.

If the connector is to be used to support the **Tachyon Powered Inventory** feature then you will also need:

- The Creating the 1E Inventory instruction set for Inventory instructions used to get data from Tachyonclients
- An appropriate Tachyon License details to permit using Tachyon connector inventory instructions. This is normally included in a standard Tachyon license.

Note

The **Tachyon Powered Inventory** feature is a prerequisite for **Patch Success**.

1.7.2.1.15.2 Creating the user

These steps create the user required by the TachyonConnector and assigns it to the **All Instructions Questioner** system role.

You need a **domain user account** in Active Directory, in our example this is **ACME\SLATACHYON**.

1. Logon to the Tachyon Portal using a user account with a **Full Administrator** role.
2. Open the **Settings** application.
3. Navigate to the **Settings→Permissions→Users and Groups** page.
    a. Click on the **Add** button, doing this displays the **Add user** popup.
    b. In the **Select user** field, type the name, or part of the name, for the Active Directory user or security group that you want to add. A list of matching names will be retrieved from Active Directory and displayed as you type, these are filtered so that users or groups that have already been added do not appear.
    c. Select the Active Directory user or security group from the list of matching names displayed in the drop-down list. In our example, this is **ACME\SLATACHYON**.
    d. Click **Add**.
4. On the **Settings→Permissions→Users and Groups** page, click on the user's name link for **ACME\SLATACHYON**.
    a. On the **User: SLATACHYON** page click the **Edit** button to display the **Edit roles assigned to user** popup.
    b. Select **All Instructions Questioner**.
    c. Click the **Save** button.

1.7.2.1.15.3 Configuring the Tachyon connector

These steps add and test a Tachyon connector:

1. Navigate to **Settings→Configuration→Connectors**

2. Click on the **Add** button.
3. In the **Add connector** popup select the **Tachyon** type.
4. In **Connector name** enter a logical name for this connector.

   Tip

   You should use a naming convention for connector names:

   <connector type> <scope> <RCR>

   Scope describes where data is coming from or what it's being used for. For example Demo, Test, Lab, Q2 Audit.

   Include **RCR** in the name if you have enabled **Run Consolidation Reports**.
5. In **URL**, enter the URL of the Tachyon consumer, in following format

   `https://<TachyonDNSAliasFQDN>/consumer`

   Tip

   Please note that, as stated above **/consumer** must be included in the URL, in the same way that **/Tachyon** needs to be added to <TachyonDNSAliasFQDN> when a Tachyon users browses to the Tachyon Portal.

   In our example, the URL is **https://tachyon.acme.local/consumer**
6. In **User Name**, enter the name of the **user** that has permission to run the Inventory instructions. For our example, this user is **ACME\SLATACHYON**.
7. In **Password**, enter the password for this account.
8. Leave the other fields empty.
9. Check the **Run Consolidation Reports** checkbox if you want consolidation actions to be processed each time the **Sync Data** action is executed for the connector.

   This can lead to unnecessary processing if you enable this on more than one connector. The recommended method of processing consolidation actions is to schedule the action **Generate Report - Basic Inventory Consolidation** to execute after the **Sync Data** actions have run for all connectors. This will execute the remaining consolidation actions. Alternatively check the **Run Consolidation Reports** checkbox on one of your connectors. You can view action processes in **Settings→Process log**.
10. Click **Add**.

You should then test the connector:

1. Select the connector you want to test from the list of **Connectors** bychecking the box at the left-hand end of the connector's row.
2. Click the **Test** button.
3. The **Test status** column for the connector will display a clock icon

indicating that the test has been queued for executing.

4. If the test succeeds **Test status** will display a check icon

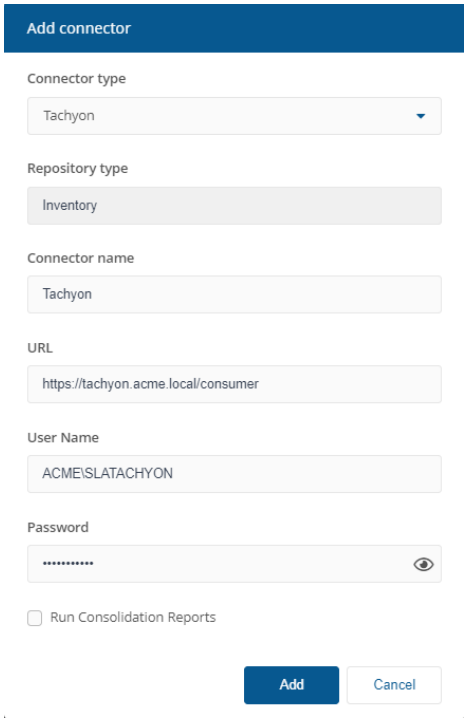
   and the **Last tested** column will display the date and time the test succeeded.

5. If the test fails the **Test status** will display a failed icon

   and you'll need to check the details you entered for the connector.

Tip

If you have access to the Process log you can see an entry for the Test action.



1.7.2.1.15.4 Creating the 1E Inventory instruction set

These steps are only required if:

- you have not already loaded the **1E Inventory** Product Pack using the Tachyon Product Pack Deployment Tool as part of the Tachyon Setup process
- you will be using **Powered Inventory**

The steps show how to create an instruction set called **1E Inventory**.

The **1E Inventory** instruction set will contain the 5 instructions listed in the following table:

<table>
<tr><th>Instruction text (ReadablePayload)</th><th>Type</th><th>Description</th><th>Data to Sync category</th><th>Instruction file name</th><th>Version</th></tr>
<tr><td>Which processors are in the device? With a stagger of <limitSecs> seconds.</td><td>Question</td><td>Processor details

Uses Device.GetProcessors method.

Note
Click here to expand details of data collected...

<table><tr><td>Method</td><td>GetProcessors</td></tr><tr><td>Library</td><td>Core</td></tr><tr><td>Action</td><td>Retrieves information about the CPUs plugged in to the motherboard of the device.</td></tr><tr><td>Parameters</td><td>(None)</td></tr><tr><td>Return values</td><td>Vendor (string): The vendor of the processor

Name (string): The vendor-defined name of this processor package

CoreCount (int): The number of cores inside this package

SpeedMhz(int): The clock speed of the processor in its current operating mode</td></tr></table></td><td>Processor</td><td>1E-Inventory-Device-GetProcessors</td><td>3</td></tr>
</table>

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		From v5.1 onwards these columns also appear : *LogicalCoreCount* (int) : The number of logical cores inside this package *Hyperthreading* (bool): Indicates whether the cores are hyperthreaded, true for yes, false for no.			
	Example	`Device.GetProcessors();`			
	Platforms	• Windows • Linux • MacOS • Solaris Intel • Solaris Sparc			
	Notes	*Name* is the immutable string that the CPU reports to SMBIOS. This often contains the publicly marketed and sold average speed of the CPU, which usually differs to the actual speed of the processor instance. *SpeedMhz* on Windows can change over time for one particular CPU.			

Instruction text (ReadablePayload)	Type	Description		Data to Sync category	Instruction file name	Version
			Modern CPU's can adjust their clock in response to heat and power from moment to moment. This parameter cannot be relied upon for scoping future instruction executions unless some kind of range of values is in the scope to cope with natural speed variance.			
Inventory - what is the summary of file usage since <startDate>? With a stagger of <limitSecs> seconds.	Question	Process Usage data inventory for SLA Uses the **$ProcessUsage_Daily** inventory table, if **Module.Inventory.ProcessUsage.Enabled** setting is true (default) in the 1E Client configuration file. Please refer to Settings for platform features of the 1E Client. **Note** Click here to expand details of data collected... Windows only. The following table shows fields available in the **$ProcessUsage_Daily** table.		Software Usage	**1E-Inventory-FileUsageSummary**	3

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version

Field	Data type	Description	Sample value	Tables
CommandLine	string	This is a string of	C:\Program Files\Git\mingw64\libexec\git-core\git-credential-manager.exe	

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		the command used to launch that instance,			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		most probably the first one. It will not co			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		n t a i n a n y d i f f e r e n c e s i f o t h e r i n s t a n c e s			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		arelaunchedwithhaslightlydifferentco			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		mandline. It is an indication of a typical			

Instruction text (ReadablePayload)	Type	Description				Data to Sync category	Instruction file name	Version
				command line for this instance.				
		Durati	integer	The enum	1			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
	on	error of minutes covered by the individual ex			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		execution(s) of at least one instance of thi			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		sexecutable. Duration cannever be more t			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		han1440minutes,beingthenumberofminu			

Instruction text (ReadablePayload)	Type	Description				Data to Sync category	Instruction file name	Version
				testing a day.				
		ExecutableHash	string	The MD5 hash of the binary that	ad3ec70ae9e82582bdf6aa6fd5811376			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		t c o n t a i n s t h e e n t r y p o i n t (u s u a l l y a n e x			

Instruction text (ReadablePayload)	Type	Description			Data to Sync category	Instruction file name	Version
		ExecutableName	string	The name of the binary that contains the		git-credential-manager.exe	

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		entrypoint to obtain ed from ms tamped ver si			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		on information where possible, the file n			

Instruction text (ReadablePayload)	Type	Description				Data to Sync category	Instruction file name	Version
				ameifnot.				
		ExecutableSize	integer	The size of the binary that is	131168			

Instruction text (ReadablePayload)	Type	Description				Data to Sync category	Instruction file name	Version
				ashedbelow				
		ExecutableVersion	string	The version information sta	1.5.0.0			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		mpedintotheexecutablewhereravailabl			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		e.			
	ExecutionCount	integer	The number of instances observed during the current execution.	2	

Instruction text (ReadablePayload)	Type	Description				Data to Sync category	Instruction file name	Version
				ngthe Duration period				
		IsOSProcess	integer	Avalueof1indica	0			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		testthatthisiscategorisedasanoperati			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		ngsystembytherulesinplaceeAvalueof0			

Instruction text (ReadablePayload)	Type	Description				Data to Sync category	Instruction file name	Version
				indicates that it is not.				
		LastSeen	integer	The UTC Time sta	1526982245			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		mpofwhenthelastinstanceoftheexecuta			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		b l e (o f a l l t h e a c c u m u l a t e d s u b j e c t s o f t h			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		is record) was last seen (polling) or actu			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		already existed (events). While stanc			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		eisrunning,forthecurrentdayrecords,			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		Last Seen will create pacross the day and dur			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		ationwillincreaseastimepassesifthep			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		rocessremainsrunning. Oncemidnightis			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		crossed the end the daily record s for ory yes ter			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		daysare'closedoff'bysettingLastSeen=			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		TS+864000(thenumberofsecondsinaday),			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		which is mid night of the next day. If all in			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		stancesofonebinaryarreexitedandneverer			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		running in that day, then the Last Seen field			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		d f o r t h a t d a i l y r e c o r d s h o u l d ' s t i c k ' a t o			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		never value and never revert change again. Inot			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		herwordsthemaximumdifferencebetween			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		TSandLastSeeninasinglerowisatmost86			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		400, being the number of seconds in a day.			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		Tracking of an execution summary from one			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		day to another ("carry-over") can be achi			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		evedbylookingforarecordbasedonTStom			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		or row = LastSeen today with all the other k			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		eyinformationthesameey. Ifthatexactkey			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		record with the 'carryover' conditionsi			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		snotfoundthenthepprocessdidnotthheore			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		tically continue across smidnight. Note t			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		hatapprocesstthatdiesafter23:59:00and			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		starts before 00:01:00 the next day will la			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		p p e a r t o b e a c o n t i n u o u s p r o c e s s i n t h e s u m			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		m a r y t a b l e s . E v e n t h o u g h i t c o u l d t h e o r e t			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		ically have stopped for near ly two minute e			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		s. This is is because the resolution of the eta			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		bleistothestartoftheminutetheeventto			

Instruction text (ReadablePayload)	Type	Description				Data to Sync category	Instruction file name	Version
				ccurredin.				
		TS	integer	When the record was added to	1526947200			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		hetable.SeeTimestamps.MidnightUTCth			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		atisthestartdayofthe24hourscoveredb			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		y t h i s r e c o r d .			
		The Tachyon client captures executable usage; this is from the moment the executable is turned into a process, hence the process usage. The Process Usage data presented is grouped by executable binary, and parallel runs are accumulated in the ExecutionCount, but not in the Duration, where coverage time period is desired instead.			
Inventory - what software is installed? With a stagger of <limitSecs> seconds.	Question	Software inventory for SLA Uses a combination of: • Software.GetInstallations method • Software.GetUserInstallations method • SQL Server registry values **Note** Click here to expand details of data collected...	Installed Software	**1E-Inventory-Software**	3

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		Method	**GetInstallations**		
		Module	Software		
		Library	Core		
		Action	Gets a list of the installed software available to all users, optionally filtered by product and/or publisher.		
		Parameters	*Product* (string; optional): If specified, search for just this product. *Publisher* (string; optional): If specified, get just this publisher's software.		
		Return values	A table of: • – *Product* (string): The product name. – *Publisher* (string): The publisher of the product. – *Version* (string): The		

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		version of the product. – *InstallDate* (string): If available, when the product was installed. – *Architecture* (string): Platform architecture of this installation (e.g. x86, x64)			

		Example
		Get all software:
		`Software.GetInstallations();`
		Find and remove all installed instances of Calculator Plus:
		`Software.GetInstallations( Publisher : "Microsoft", Product : "Microsoft Calculator Plus");`
		`evaluate;`
		`Agent.Echo( Message: "Is installed");`
		`Software.Uninstall( Publisher : "Microsoft", Product : "Microsoft Calculator Plus");`			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version

		To select a specific version, use a SQL WHERE clause:
		`@installs = Software.GetInstallations( Publisher : "Microsoft", Product : "Office Professional");`
		`SELECT DISTINCT * FROM @installs WHERE Version LIKE "16.0%";`			

		Platforms • Windows • Linux • MacOS • Solaris Intel • Solaris Sparc • Android			
		Notes To find additional software installed for specific users, use Software.GetUserInstallations.			
		Method **GetUserInstallations**			
		Li Core			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
	array				
	Action	Gets a list of the software installed for specific users, optionally filtered by product and/or publisher.			
	Parameters	*Product* (string; optional): If specified, search for just this product. *Publisher* (string; optional): If specified, get just this publisher's software.			
	Returnvalues	A table of: • – *Architecture* (string): Platform architecture of this installation (e.g. x86, x64) – *InstallDate* (string): If available, when the product was installed.			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		– *Product* (string): The product name. – *Publisher* (string): The publisher of the product. – *Sid* (string): The user identifier for whom this software has been installed. – *Username* (string): Friendly representation of the *Sid* - this will only be resolved locally. – *Version* (string): The version of the product.			
Example		Get all user specific software: `Software.GetUserInstallations();`			
Platforms		• Windows			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
	Notes	• *Sid* resolution may fail as this method will not go over the wire. In this case Username will be NULL. • The file modified and accessed time attributes of the NTUSER.dat directory entries under the %USERPROFILE% folder for each user and service principal might be updated to some time during the execution of this method. This is a side effect of loading and unloading the user hive and is housekeeping performed by Windows, not the 1E Client. This can cause "unused" profiles to appear to be used if the modified times are employed to determine whether a user has logged in, which is not a reliable method of establishing this fact. • This method reads user uninstall registry keys from HKU, but will not load hives. • Installs for this function are retrieved from *HKU:\<SID>\Software\Microsoft\Windows\CurrentVersion\Uninstall*			

<table>
<tr><th>Instruction text (ReadablePayload)</th><th>Type</th><th>Description</th><th>Data to Sync category</th><th>Instruction file name</th><th>Version</th></tr>
<tr><td>Inventory - summary of which users have logged on since <startDate>? With a stagger of <limitSecs> seconds.</td><td>Question</td><td>User data inventory for SLA

Uses the $UserUsage_Daily inventory table, if Module.Inventory.UserUsage.Enabled setting is true (default) in the 1E Client configuration file. Top Console User is also calculated from this table.

Please refer to Capture source settings.

Note
Click here to expand details of data collected...
Windows only. The following table shows fields available in the $UserUsage_Daily table.

<table><tr><th>Field</th><th>Datatype</th><th>Description</th><th>Sample value</th><th>Tables</th></tr><tr><td>Duration</td><td>integer</td><td>The enumerator</td><td>12</td><td>• $UserUsage</td></tr></table></td><td>User</td><td>1E-Inventory-UserUsageSummary</td><td>3</td></tr>
</table>

Instruction text (ReadablePayload)	Type	Description			Data to Sync category	Instruction file name	Version
			f m i n u t e s c o v e r e d b y t h e i n d i v i d u a l u s e r s	_ D a i l y			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		session(s) of at least one instance of this			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		login. Duration cannot be more than 144			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		0 minutes, being the number of minutes in a			

Instruction text (ReadablePayload)	Type	Description				Data to Sync category	Instruction file name	Version
		day.						
	Email	string	The email address that is cached in	abrown@acme.org	• $UserUsage_Daily			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		hesystemforthisuser.Thismaynotnecessarily			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		sarilybetheemailaddressstousetocconta			

Instruction text (ReadablePayload)	Type	Description				Data to Sync category	Instruction file name	Version
			c t t h e u s e r v i a c o r p o r a t e e m a i l .					
FirstNa	string	The fore	Alice	• $User Us				

Instruction text (ReadablePayload)	Type	Description			Data to Sync category	Instruction file name	Version
		name	name that the system has cached for the user	age_Daily			

Instruction text (ReadablePayload)	Type	Description			Data to Sync category	Instruction file name	Version
		r.					
		LastName	string	The surname that the system has cached	Brown	• $UserUsage_Daily	

Instruction text (ReadablePayload)	Type	Description					Data to Sync category	Instruction file name	Version
		for the user							
	LastSeen	integer	The UTC Timestamp of when the	1526990846	• $User_Usage_Daily				

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		last instance of the user session (of all t			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		h e a c c u m u l a t e d s u b j e c t s o f t h i s r e c o r d) w			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		last seen (polling) or actually existed			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		(events), rounded down to the start of the			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		minutes in which the event occurred. Whils			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		tanysessionisinprogress,forthecurre			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		ntdayrecordss, LastSeenwillcreepacros			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		s t h e d a y a n d t h e d u r a t i o n w i l l i n c r e a s e a s			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		timepassesiftheuserremainsloggedin.			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		That is Duration and Last Seen will increa			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		seeachtimeyouquerythetable(withatle			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		astaminutebetweenqueriess). Oncemidni			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		ghtiscrossedthenthedailyrecordsforry			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		esterdayare'closedoff'bysettingLast			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		Seen=TS+86400(thenumberofsecondsina			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		day), whichismidnightofthenextday. If			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		allusersessionsforoneuserareexited			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		and never occur again that day, then the last			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		stSeenfieldforthatdailyrecordshould			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		'stick' at one value and never ever change			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		again. Inotherwordsthemaximumdifferee			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		nceb etwe enTS and Last Seen inas ingle row			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		is at most 86400, being the number of seconds			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		daily. Tracking of auser sessions summ			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		array from one day to another ("carry-over"			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		) can be achieved by looking for a record dba			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		sedonTS tomorrow=LastSeen today with hal			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		l t h e o t h e r k e y i n f o r m a t i o n t h e s a m e . I f t h			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		atexactkeyrecordwiththe'carryover'c			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		ondition is not found the user sessi			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		ondidnotthheoreticallycontinueacross			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		midnight. Note that a session that a			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		after23:59:00andstartsagainbefore00:			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		01:00 the next day will appear to be a conti			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		nuoususerssessionintheesummarytables.			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		Event though it could the oretically have ven			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		not existed for near lytwo minutes. This is			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		because set the resolution of the table is to ot			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		the start of the minute the event occurred i			

Instruction text (ReadablePayload)	Type	Description				Data to Sync category	Instruction file name	Version
		n. SeeTimestamps.						
	SID	string	The Windows NT SID of type	S-1-5-21-xxxx-yyyy-z	• $UserUsage_Daily			

Instruction text (ReadablePayload)	Type	Description					Data to Sync category	Instruction file name	Version
				heuser.	zz				
		TS	integer	When the record was added to the	1526947200	• $UserUsage_Daily			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		able. See Timestamps.			
	Username	string	The user account name.	alice bacme\Alice B	• $UserUsage_Dai

Instruction text (ReadablePayload)	Type	Description				Data to Sync category	Instruction file name	Version
			ame, with a domain prefix if applicable.	rown	ly			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		For Windows devices not a in a domain, the '			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		domain' is the local machine name. For non			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		-Windowsdevicessuchas Linuxthereisno			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		domain part. The Tachyon client captures user sessions (usage); this is from the moment the user instigates a login/logout, hence User Usage. The usage data presented is grouped by SID and Username, and parallel login durations are really the coverage of the time period, not the total time for all the individual sessions. User and administrator accounts are included, either local or remote. System accounts, and accounts used to run services, are excluded.			
Returns patch status for 1E Inventory consumption, staggering for <limitSec	Question	Returns patch status for 1E Inventory consumption	Patch	**1E-PatchSuccess-PatchStatus**	5.0

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
s> seconds.					
Tip The **1E-PatchSuccess-PatchStatu**					

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
s i n s t r u c t i o n i s n o t r e q u i r e d i f y o u d o n o t					

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
intendtousethePatchSuccessapplicati					

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
on, and will not run unify you do not have valid ice					

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
nsforPatchSuccess.Formoreinformati					

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
onaboutconfiguringPatchSuccessplleas					

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
e r e f e r t o C o n f i g u r i n g P a t c h S u c c e s s . **W a r n i**					

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
ng This instruction is part of this **1E** **Inv**					

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
entory instructionsetusedbythetachyo					

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
nConnector.Do not move it to the **1E Patch**					

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
Success instructions set used by the bubutt					

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
onsvisibleinthePatchSuccessapplicat					

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
ion.					

Tip

You can use the Product Pack Deployment tool to simultaneously Upload the instructions and Create the Instruction set, or use the manual steps below.

These instructions are included in the **1E Inventory** product pack, available in the **TachyonPlatform.vx.x.x.x.zip** file downloaded from the 1E Support Portal.

1.7.2.1.15.4.1 Upload the instructions

First upload the instructions:

1. Download the **TachyonPlatform.v8.x.x.x.zip** file from the 1E Support Portal
2. Extract the **1E-Inventory.zip** from the Classic folder
3. Logon to the Tachyon Portal using a user account with the **Full Administrator** role.
4. Open the **Settings** application.
5. Navigate to the **Settings→Instructions→Instruction sets** page.
6. Click on the **Upload** button.
7. In the Open dialog, navigate to the location of the **1E-Inventory.zip** file.
8. Select **1E-Inventory.zip** and click **Open**.

1.7.2.1.15.4.2 Create the Instruction set

All the instructions contained in the zip file will initially be added to the default **Unassigned** instruction set. Instructions in the **Unassigned** instruction set cannot be used, so first you will need to create a new instruction set with the verification instructions.

1. Select the **5** instructions you want to add to the new set, by clicking the checkbox at the start of each instruction row in the list.
2. Click the **Add new set** button in the button panel to the right of the page.

3. In the **Add new instruction set** popup subsequently displayed, and type:
    a. **1E Inventory** as the name.
    b. **Tachyon portalPowered Inventory** as the description.
4. Ensure that the **Include 5 selected instructions** checkbox is checked.
5. Click the **Add** button to add the new instruction set, with the selected instructions.

1.7.2.1.15.4.3 Configure the Tachyon Connector

Follow the steps in Configuring the Tachyon connector and then return to Executing the Tachyon Connector Sync Data action.

1.7.2.1.15.5 Executing the Tachyon Connector Sync Data action

When you've finished setting up the connector, you will then need to synchronize it to populate an inventory repository with the data from Tachyon.

You can execute the Connector **Sync Data** action in the same way as other connectors, manually or using a schedule, however the Tachyon connector manages its actions differently to other connectors. It uses Tachyon instructions to collect data from the client, once every 24 hours.

First, you should run the Sync Data action manually to confirm it works, in particular to test the user permissions and its ability to run the instructions.

- To manually sync data, please refer to Execute a connector sync action.
- To schedule the sync data action, please refer to Schedules page.

For our example, you will be running the **Sync Data - Tachyon** action on the default inventory repository called **Default inventory**. You can select which **Data to Sync**. The data categories displayed are dependent on the type of connector. For Tachyon, you can select from the following:

- Device
- Installed Software
- Processor
- User
- Patch
- Software Usage

Note

Each data category corresponds to one of the inventory instructions. Each instruction runs once every 24 hours, for 24 hours, collecting data if the device is online, or comes online during that period.

The exception is the **Device** category, which does not run an instruction, but instead it gets device data directly from the TachyonMaster database. To use

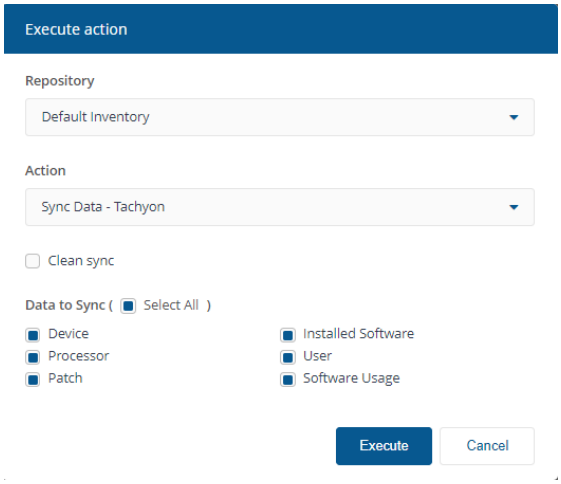
Management Groups in client-based applications (Explorer, Experience and Guaranteed State) you must use the **Default Inventory** repository, and select **Device** data.

Warning

When you schedule the **Sync Data - Tachyon** action to run automatically instead of manually, ensure you do *not* schedule it to run more frequently than the duration for the 1E Inventory instructions, that is every 24 hours. To understand why, please refer to How Tachyon Powered Inventory works.

You can review the results as they come in by reviewing the instruction history.

1. Switch to the **Explorer** application.
2. Navigate to the **Instructions→History** page.
3. Observe that all 5 instructions are running with a duration of 1440 minutes. Any devices coming online during that period will respond.
4. Click on any of the 5 instructions to review the response content and status.



If you want to review in detail the data that was imported into the **inventory repository**, navigate to the **Inventory** Application pages:

1. The **Inventory→Hardware→Hardware Inventory** page shows software details retrieved from the devices that have Tachyon clients.
2. The **Inventory→Hardware→Device** page shows hardware and OS details for devices that have Tachyon clients.
3. The **Inventory→Software Inventory→Product Usage** page shows the software product usage that has been retrieved from devices that have Tachyon clients.

The above data from Tachyonclients may be consolidated with data from other inventory sources using their inventory connectors.

1.7.2.1.15.6 How Management Group Synchronization works

The SLA components are responsible for storing information about management groups, including group definitions and membership, in the SLA databases. Tachyon maintains a synchronized copy in the TachyonMaster database. Whenever SLA Engine evaluates group membership, and it detects changes in the **Default Inventory** repository, it notifies Tachyon by initiating a sync. The Coordinator service receives the sync, fetches the changes, and updates the TachyonMaster database. To contact Tachyon, the SLA Engine uses the URL of the **Consumer** defined in the Tachyon Connector and the **Network Service** account is a member of the **Full Administrator** role.

Membership evaluations occur whenever the **Default Inventory** repository is updated by a manual or scheduled Connector **Sync Data** action, or the **Evaluate** button is pressed, as described in the Management Groups page.

1.7.2.1.15.7 How Tachyon Powered Inventory works

1.7.2.1.15.7.1 1E Inventory instructions

The Tachyon connector works differently compared with other connectors. Other connectors import data in a single operation, whereas a **Tachyon connector sync** issues a set of instructions, and then runs a two-phase process to gather the data. The default gather period behavior is controlled using settings for the inventory repository in the SLA-Data database. These must not be changed unless otherwise instructed by 1E.

When a Tachyon connector sync is actioned, either manually using **Create a new action**, or as a scheduled sync, the following happens.

1. The SLA Engine polls Tachyon to retrieve the information that is routinely sent back by the connected devices
2. The SLA Engine asks Tachyon to run each instruction
   - Each instruction runs for **1440** minutes (24 hours), known as a **gather period**
   - Tachyon sends each instruction to all devices at the same time
   - Devices respond immediately if they are online, or catch-up shortly after coming online
   - Each device will respond only once to each instruction during the **gather period**
   - Each instruction has a short random delay before the device sends its response back to the Tachyon server
   - Responses are stored in the database and only deleted at the end of the **gather period** plus a 6-hour **keep period**
3. The SLA Engine polls Tachyon
   - The poll is every **360** minutes (6 hours) after starting the instruction run for 24 hours, and fetches all the responses gathered so far
   - Data is stored in the inventory repository, and kept after the Tachyon deletes its copy of the data.

Devices only appear in the inventory repository if they respond, or if they have responded earlier to a previous sync.

Tachyon has minimal impact on the network and client devices when the instructions are run and responses are sent back to the Tachyon server. The low impact is further reduced by the random delay used by each instruction.

During each poll there is a small performance impact on the Tachyon server (master stack) and SLA components, when the initial responses are processed, and when the deltas are processed for subsequent polls, for other machines coming online.

1.7.2.1.15.7.2 How to schedule your Tachyon connector syncs

This is not a precise science, but here are some points you might want to consider when deciding what schedule you want to set for your Tachyon connector syncs:

- As we've described under 1E Inventory instructions, the instructions run for 24 hours and poll all the devices that are connected to Tachyon during that time
- Avoid creating overlapping sync schedules for an inventory repository - use only one Tachyon connector per inventory repository and sync it once every 24 hours
- Because of the 24-hour instruction TTL, the Tachyon connector sync allows time for devices in different time zones to be online and connected
- The information related to a device is updated just once during the sync period. Any updates will be captured during the next sync period.

1.7.2.1.15.7.3 Tachyon client configuration

Process and User usage capture is available only on Windows devices.

The 1E Client is required, with the following Tachyon client features enabled:

- Module.Inventory.Enabled=true (default, and this setting is visible in the 1E Client configuration file)
- Module.Inventory.ProcessUsage.Enabled=true (default - in 3.3 this was also true by default, but in 4.0 it was false by default)
- Module.Inventory.UserUsage.Enabled=true (default)

For more detail about configuring these and other settings in 1E Client, please refer to Tachyon client settings.

1.7.2.1.15.7.4 Tachyon License details

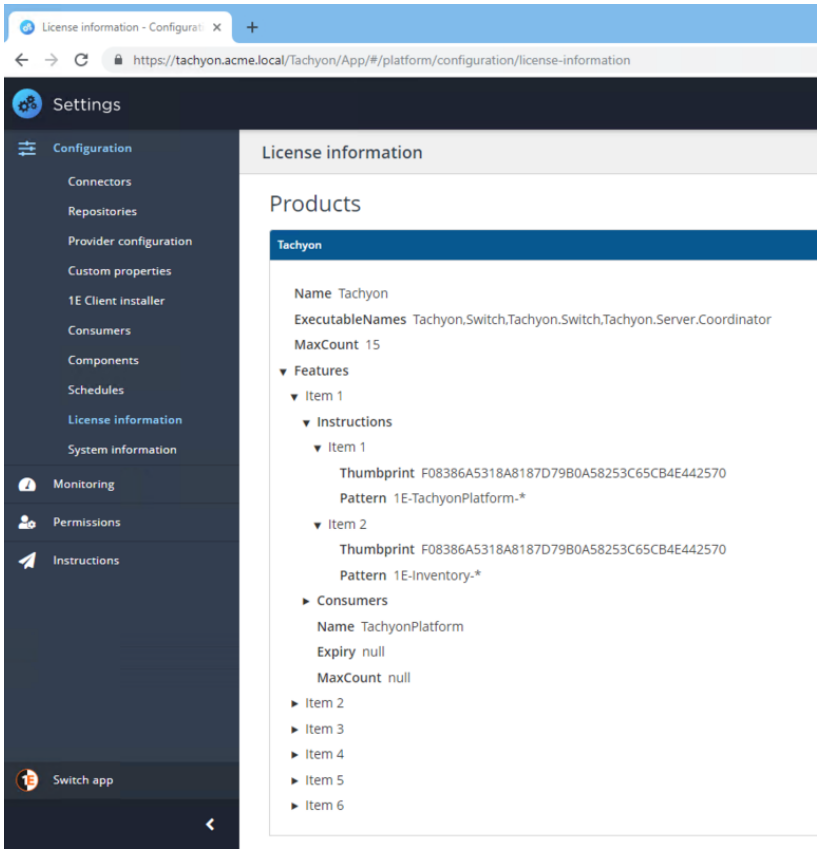
Ensure your Tachyon License file has the Inventory consumer enabled and includes the pattern for **1E-Inventory-***

You can view your Tachyon license details using either of the following methods:

- in the Settings Application, under **License info**, look in the Products section and expand Features and instruction items
- in the license file **Tachyon.LIC** found in **C:\ProgramData\1E\Licensing**

If the pattern does not exist, then the **1E-Inventory** instructions will not run. You may have an old version of Tachyon, or your license needs to be updated.

```
   <Features>
      <Feature name="TachyonPlatform">
        <Consumer name="Inventory" enable="on"></Consumer>
        <Instructions signersha="F08386A5318A8187D79B0A58253C65CB4E442570" patt
ern="1E-Inventory-*"> </Instructions>
        ...
      </Feature>
      ...
      ...
      ...
    </Features>
```



1.7.2.1.16 vCenter connector

Connects to a vCenter server and pulls in inventory data.

Before adding a new vCenter connector, you will need the following:

- Install VMware PowerCLI
- A vCenter user account and password.

1.7.2.1.16.1 vCenter connector configuration

To add the vCenter connector:

1. In **Connector name** enter a logical name for this connector.

   Tip

   You should use a naming convention for connector names:

   <connector type> <scope> <RCR>

   Scope describes where data is coming from or what it's being used for. For example Demo, Test, Lab, Q2 Audit.

   Include **RCR** in the name if you have enabled **Run Consolidation Reports**.

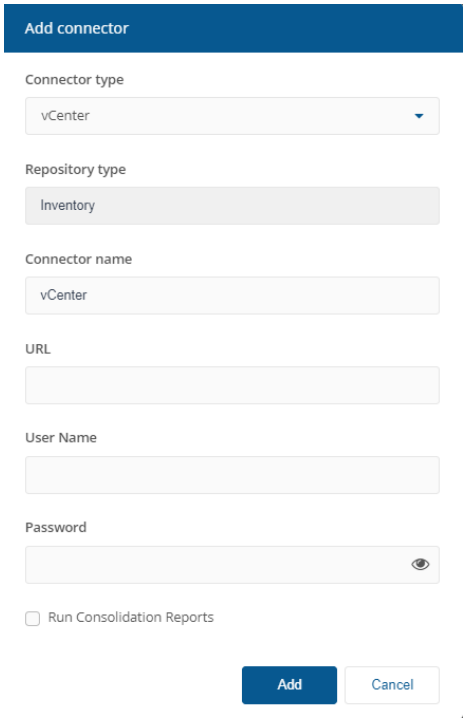
2. In **URL** enter location of vCenter server with **\sdk** appended.
3. In **User Name** enter the name of the account you want to use to connect to the database.
4. In **Password** enter the password for this account.
5. Check the **Run Consolidation Reports** checkbox if you want consolidation actions to be processed each time the **Sync Data** action is executed for the connector.

   This can lead to unnecessary processing if you enable this on more than one connector. The recommended method of processing consolidation actions is to schedule the action **Generate Report - Basic Inventory Consolidation** to execute after the **Sync Data** actions have run for all connectors. This will execute the remaining consolidation actions. Alternatively check the **Run Consolidation Reports** checkbox on one of your connectors. You can view action processes in **Settings→Process log**.

6. Click **Add**.

After adding the connector, please refer to:

- Test a connector - to test the connector configuration
- Execute a connector sync action - to actually sync data into a repository
- Delete a connector



1.7.2.1.16.2 VMware PowerCLI

VMware PowerCLI 11.1.0 (code.vmware.com/web/dp/tool/vmware-powercli/11.1.0) must be installed on the Tachyon Master server (where the SLA Integrate Services Agent service is hosted) before you can configure and use the vCenter connector. Earlier or later versions of PowerCLI are not supported and may cause errors. VMware PowerCLI is freeware and was previously known as vSphere PowerCLI.

VMware PowerCLI supports multiple versions of VMware vCenter Server. For details, please refer to the VMware compatibility matrix using the following link:
https://www.vmware.com/resources/compatibility/sim/interop_matrix.php#interop&2=&106=

1.7.2.1.17 Windows Server Update Services connector

Connects to a WSUS database and pulls in patch data.Before adding a new Windows Server Update Services connector, you will need the following:

- a SQL Login for the WSUS database, if not using Network Service (computer$).

Warning

This connector only supports WSUS that has been configured to use an external SQL database via TCP/IP protocol. Named Pipes protocol is not supported, as required by internal MSSQL$MICROSOFT##WID database instance.

1.7.2.1.17.1 Windows Server Update Services connector configuration

1. In **Name**, enter a logical name for this connector.

Tip

You should use a naming convention for connector names:

<connector type> <scope> <RCR>

Scope describes where data is coming from or what it's being used for. For example Demo, Test, Lab, Q2 Audit.

Include **RCR** in the name if you have enabled **Run Consolidation Reports**.

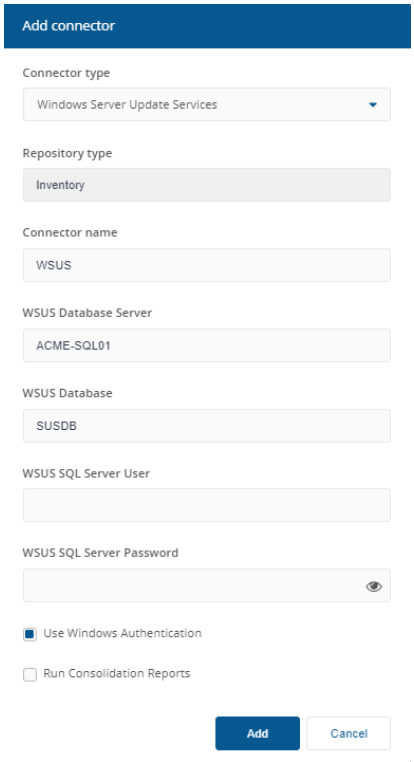
2. In **WSUS Database Server**, enter the name of the SQL Server instance where the Configuration Manager database is hosted using one of the following formats:
   - **<Server Name>**
   - **<Server Name>\<Instance>** - for a named instance
   - **<Server Name>\<Instance>,Port** - for a custom port
3. In **WSUS Database**, enter the name of the database you want to connect to.
4. If you are authenticating with Windows:
   a. Ensure **Use Windows Authentication** is checked.
   b. You do not need to populate the WSUS SQL Server User and WSUS SQL Server Password fields.
5. If you are authenticating with a SQL login:
   a. Ensure **Use Windows Authentication** is unchecked.
   b. In **WSUS SQL Server User**, enter the name for the account you want to use to connect to the database.
   c. In **WSUS SQL Server Password**, enter the password for this account.
6. Check the **Run Consolidation Reports** checkbox if you want consolidation actions to be processed each time the **Sync Data** action is executed for the connector.

   This can lead to unnecessary processing if you enable this on more than one connector. The recommended method of processing consolidation actions is to schedule the action **Generate Report - Basic Inventory Consolidation** to execute after the **Sync Data** actions have run for all connectors. This will execute the remaining consolidation actions. Alternatively check the **Run Consolidation Reports** checkbox on one of your connectors. You can view action processes in **Settings→Process log**.
7. Click **Add**.

The following fields are available in the **Add connector** and **Edit connector** popups when the **Windows Server Update Services Connector type** is selected, as shown in the picture opposite:

Field	Description
Connector type	Shows the connector type: **Windows Server Update Services**.

Field	Description
Repository type	Shows which type of repository the connector works with. For the **Windows Server Update Services Connector type** this is always **Inventory**.
Connector name	This lets you set the Connector name. **Tip** You should use a naming convention for connector names: **<connector type> <scope> <RCR>** **Scope** describes where data is coming from or what it's being used for. For example Demo, Test, Lab, Q2 Audit.
WSUS Database Server	The name of the SQL server instance where the WSUS database is installed. For example **ACME-SQL01**.
WSUS Database	The name of the WSUS database. For example **SUSDB**.
WSUS SQL Server User	The name of an SQL login account. This is ignored if the **Use Windows Authentication** checkbox is checked.
WSUS SQL Server Password	The password for the SQL login account. This is ignored if the **Use Windows Authentication** checkbox is checked.
Use Windows Authentication	Check this box if you want the **1E SLA Platform Integrate Agent** service account and not a specific SQL login account to be used to access the WSUS database. The **1E SLA Platform Integrate Agent** service account is Network Service by default.
Run Consolidation Reports	Check the **Run Consolidation Reports** checkbox if you want consolidation actions to be processed each time the **Sync Data** action is executed for the connector. This can lead to unnecessary processing if you enable this on more than one connector. The recommended method of processing consolidation actions is to schedule the action **Generate Report - Basic Inventory Consolidation** to execute after the **Sync Data** actions have run for all connectors. This will execute the remaining consolidation actions. Alternatively check the **Run Consolidation Reports** checkbox on one of your connectors. You can view action processes in **Settings→Process log**.



1.7.2.2 Repositories page

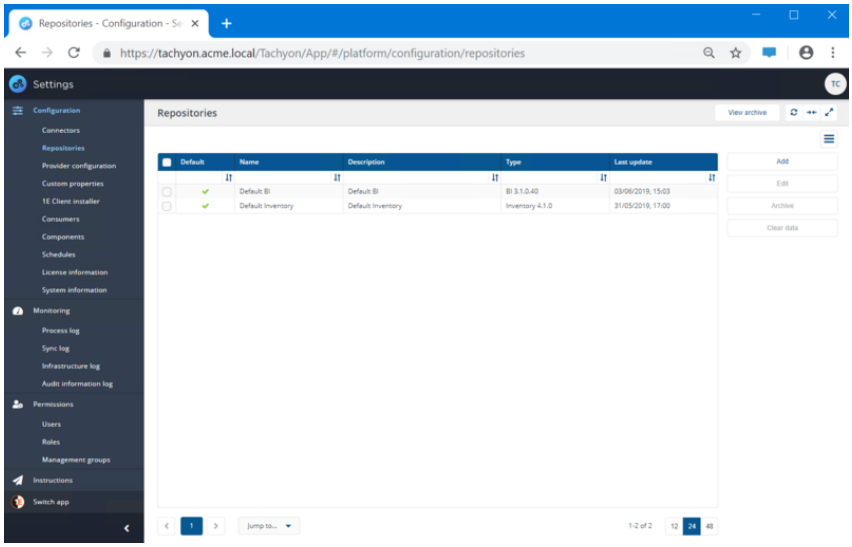
Repositories are used by applications to process and store information. Tachyon provides an Inventory repository out-of-the-box. Some consumer applications provide their own types of repositories.

Repository types	Used by	Used for
Application Migration	• Application Migration	Migration rules.
Business Intelligence	• Patch Success	Patch data for Patch Success.
Compliance	• AppClarity	Compliance data for AppClarity. Reclaim policies and history.
Entitlement	• AppClarity	Entitlements for AppClarity.
Inventory	• Inventory • AppClarity • Application Migration	Hardware and software inventory for devices. Optionally stores associations between Catalog products and Configuration Manager packages and applications.

Repository types	Used by	Used for
	• Patch Success	

A default repository is provided for each type of repository. You cannot delete a repository but you can change its details, clear its data or archive it. You can add further repositories for each type.

Repositories are populated using Connectors page which are executed either manually or on schedule, and data is then processed by applications. In some cases you can manually enter data.



1.7.2.2.1 Adding a new repository

Go to **Settings → Configuration → Repositories**

Adding a new repository

1. Click on the **Add** button.
2. In the **Add repository** popup enter the details for the new repository.
3. Enter a suitable **Name** for the repository this must not match any existing repository.
4. Select the **Repository type**.
5. Enter a suitable description for the new repository.
6. If you want the new repository to be the default for the selected **Repository type** then check the **Default repository** checkbox, otherwise leave this unchecked.
7. When all the settings have been made click **Add** to create the repository.

Tip

You should use a naming convention for repository names:

<scope> <repository type>

Naming with **scope** first makes it easier to know which repository you are using. The name of the **repository** you are currently using is visible in a drop-down list at the top of pages in the user interface.

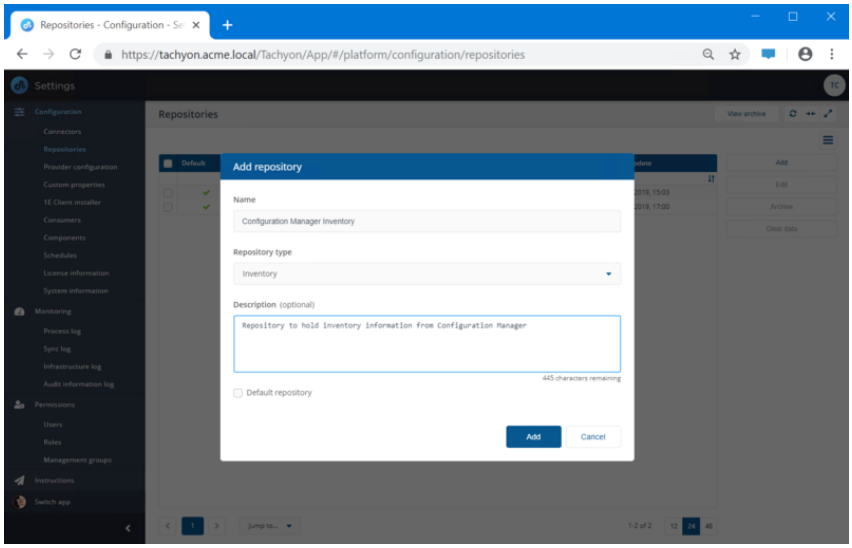
Including the **repository type** in the name helps when creating an action or schedule.

1.7.2.2.1.1 Changing the name of a repository

1. Select a repository and click **Edit**
2. In the **Edit repository** popup change the Name
3. Change the description if required.
4. If you want the repository to be the default for the selected **Repository type** then check the **Default repository** checkbox, otherwise leave this unchecked.
5. Click **Save**.

1.7.2.2.1.2 Setting the default repository

1. Select a repository, for example **Configuration Manager Inventory** and click **Edit**.
2. In the **Edit repository** popup check the **Default repository** checkbox and click **Save**.
3. Confirm the repository is listed as Default for its repository Type.
4. From this point on all pages that show information from an inventory repository would show the **Configuration Manager Inventory** by default. You can still change the repository for a particular page by clicking on the repository selector at the top-right of the page.
5. If you no longer wish a repository to be the default, then you must choose another repository instead.



Tip

Repositories are useful when you want to segregate different types of data. For example, you could have one inventory repository for Configuration Manager inventory data, and another one for BigFix data. Alternatively, you can have connectors to

different inventory sources pushing data into one repository. Any Management Groups that you create will span all the repositories you have.

Note

Once you've created a new repository you cannot delete it. You can only change its details, clear its data or archive it.

The name of a repository must be unique, but can be changed.

Setting a repository as the default repository means it is used as the default on certain screens.

1.7.2.2.2 Clearing data from a repository

This will reset all the data for a particular repository, which resets all the synced data imported by all/any of the connectors synced for that repository.

Note

We recommend you only use **Clear Data** under the following circumstances:

- If the data in a repository is no longer needed you can clear its data to free up space in the database.
- If you created connectors and associated them with the wrong repository and ran a synchronization action which returned inaccurate data
- If the data source was corrupted and the synchronization returned unreliable data
- If the synchronization failed after a partial completion

Warning

When you run **Clear Data**, scheduled or manual synchronization actions cannot take place. If there are existing background synchronization actions running, you will be notified when you attempt to reset your data.

Once you start a **Clear Data** action, do not cancel the process – when the deletion starts, existing data will lose its integrity and will no longer be reliable.

To **Clear Data**:

1. From the list of repositories, locate the active repository you want to clear the data from.
2. Check the box at the left-hand end of the repository's row.
3. Click the **Clear data** button.
4. In the **Clear data from repository** popup you will be asked if you want to proceed to clear the selected repository.

Note

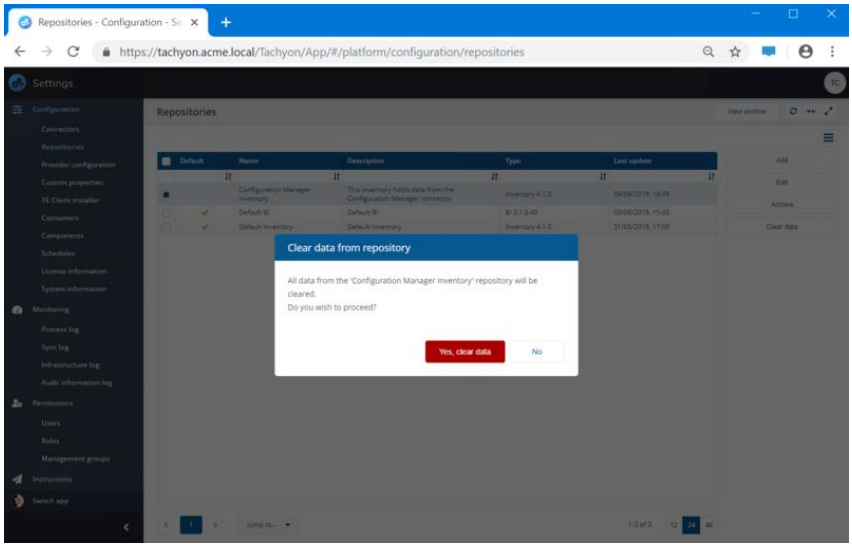
If you click the **Yes, clear data** button all the data held in the repository will be lost and cannot be retrieved.

5. Click the **Yes, clear data** button to empty the repository.
6. The repository will then be cleared.

Note

If you only want to clear data for a specific connector then use the **Clean Sync** action:

- Execute a connector sync action
- Execute an action



1.7.2.2.3 Archiving repositories

Repositories cannot be deleted. When you no longer need a repository you can archive it. It's not deleted and can still be restored for future use.

Note

When you archive a repository you should be aware that any currently defined schedules that populate or process its data will still be active. You should disable these before archiving.

1.7.2.2.3.1 Archiving an existing active repository

To archive an active repository:

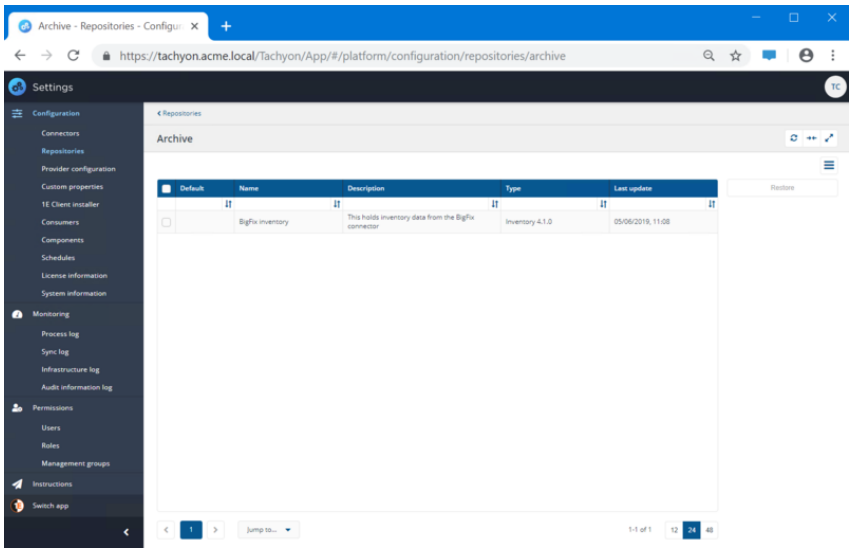
1. From the list of repositories, locate the active repository you want to archive.
2. Check the box at the left-hand end of the repository's row.
3. Click the **Archive** button.
4. In the **Archive repository** popup you will be asked if you want to proceed to archive the selected repository.
5. Click the **Yes, archive repository** button to archive it.

6. The repository will then be archived

1.7.2.2.3.2 Viewing the archived repositories

To view the archived repositories:

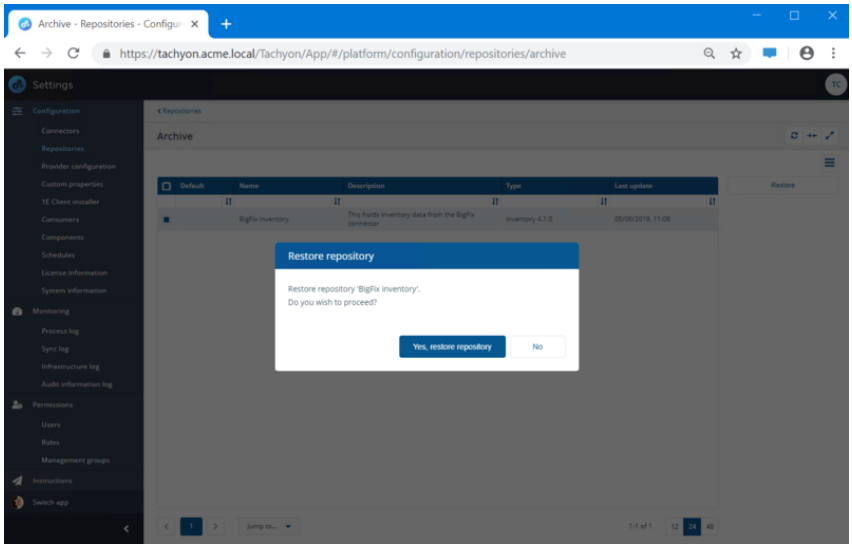
1. Click the **View archive** button.
2. The page will change to the **Archive** showing any repositories that have been archived.
3. To navigate back to the default Repositories page click on the **<Repositories** link at the top of the page.



1.7.2.2.3.3 Restoring archived repositories

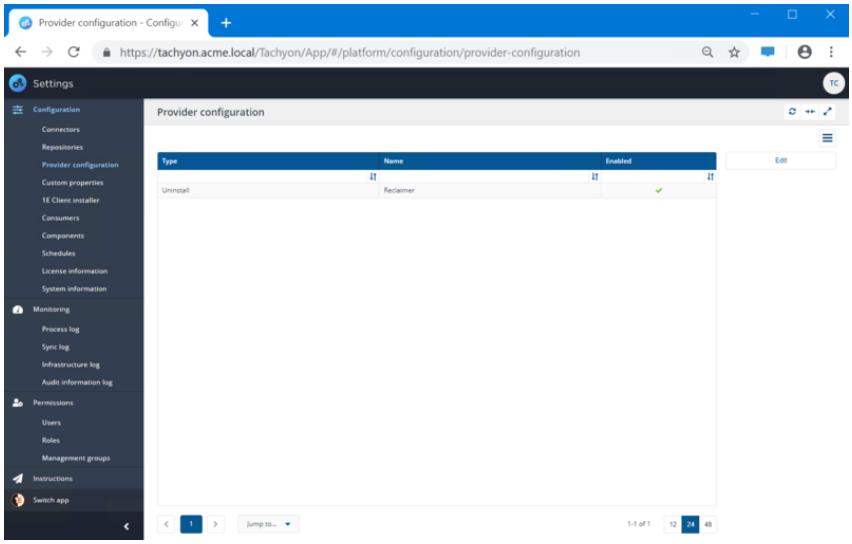
To restore a previously archived repository:

1. From the **Archive** page locate the archived repository you want to restore.
2. Check the box at the left-hand end of the repository's row.
3. Click the **Restore** button.
4. In the **Restore repository** popup you will be asked if you want to proceed to restore the selected repository.
5. Click the **Yes, restore repository** button to restore it.



1.7.2.3 Provider configuration page

Providers can be used by applications to leverage external tools to perform specific operations. For example the reclaim provider enables software to be uninstalled, thereby extending the functionality of the platform to include uninstallation.



1.7.2.3.1 Provider configuration table

The columns in the table are described below:

Column	Description
Type	This indicates the type of the provider. For example, the type of the **Reclaimer** provider is **Uninstall**.
Name	This displays the name of the provider.

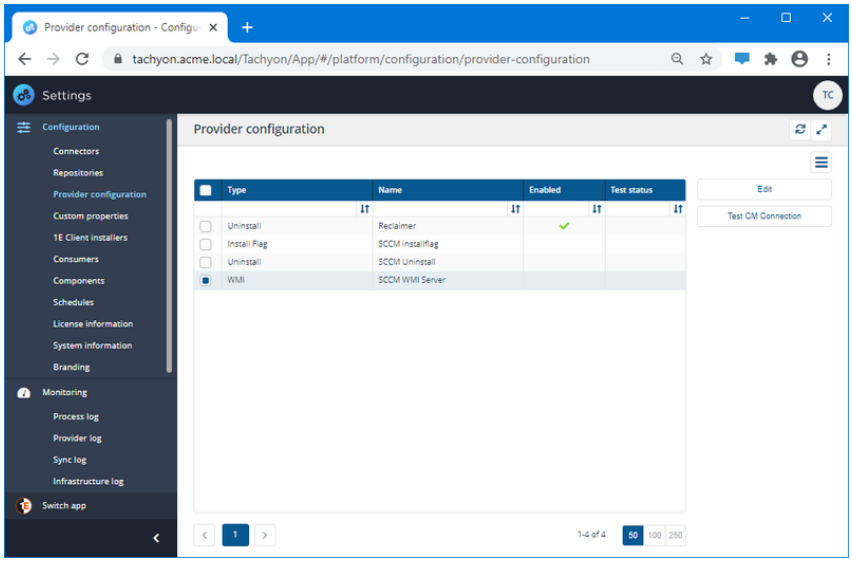
Column	Description
Enabled	This indicates whether the provider is enabled. If this cell contains a check the provider is enabled. If this cell is empty the provider is disabled.
Test status	Tells you if you have successfully tested the connection.

Providers get automatically added to the system when you install AppClarity and when you create at least one Configuration Manager (SCCM) connector.

The picture shows the **Reclaimer** provider, which lets you uninstall software using the reclaimer and is installed with AppClarity, and three providers that get created when you have added a Configuration Manager connector.

Provider	Description
Reclaimer	Used by AppClarity to connect to the Software Reclaimer, also referred to as **Traditional reclaim**. Please refer to Reclaiming a product using SCCM Uninstall for more details.
SCCM installflag	Used by Application Migration for the auto-install feature. Please refer to Enable Auto Install for Configuration Manager Applications and Packages.
SCCM Uninstall	Used by AppClarity as an alternative to the Software Reclaimer, also referred to as **SCCM custom Reclaim**. Please refer Reclaiming a product using SCCM Uninstall for more details.
SCCM WMI Server	The **SCCM WMI Server** provider lets you define credentials for accessing Configuration Manager that are subsequently used by the other two SCCM providers. You can test that the credentials are correct by selecting the SCCM WMI Server provider and then clicking the **Test CM Connection** button. In a Microsoft Endpoint Configuration Manager hierarchy, the SCCM WMI Server would be the CAS.

If you have multiple Configuration Manager connectors it's only when you have deleted the last one, that the SCCM providers are removed.



1.7.2.3.1.1 Enabling SCCM WMI Server

The WMI provider holds the connection details of the Configuration Manager server.

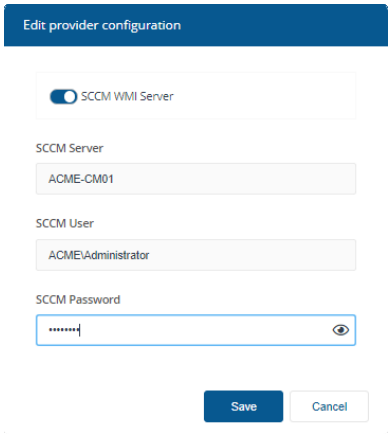
To set the provider configuration:

1. Navigate to **Settings**→**Provider configuration**.
2. Select **SCCM WMI Server** and click **Edit**.
3. In the **Edit provider configuration** popup, slide the **SCCM WMI Server** toggle to on and complete the displayed form using the following information as guidance:

Field	Description
SCCM WMI Server	Toggle this control to on (to the right) to enable the **SCCM WMI Server**.
SCCM Server	Enter the name of the Configuration Manager server. In our example this is **ACME-CM01**. In a Microsoft Endpoint Configuration Manager hierarchy, this would be the CAS.
SCCM User	The credentials for provider **SCCM WMI Server** may differ from those used for your System Center Configuration Manager (SCCM) connector. Make sure the credentials used here have SCCM administrator rights. SCCM Uninstall must be run under an account that's a member of the **dbcreator** server role on the database server where the SCCM database is hosted, in our example this would be **CM_CM1** on **ACME-SQL01**.

Field	Description
	The **SCCM User** account in our example is **ACME\Administrator**.
SCCM Password	The password for the **SCCM User** account.

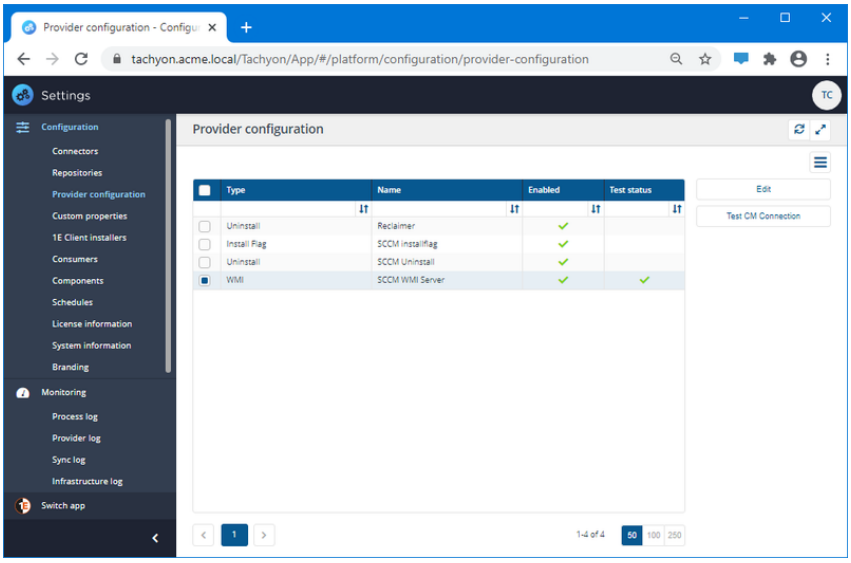
4. When you have entered the correct information, click **Save**.



1.7.2.3.1.2 Testing SCCM WMI Server

As the SCCM WMI Server provider defines how all the SCCM providers access Configuration Manager - you should test the details and credentials you have entered as soon as the provider has been saved.

1. Navigate to **Settings→Provider configuration**.
2. Select the provider with the name **SCCM WMI Server.**
3. Click on the **Test CM Connection** button, this button is enabled when only the **SCCM WMI Server** provider has been selected.
4. A test will be scheduled to run. When the test has completed successfully a green checkmark appears in the **Test status** column for the **SCCM WMI Server** row in the table, as shown in the picture opposite.
5. If the test fails you will need to recheck the details and credentials you have provided, making sure that the selected account has necessary permissions as described in Enabling SCCM WMI Server.



1.7.2.4 Custom properties

The following sections describe how you can set custom properties using Device and Software tags:

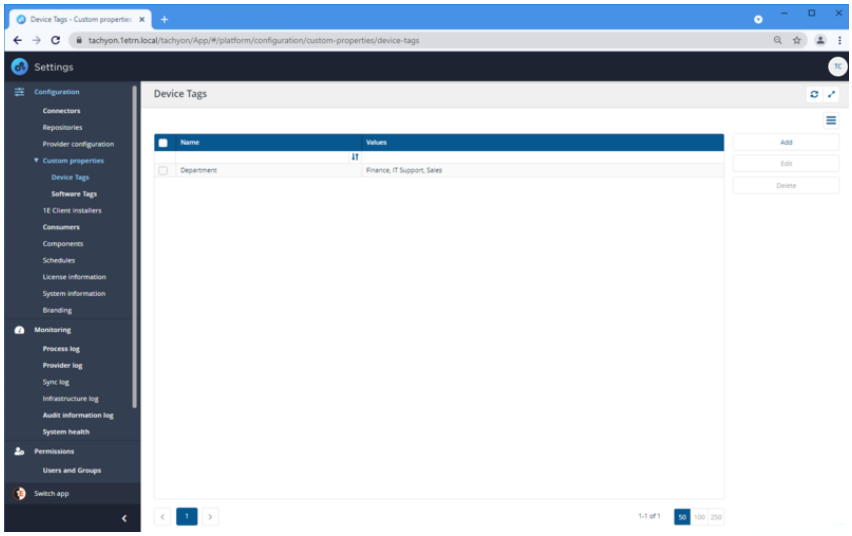
- **Device Tags** - are generally associated with Explorer and can be used when setting coverage to target Instructions to particular devices, but they can also be used to define Management Groups optionally used by all applications.
- **Software Tags** - using Software Tags allows you to create custom labels and associate them with the software titles you have deployed in your estate.

1.7.2.4.1 Device Tags page

Device Tags are generally associated with Explorer and can be used when setting coverage to target Instructions to particular devices, but they can also be used to define Management Groups optionally used by all applications.

Device Tags must be defined by a **Full Administrator** before they can be used to tag devices or used to set the coverage of Instructions.

This is done from the **Settings**→**Configuration**→**Custom properties**→**Device Tags** page, which can be viewed by users with the **Full Administrator** role.



1.7.2.4.1.1 Device Tag properties

Device Tags are used as part of the tagging workflow in Explorer, where they can be applied to devices and subsequently used to set the coverage for questions. The following table shows the constraints of the text that can be used for property names and values.

Property	Constraints
Name	Consists of a combination of alphanumeric characters, underscores, and dots - spaces are *not* allowed. Case is *not* significant, so names "*myname*" and "*MYNAME*" correspond to the same property name. The maximum length of a property name entered using the Administration console is 16 characters.
Values	Consists of a combination of alphanumeric characters, underscores, dots, and spaces. Case is preserved. The maximum length of a property value entered via the Administration console is 32 characters.

The following headings show steps to add, edit and delete properties and set property values.

1.7.2.4.1.1.1 Add a property and values

The following steps can be used to create a property name:

1. Navigate to **Settings**→**Configuration**→**Custom properties**→**Device Tags**.
2. Click the **Add** button.
3. Type in a name for the new device Tag.
4. You now need to add values to the property:
    a. In the edit field below the **Values** heading, type in a value for the property.
    b. If you want to add more values, click the **+** button beneath the **Values** heading.

5. Repeat step 4 to add as many values as you require for the selected property name.
6. When all the values have been added, click **Add**. (An error message is displayed if you exceed a maximum of 16 characters).

1.7.2.4.1.1.2 Edit a property

The following steps show how to edit the settings for an existing property:

1. Check the checkbox at the start of the row for the property you want to edit.
2. Click the **Edit** button.
3. You can change the **Name** or **Property type** and add and remove **Values**.
4. To add a value, click on the **+** icon and fill out the edit field.
5. To remove a value click on the trash can icon

   that appears when you hover the mouse to the right next to the value field you want to remove.
6. Clicking on the trash can removes the item immediately.
7. Click **Save**, when you have made all your changes.

1.7.2.4.1.1.3 Delete an entire property

The following steps show how to delete an existing property and all its values:

1. Check the checkbox at the start of the row for the property you want to delete, click **Delete**.
2. A notification will be displayed asking if you wish to proceed.
3. Click the **Yes, delete device tag** button to delete the property and all its values, or click the **No** button to abandon the deletion.

1.7.2.4.1.2 Working with Device Tags

Using Device Tags allows you to create custom labels and associate them with devices. An administrator with either the **Full Administrator** or **Group Administrator** role can set Device Tags to devices in their environment, they can also create Management Groups based on the tag name and value. For details about configuring Tachyon users, Roles, and Management Groups refer to the Permissions Menu pages.

In the following example, we create a Device Tag for use with a planned phased deployment affecting devices in our **All Managed Windows 10 Devices** Management Group. We will have values for the devices used for Testing (TestGroup), Pilot (PilotGroup), Group1 and Group2. We will, set our Windows 10 devices as a Pilot group using tags, then ask a question using the Tag as our coverage parameter.

> **Note**
>
> Management Groups are containers used to group devices and the software installed on those devices. Management Groups are defined using configurable rules that look at

various properties of the devices and their installed software, these are then evaluated to determine the group membership. This means that Management Group membership adapts to changes to the devices and software in your environment.

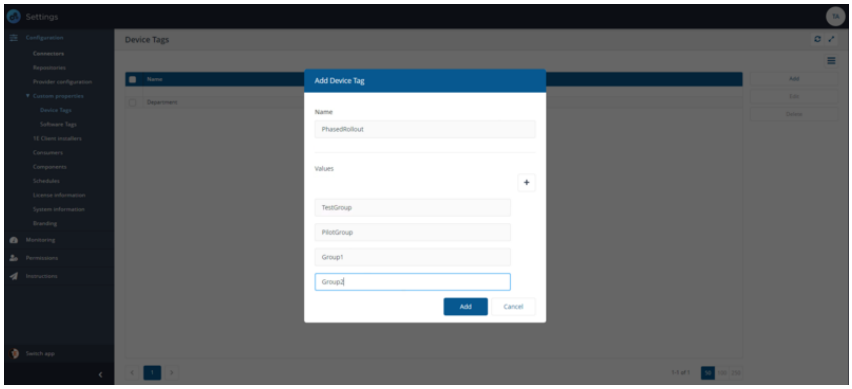
Refer to the Management Groups page and Management Groups - tutorial pages for details.

Note

For more details about using tags with client devices refer to Tagging client devices, and for more details about the system and custom Tachyon Roles, refer to the Roles page .

1.7.2.4.1.2.1 Create tags for a pilot group

1. To create our pilot group tag, our Full Administrator logs into Tachyon and switches to **Settings→Configuration→Custom Properties→Device Tags**
2. Then they click **Add**. In the **Add Device Tag** box type they type **PhasedRollout** in the Name field.
3. In the **Values** box, they add the following values by clicking the plus button, and click **Add**.
   - TestGroup
   - PilotGroup
   - Group1
   - Group2.

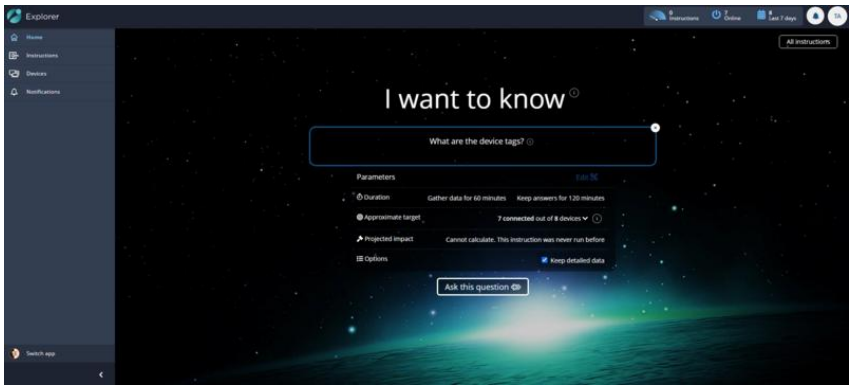


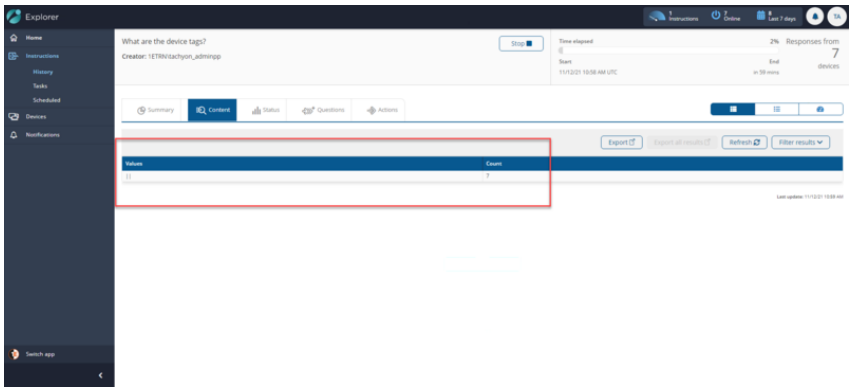
1.7.2.4.1.2.2 Apply Device Tags

Now our Full Administrator has set up the Device Tags for the planned deployment, they can assign the tags to every Windows 10 device in their environment in the **All Managed Windows 10 Devices** Management Group. Before they do this, they want to check what tags, if any, are already present in their environment.

1. Switch to the Explorer Application. Navigate to **Home** .
2. Click on **All Instructions** and searches for device tag, which brings back device tag related instructions which are in the **1E Explorer TachyonCore** instruction set.
3. They select **What are the device tags**, the leave the parameters as they are.
4. Then they click **Ask This Question**.

The administrator views the results in **Aggregated table view** , at the moment there are no tags in the environment. In the results, you can see the || delimiter which will be used for the list of tags on each device.





Next, our administrator wants to run the question on the **All Win10 Lab Workstations** Management Group and set the tags for the rollout.

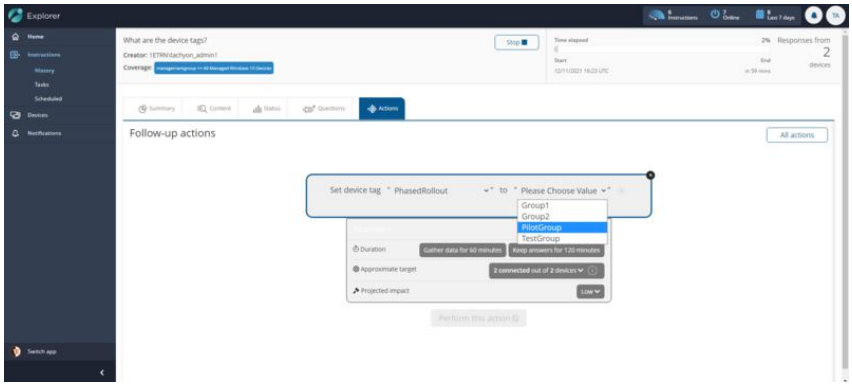
1. They ask the question again, but this time change the coverage to **All Win10 Lab Workstations** Management Group, then they click on **Ask This Question**.
2. Next, they click on **Actions** from the Question we just asked and click **All Actions**.
3. They select the **Set device tag <tagname> to <tagvalue>** action
4. They select **PhasedRollout** and **PilotGroup** and click **Perform this Action**.
5. Because this is an action, it requires approval, so prompts the administrator to confirm their password and then use an emailed confirmation code.

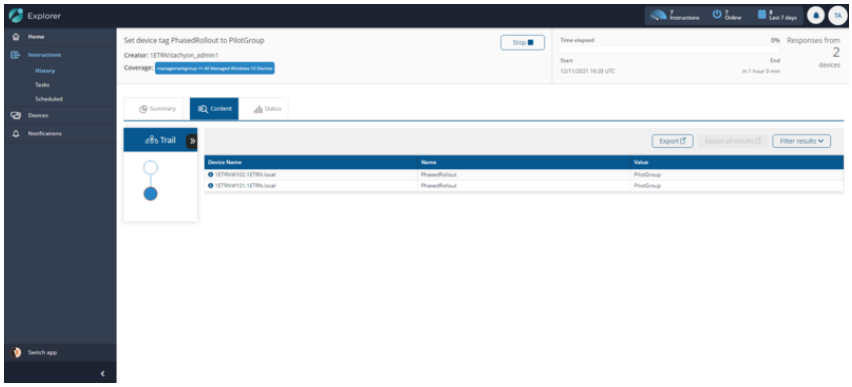
   Note

   In our environment, this requires approval from a user with the **All Instructions Approver** role. Once they have approved this action, the instruction is carried out.
6. Now, our administrator can see that they have two devices set as the **PhasedRollout - PilotGroup**.

Note

To find out more about using loading and managing Instruction sets, refer to the Instructions Menu.





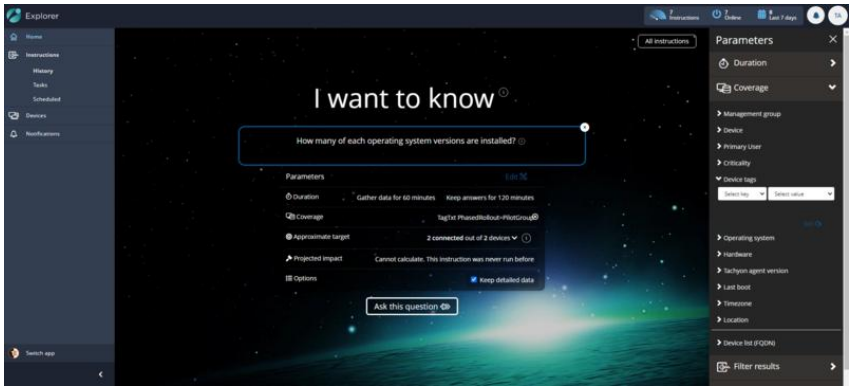
1.7.2.4.1.2.3 Ask a question using a Device Tag

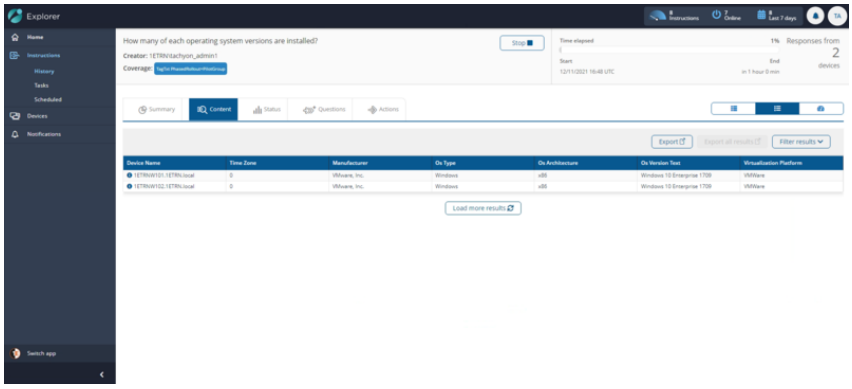
Our administrator now has Device Tags applied to the Windows 10 devices that will be in the deployment pilot group. Using these Device Tags as coverage they can ask questions using Explorer, for example to confirm how many devices have Windows 10 as an OS with the **How many of each operating system versions are installed?** Instruction from the **1E Explorer TachyonCore product pack**.

Note

The **How many of each operating system versions are installed?** Instruction returns a count of all distinct Operating Systems, version and virtual platform for each Tachyon-connected device. It is included in the Classic Product Pack used to create the **1E Explorer TachyonCore** instruction set that includes instructions for Tagging and Quarantine.

You can find a complete reference for the Product Packs included in the Tachyon Platform in the Tachyon Product Packs reference.

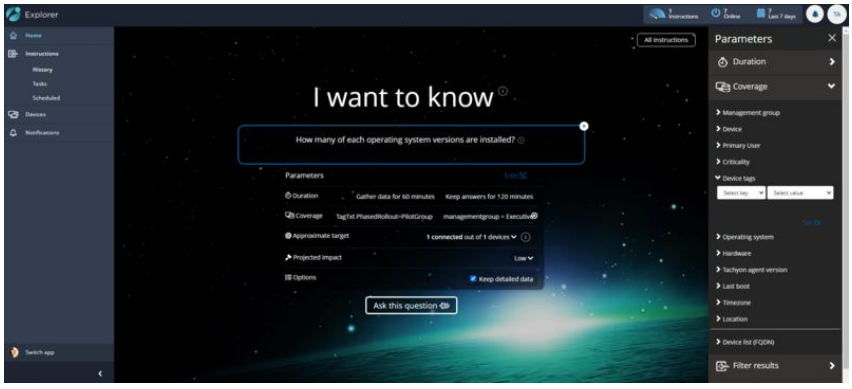


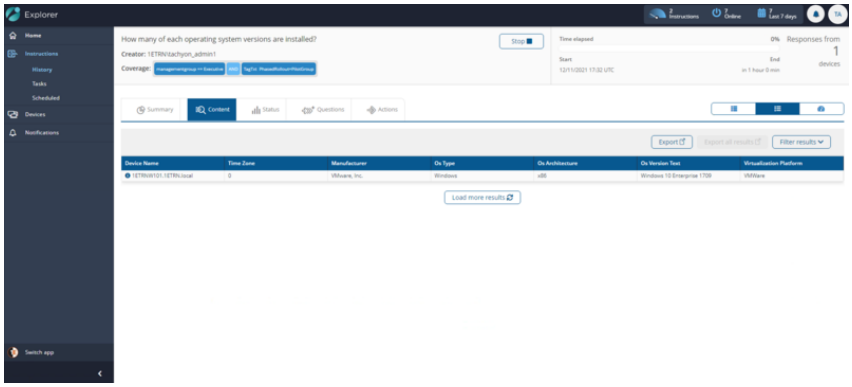


The administrator can also now cross-reference devices in the planned pilot group with any Management Groups they have created in Tachyon.

For example, our administrator wants to confirm if one of the Windows 10 devices is in the Executive Management Group, they can do this by running the
How many of each operating system versions are installed? Instruction again.

This time they include the **Executive** Management Group as a coverage parameter in addition to the Device tags, **PhasedRollout - PilotGroup**.

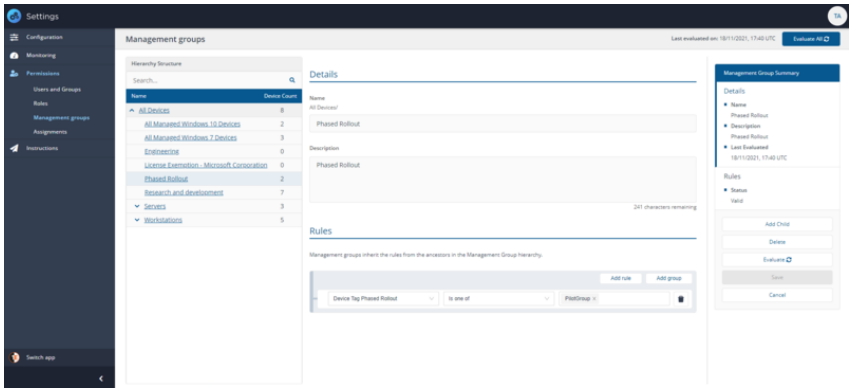




1.7.2.4.1.2.4 Management Groups based on Device Tags

In the exampleApply Device Tags our administrator checked for the presence of Device Tags in their environment and then applied those Device Tags to their Windows 10 devices. Following this, they were able to use those Device Tags as coverage parameters, so they can ask related questions using Explorer. In addition, once our administrator has created and applied their Device Tags, they could create Management Groups based on those Device Tags.

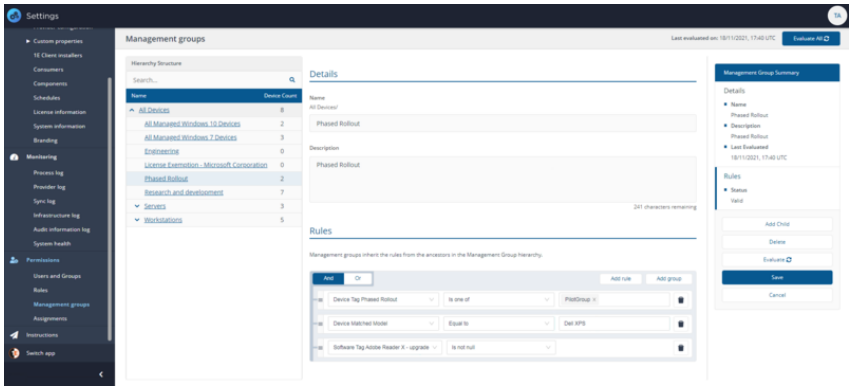
For example, now our administrator knows their Windows 10 devices have the **Phased Rollout** and **PilotGroup** Device Tag applied to them, they can create a Management Group called **Phased Rollout** based on these criteria. Using Explorer they can apply instructions focused to Windows 10 devices using the **Phased Rollout** Management Group as a coverage parameter.



Our administrator could then apply additional rules to their Management Group. For example, they could apply additional rules to narrow their focus to specific devices based on their hardware configuration . For example, they could add a Rule like **Device Matched Model Equal to Device XPS** , and then run **Evaluate**.

They could also use **Software Tags**, if they have created some, to focus group membership on devices with specific software titles if they are significant to the particular project.

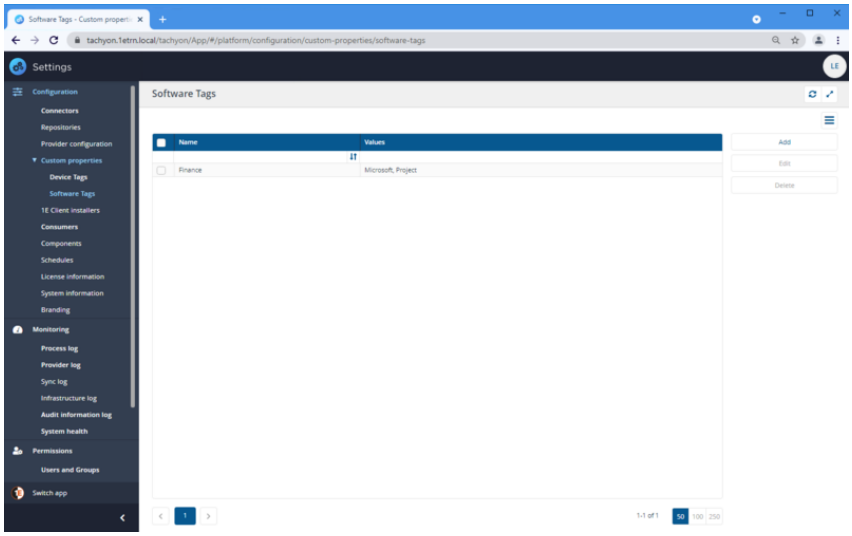
> **Note**
>
> Refer to the Software Tags page for details about using Software Tags which allow you to create custom labels and associate them with the software titles you have deployed in your estate.
>
> Refer to the Management Groups page for details about using rules and a full list of the rules used to create Management Groups, and which connectors that provide data to support the rules.



1.7.2.4.2 Software Tags page

Using Software Tags allows you to create custom labels and associate them with the software titles you have deployed in your estate.

You can do this from the **Settings→Configuration→Custom properties→Software Tags** page, which can be viewed by users with the **Full Administrator** role.



The following headings show the steps to add, edit and delete properties and set property values.

1.7.2.4.2.1 Software Tag custom properties

The following table shows the constraints of the text that can be used for property names and values.

Property	Constraints
Name	Consists of a combination of alphanumeric characters, underscores and dots - spaces are allowed. Case is *not* significant, so names "*myname*" and "*MYNAME*" correspond to the same property name.

Property	Constraints
Values	Consists of a combination of alphanumeric characters, underscores, dots and spaces. Case is preserved.

When creating your Software Tags, note that:

- You can have multiple tag values under one tag name
- A combination of one tag name and tag value is a Software Tag
- You can associate Software Tags with Software at Vendor, Title, and Edition (VTE) level
- A VTE can be associated with none or as many Software Tags as needed, there's no upper or lower bound
- A VTE can be associated with 1 tag value only under a tag name
- You can create Management Groups based on your Software Tag
- Any change in Software Tags will be reflected in Inventoryafter running Management Group evaluation.

1.7.2.4.2.1.1 Adding a property and values

The following steps can be used to create a property name:

1. Navigate to **Settings**→**Configuration**→**Custom properties**→**Software Tags**.
2. Click the **Add** button.
3. Type in a name for the property (the field warns you if you exceed a maximum of 16 characters).
4. You now need to add values to the property:
    a. In the edit field below the **Values** heading, type in a value for the property.
    b. If you want to add more values, click the **+** button beneath the **Values** heading.
5. Repeat step 5 to add as many values as you require for the selected property name.
6. When all the values have been added, click **Add**.

1.7.2.4.2.1.2 Editing a property

The following steps show how to edit the settings for an existing property:

1. Check the checkbox at the start of the row for the property you want to edit.
2. Click the **Edit** button.
3. You can change the **Name** or **Property type** and add and remove **Values**.
4. To add a value, click on the **+** icon and fill out the edit field.

5. To remove a value click on the trash can icon

   that appears when you hover the mouse to the right next to the value field you want to remove.

6. Clicking on the trash can removes the item immediately.

7. When all the required changes have been made click **Save**.

1.7.2.4.2.1.3 Deleting an entire property

The following steps show how to delete an existing property and all its values:

1. Check the checkbox at the start of the row for the property you want to delete, click **Delete**

2. A notification will be displayed asking if you want to remove the property and reminding you that the property and all of its values will be deleted

3. Click the **Yes, delete software tag** button to delete the property and all its values, or click the **No** button to abandon the deletion.

1.7.2.4.2.2 Working with Software Tags

Using Software Tags allows you to create custom labels and associate them with the software titles you have deployed in your estate. An administrator with either the **Full Administrator** or **Group Administrator** role can set Software Tags in their environment, they can also create Management Groups based on the tag name and value. For details about configuring Tachyon users, Roles, and Management Groups refer to the Permissions Menu pages.

In short, you can work with Software tags by:

1. Creating your Software Tag.

2. Associating the new tag with a software title.

3. Creating a Management Group based on the Software Tag name and Tag value rules (This step can be run anytime before evaluation).

4. Evaluating the new Management Group by running a Basic Inventory Consolidation.

If an administrator adds or modifies Software Tags or associations, they will have to run the Management Group evaluation report again to see the updated devices reflected in Inventory.

In the following example, we create a Software Tag to show how an EUC Manager who is a Full Administrator can use this feature alongside Management Groups and Experience. They want to do this, as part of an initiative to track down the causes for a recent spate of software crashes in their estate, because they want to prohibit this software from use.

> **Note**
>
> To find out about, how an EUC manager can use Experienceto track down the causes of a recent spate of software crashes, refer to Investigating software crashes and Broadcasting information via Announcements.

1.7.2.4.2.2.1 Creating tags for a software installations

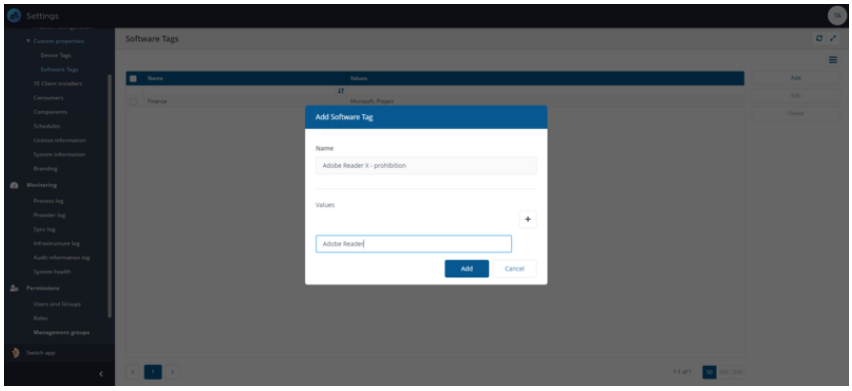
Our administrator, needs to create their Software Tag and associate the new tag with a software title.

1. To create our Software Tag, our administrator logs into Tachyon and switches to **Settings**→**Configuration**→**Custom Properties**→**Software Tags**

   There are already tags for the Finance department for Microsoft products and specifically installations for Microsoft Project. Now, they will create a new tag called **Adobe Reader X - prohibition.**

2. Then they click **Add**. In the **Add Software Tag** box, they type **Adobe Reader X - prohibition** in the Name field.

3. In the **Values** box, they add the **Adobe Reader X** values by clicking the plus button, and click **Add**.



1.7.2.4.2.2.2 Apply Software Tags

Now our administrator has set up the Software Tag for the legacy software, they can assign the tag to installations of **Adobe Reader X** software.

1. They switch to the **Inventory**→**Software Inventory**→**Aggregate** page.

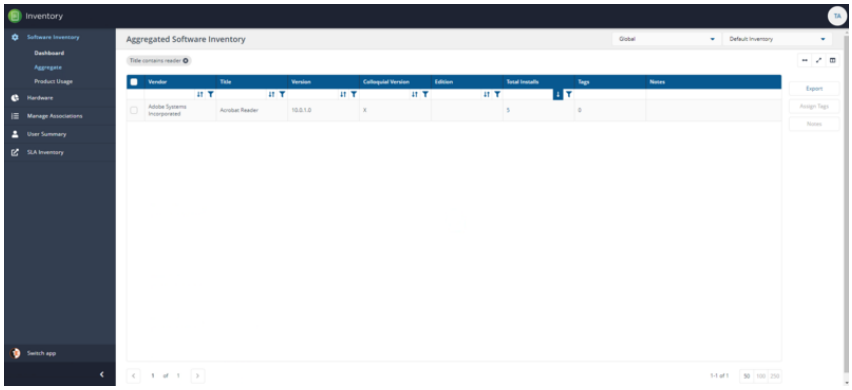
2. Then, filter on **Title contains reader** which returns five **Total Installs**.

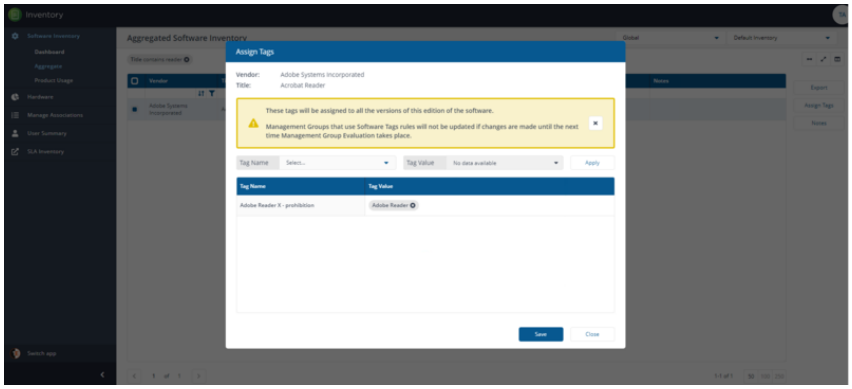
3. With the results selected, our administrator can click **Assign Tags**. In the Assign Tags pop-up, they choose **Adobe Reader X - prohibition** for the **Tag Name** and **Adobe Reader** as the **Tag Value** from the drop-down lists, and then click **Save**.

Note

Please note, Software tags will be assigned to every version of that software edition. For example, in our example we only have one version of Acrobat Reader, which is version 10.0.1.0, the one we want to prohibit.

But in a production environment, it's common to have multiple versions of a software title, Software Tags apply to all versions of a software edition not individual versions of that title.



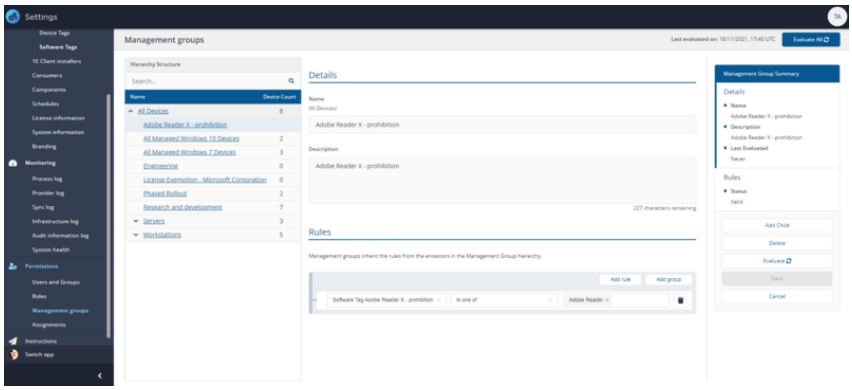


1.7.2.4.2.2.3 Create a Management Group

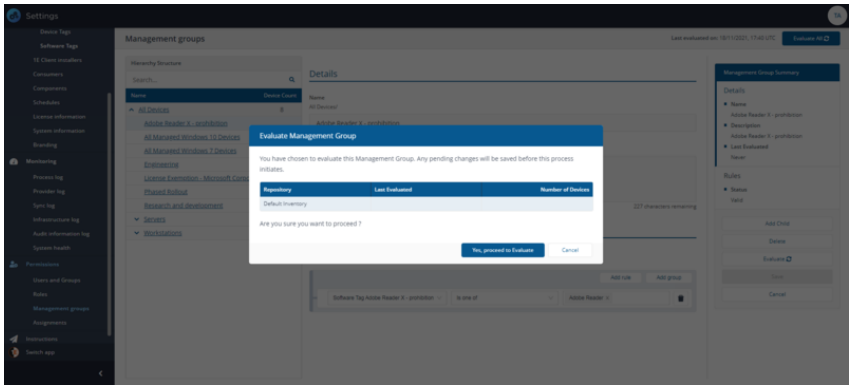
Now our administrator has created their Software Tag and associated it with a software title, they will create a Management Group based on the Software Tag name and Tag value rules. When they have completed this step, they will evaluate the new Management Group by running a Basic Inventory Consolidation.

1. To create the Management Group for Adobe Reader X, our administrator navigates to **Settings→Permissions→Management groups**. Because our administrator wants to create a group that captures every install of this legacy software, they decide to create a **Child** group under All Devices called **Adobe Reader X - prohibition**.

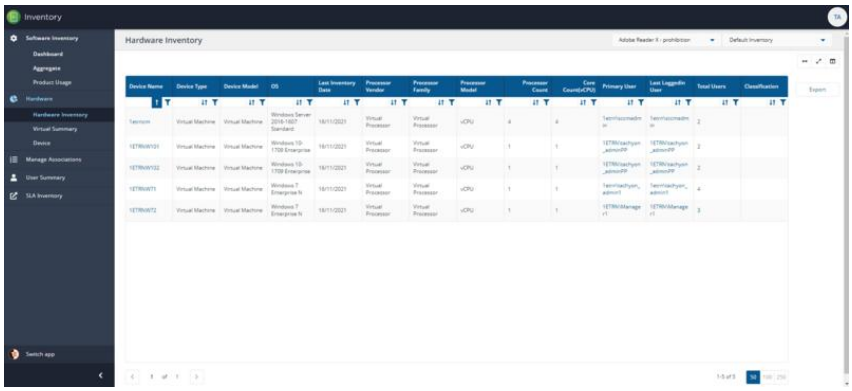
2. Next, the administrator needs to add at least one rule to the new group to define its scope. They select, **Software Tag Adobe Reader X - prohibition is one of Adobe Reader** and then click **Save**.



1. Now, they click **Evaluate**. This evaluates then new group against the default Inventory, and matching items populate the Management Group.



1. Finally, our administrator navigates to **Inventory→Hardware→Hardware Inventory** and filters the view by the newly created Management Group, **Adobe Reader X - prohibition**. Now, they can view every device where **Adobe Reader** is installed.



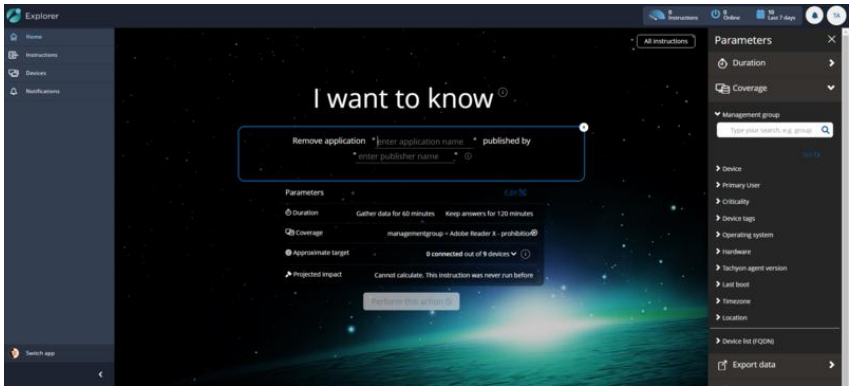
Now our administrator has identified their problematic software installations, they can use Explorer to run instructions against that Management Group. For example, they could run **Remove application <appname> published by <publisher>** using the **Adobe Reader X - prohibition** Management Group as a coverage parameter to remove all versions of the specified application published by the specified publisher, if present.

Or, they could use **Remove version <version> of application <appname> published by <publisher>** to remove the specified version of the specified application published by the specified publisher, if it is present. Our administrator could identify these details using Inventory filtered to the **Adobe Reader X - prohibition** Management Group.

Note

Both **Remove application <appname> published by <publisher>** and **Remove version <version> of application <appname> published by <publisher>** are included in the Instructions.

Refer to Tachyon Product Pack Deployment Tool to find out about the PPDT that you can use to upload multiple Classic and Integrated Product Packs into Tachyon.



1.7.2.5 1E Client installers page

Enables you to upgrade the 1E Client across your network, and allows you to select the 1E Client installer you want to use for the installation. This process will only upgrade the client on Windows 8.1 devices and above. And will keep the settings from the previous deployment, it will not allow you to enable or change any features.

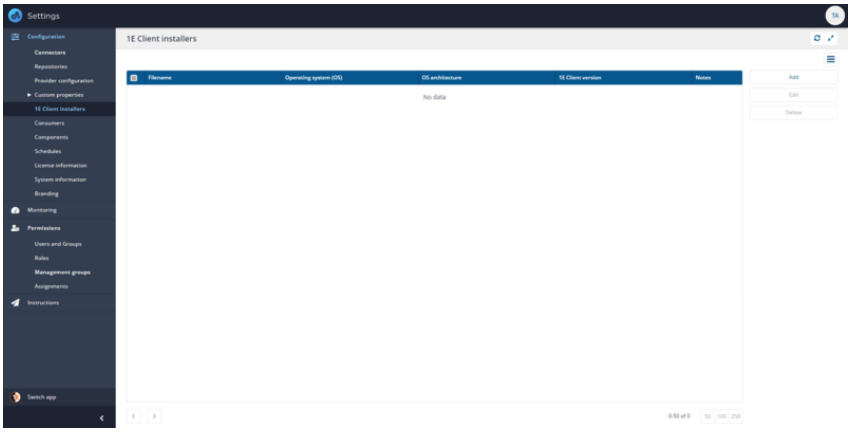
If you are deploying the 1E Client for the first time, or you need to enable new features or remove existing, then you will need to deploy the 1E Client using the Client Deployment Assistant, please refer to Deploying 1E Client.

> **Note**
>
> This feature does not support deployment of patches (accumulated hotfix).
>
> **Note**
>
> Please contact your 1E Account Team if you need help with this.

1.7.2.5.1 Preparation

First you will need to download the 1E Client Installer files from the 1E Support Portal, https://support.1e.com/ and save these to a location accessible to a user who can access Tachyon using the **Full Administrator** role.

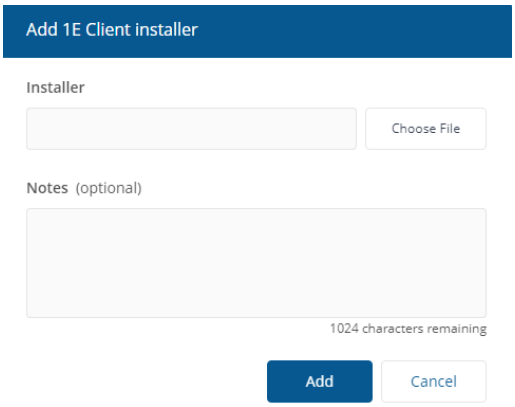
1. Open the Tachyon Portal and navigate to **Settings→Configuration→1E Client installers** page.



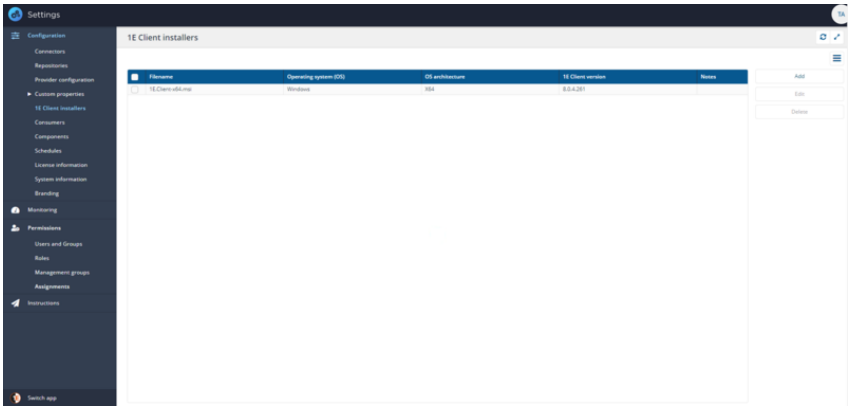
2. On the right-hand side of the screen, click **Add**.

3. From the displayed screen, select **Choose File** and browse to the location where you saved the MSI.

4. Select the **1E.Client-x64.msi** and optionally add any notes you want, click **Add**.



5. The Installer is then listed on the **1E Client installers** page, repeat the process if you have any 32 bit clients to deploy to.



1.7.2.5.2 Upgrading the clients

The upgrade runs using an Instruction called
Trigger 1E Client upgrade to <ClientVersion> for targeted devices, this is included with one of the Product Packs imported as a final task when running Tachyon Setup. You will need to have carried out the upload of new Product Packs at the end of the upgrade, before carrying out this step, refer to Upgrading Tachyon Platform for details.

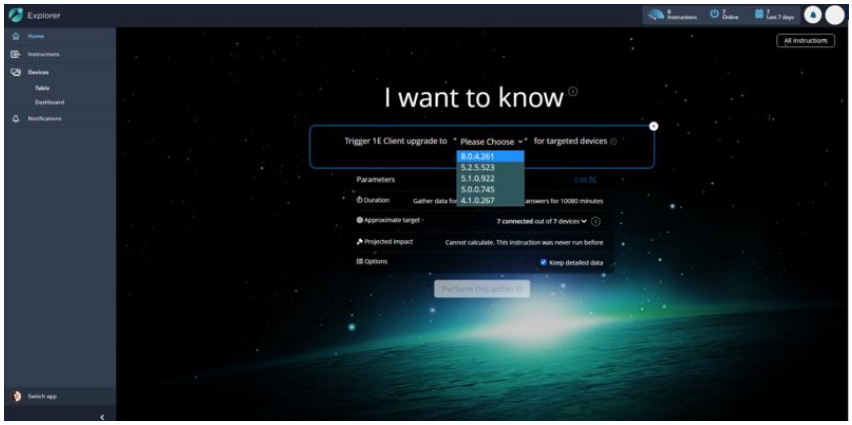
1. Choose **Switch app** and choose the **Explorer** application, the user carrying out this task will need the **All Instructions Actioner** role as a minimum, although **Full Administrator** will also be able to carry out these tasks.

2. In **I want to know**, search for and select
Trigger 1E Client upgrade to <ClientVersion> for targeted devices action, in the drop list for the Client version choose a client version, for example **8.1.2.62** as that is the Client version for this release of Tachyon.

3. Once selected, confirm the target and **Duration** are correct. We set this to be a longer gather time to ensure clients have enough time to come online, receive the instruction and run the action.

4. When you have confirmed the coverage and duration, click on **Perform this action**, and follow the 2FA process.

In a production environment, you would first target a subset of devices on your estate, to confirm the upgrade is successful, and the client correctly communicates with Tachyon. You would do this by selecting the **Edit** option next to **Parameters**, and select your target, this may be a testing management group, or a Ring 1 Device Tag.



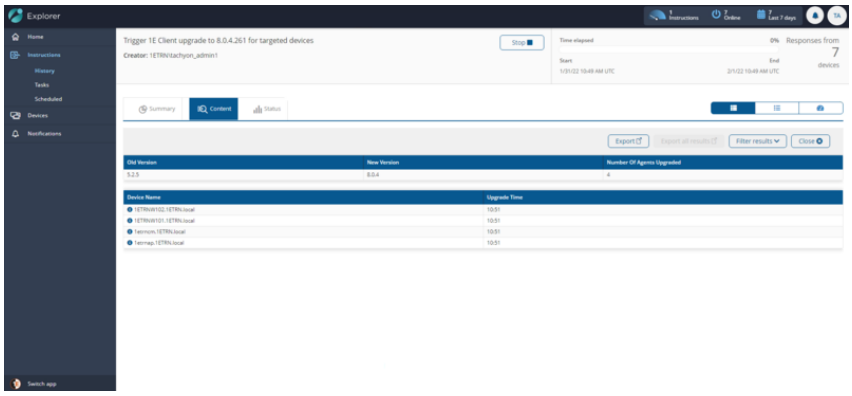
The upgrade then runs and responses are returned, and we see that the new version is now installed.

We can confirm the upgrade has been carried out and can see the old and the new version listed in the top table. This Action only upgrades devices that are Windows 8.1 or above. So, in this environment, 3 devices did not upgrade.

Tip

You can take an optional lesson contained within the Upgrade course which shows this process. You can access the lesson at https://1e.tovuti.io/1e-courses/course/tachyon-upgrade-supported-version-to-v80

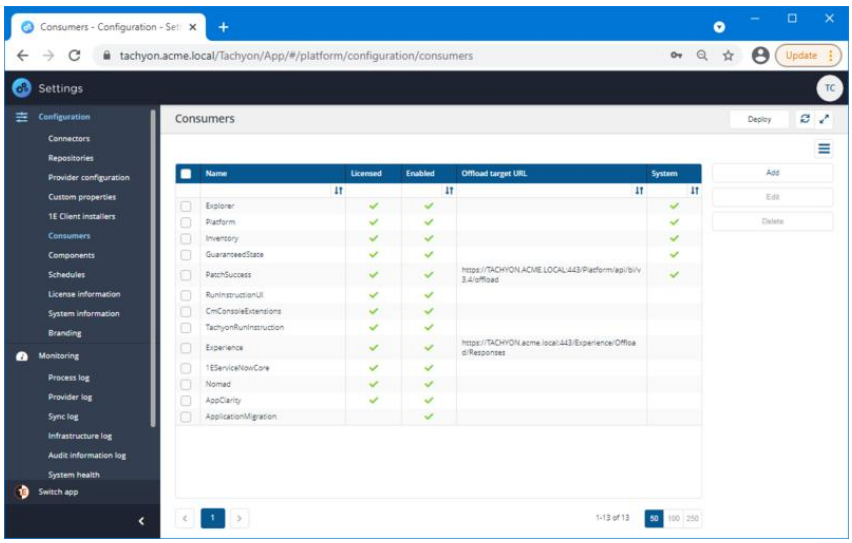
You will need to log into Tovuti to view the course, using the **Login** option at the top right of the screen. If you do not have an account, then select the **Register** option.



1.7.2.6 Consumers page

The **Consumers** page lets you register the consumers that can access Tachyon. To enhance the security of the Tachyon system, only consumers that have been registered on this page will be allowed to access Tachyon.

Tachyon can integrate with third-party applications to enable its instruction-based investigation and resolution capabilities to be leveraged by other products. Some examples include: the Content Distribution Content Pause and Configuration Manager integration features.



1.7.2.6.1 The Consumers page

Some consumers provided by 1E create their own consumer entries on the consumers page, others require that these are added by hand.

You can create a consumer entry by hand by clicking on the **Add** button. Doing this displays a form used to define how the consumer will interact with Tachyon. The parameters available on this form are described in the following table:

Parameter	Description
Name	Sets the name for the consumer. This will be determined by the third-party application and must be entered correctly to enable the consumer to work. For example the Tachyon Configuration Manager console extensions must have a consumer defined that is called **CmConsoleExtensions**.
Consumer URL (optional)	This value can be used as a placeholder for any URL that is used by the Consumer. Tachyon never makes use of this, so this is more of a reference for Tachyon Consumer Administrators if they want to look at the Consumer interface. It is also the case that not all Consumers have a URL, so this parameter can be safely left at its default.

Parameter	Description
Maximum simultaneous instructions	Determines the number of simultaneous instructions that may be made by the Consumer. Instructions in Tachyon have a **Gather data for** setting which determines how long the instruction will be in operation gathering data. The **Maximum simultaneous instructions** value sets how many instructions a Consumer can have in operation at any one time. If the value is exceeded, newly requested instructions will be delayed until one of the in operation instructions has completed.
Offload target URL (optional)	Determines the target URL when attempting to offload responses to a Consumer. The Consumer will need to have a listener at that URL waiting to receive the responses.
Offload timeout seconds (optional)	Determines the timeout for offloading responses to a Consumer. This governs the amount of time Tachyon allows for the Consumer to respond to its offloading before logging an error in the log file.
Use Windows Authentication	Determines whether Tachyon will try and use Windows Authentication when attempting to offload responses to a Consumer. For example, when Tachyon retrieves data back from a question asked by a Consumer, it can be configured to offload the responses directly to the Consumer. To do that Tachyon has to make a connection. Checking the **Use Windows Authentication** checkbox configures Tachyon to use Windows Authentication for that connection. Otherwise, if **Use Windows Authentication** is not checked, Tachyon assumes there is no authentication/anonymous authentication.
Enabled	This checkbox specifies whether the Consumer is enabled or not. In order for a Consumer to work with Tachyon, its Consumer entry on the Consumers page must be enabled.

Once the information has been set click on the **Save** button to commit the changes.

1.7.2.6.2 Deploying policies for all consumers

The **Consumers** page has a **Deploy** button at the top-right of the page, this can be used to deploy all policies, rules, events and surveys across all the consumers. When you click the button you will be notified whether there are any pending changes waiting to be deployed and reminded that this will deploy for all the consumers.

1.7.2.6.2.1 Deploying policies for consumer applications

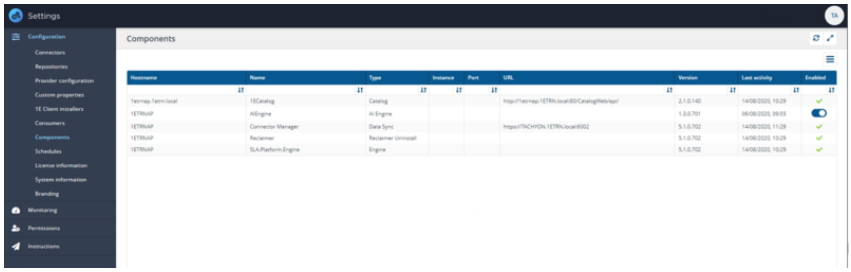
Most consumers with items that can be deployed have their own deploy buttons in their associated applications. Clicking the deploy button in any one of those applications deploys the policies, rules, events and surveys that are relevant to just that application. Content Distribution is the single exception to this as it has no deploy button in its application. The only way you can manually deploy the Content Distribution event registrations is by clicking the **Deploy** button on the **Consumers** page. Tachyon Setup performs an automatic deployment after installation but before any additional policies have been loaded. This enables the event registrations for both the Content Distribution and Experience applications without users having to do this manually.

1.7.2.6.3 Consumer example

An example of defining a consumer can be found on the Preparing for the Tachyon extensions for the Configuration Manager Console. page.

1.7.2.7 Components page

The **Components** page displays the configuration options and activity for all the components that make up the Tachyon platform.



1.7.2.7.1 The Components table

The following table provides a description of the columns in the **Components** table:

Column	Description
Hostname	The hostname of the server where the component is installed.
Name	The name of the component.
Type	The type of the component. This is entirely determined by the component. Examples are: **Catalog**, **Data Sync**, **Reclaimer Uninstall** and **Engine**.
Instance	
Port	

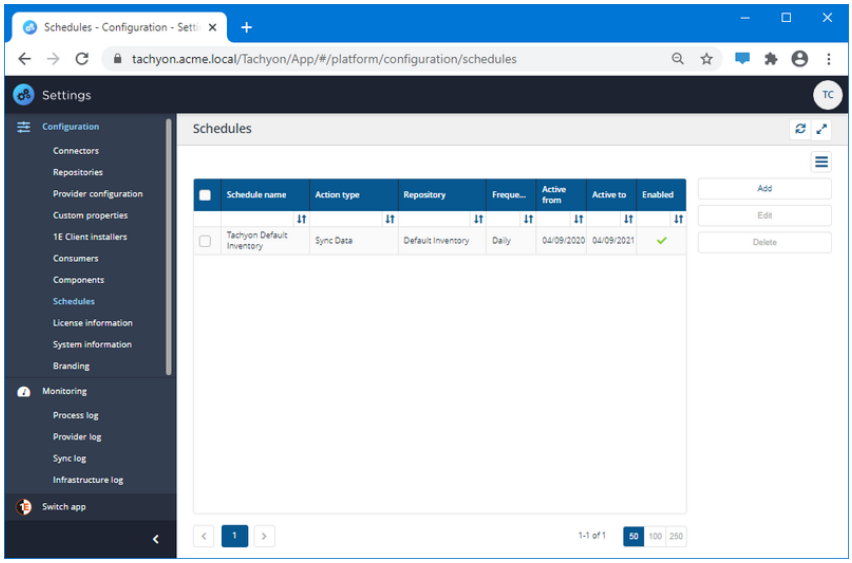
Column	Description
URL	This shows a URL that can be used to access the component. For example: **http://ACME-TCN01.ACME.LOCAL/CatalogWeb/api/** for accessing the **1ECatalog** component on a particular installation.
Version	The version number for the component. For example the **1ECatalog** component may have a version number of **2.1.0.140**.
Last activity	This shows the last date and time the component was active.
Enabled	A check in this column shows that the component is enabled. If this cell for a component is blank the component is not enabled.

Note

The **AIEngine** component can be turned on or off using the toggle control. Slide the toggle to the left to turn the AI feature off or to the right to turn the AI feature on.

1.7.2.8 Schedules page

The **Schedules** page lets you add schedules for executing actions on repositories, and select the categories of data you wish to collect.



1.7.2.8.1 Schedules table

The Schedules table lists each schedule that has been created and displays the following information:

Column	Description
Schedule name	The name set for the schedule. This can be used to identify the schedule in the **Process log**.
Action type	The type of action selected for the schedule. The available action types are dependent on the selected repository type.

Action type	Description
Sync Data	Only available for inventory repositories when one or more inventory connectors have been created. Performs a sync action where the selected connector is run to fetch data from a data source and place it into the selected inventory repository.
Generate Report	Performs a data processing action on the data in the selected repository.

Repository	The repository the action will be run on.
Frequency	The frequency for the schedule.
Active from	The date the schedule will be active from.
Active to	The date when the schedule will stop being active.
Enabled	A green tick in this cell indicates that the schedule is enabled. If the cell is empty the schedule is not enabled.

1.7.2.8.2 Adding a new Schedule

On the Schedules page you can create a new schedule by clicking the **Add** button.

> **Note**
>
> All schedules are defined in UTC time.

To add a new schedule:

1. Navigate to the **Settings**→**Configuration**→**Schedules** page.
2. Click the **Add** button.
3. In the **Add schedule** popup enter a **Schedule name**.

Tip

You should use a naming convention for schedule names:

<action type> <repository name> <schedule>

For example:

SCCM Demo Inventory 11pm *(only need to say Demo once)*

SCCM Demo Default Inventory 3am *(demo connector but default inventory)*

SCCM with RCR Default Inventory Friday 2am

4. Select the **Repository** from the drop-down list. For example, **Default Inventory**.
5. Select the **Action type** from the drop-down list. For example, **Sync Data - Tachyon** action for a Tachyon connector created previously.
6. For inventory **Sync data** actions you can perform a **Clean sync**, which deletes the data in the selected inventory repository before performing the new sync.
7. If AI Powered Auto-curation has been enabled, then inventory **Sync data** and **Basic Inventory Consolidation** actions allow you to select **Run AI action**, which performs additional processing to normalize software product names that are not in the 1E Catalog.
8. For inventory **Sync data** type actions you also get to select the categories of data that you want to sync. In the **Data to Sync** heading there is a**Select All** checkbox that lets you select or deselect all the following data categories, you can also select or deselect these individually:

   Note

   The categories displayed are dependent on the type of connector.

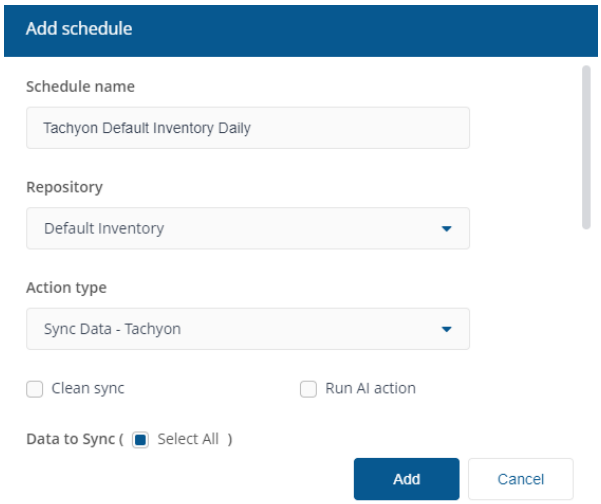
   - AD Organizational Unit
   - CM Application & Package
   - Device
   - Installed Software
   - Patch
   - Processor
   - Software Usage
   - User
9. Select a **Frequency** for the schedule. For example, you can create a **Daily** schedule. Doing this adds the relevant controls to the **Add schedule** popup.

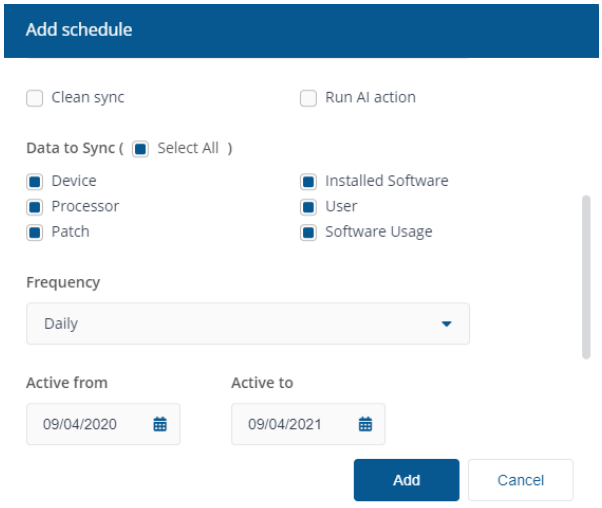
   Note

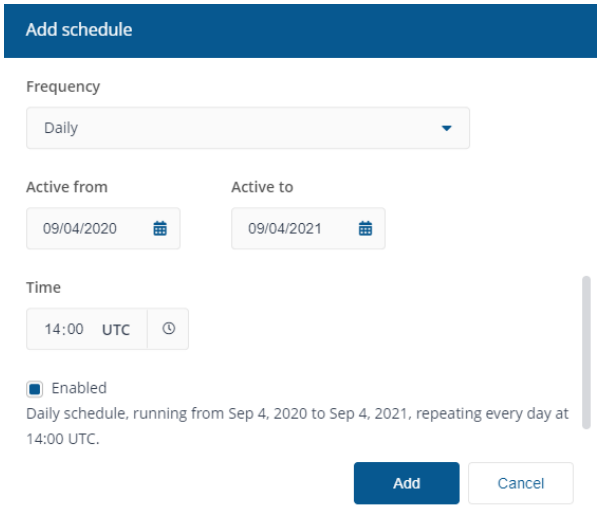
   - Repeat Minutes
   - Daily
   - Weekly
   - First week of month

- Second week of month
- Third week of month
- Last week of month
- Day of the month

10. Select the **Active from** date. For example, the current date.
11. Select the **Active to** date. For example the same day in the following year.
12. Select other settings according to the Frequency you selected. For example, you can set the **Time** to **00:01**, so that the schedule runs at 1 minute past midnight in UTC time.
13. Ensure that the **Enabled** checkbox is checked to make the schedule immediately active.
14. When all the schedule fields are set click **Add** to add the active schedule.







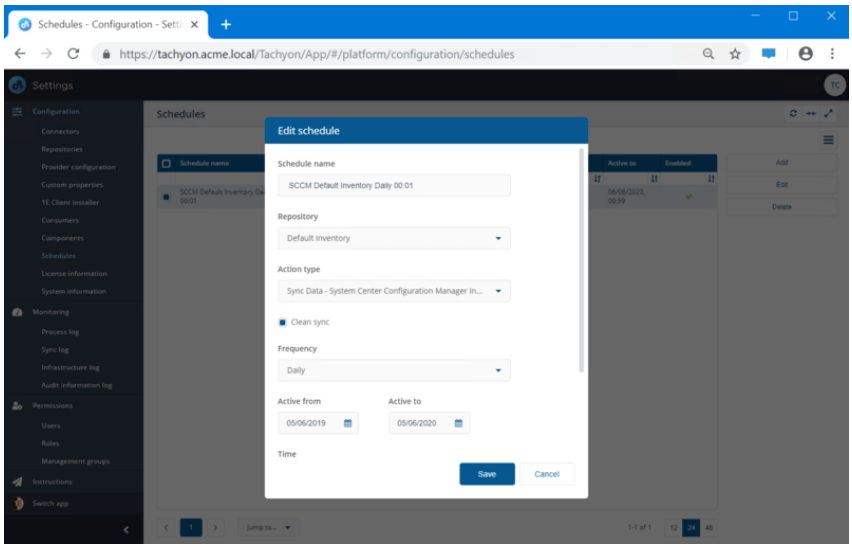
1.7.2.8.3 Editing an existing Schedule

You can edit a particular schedule to change any of its parameters. To do this:

1. Navigate to the **Settings→Configuration→Schedules** page.
2. Check the checkbox next to the one schedule you want to edit.
3. Click the **Edit** button.
4. In the **Edit schedule** popup make any changes you need to the schedule.
5. When you are finished, click **Save** to commit the changes.

1.7.2.8.3.1 Enabling and disabling a Schedule

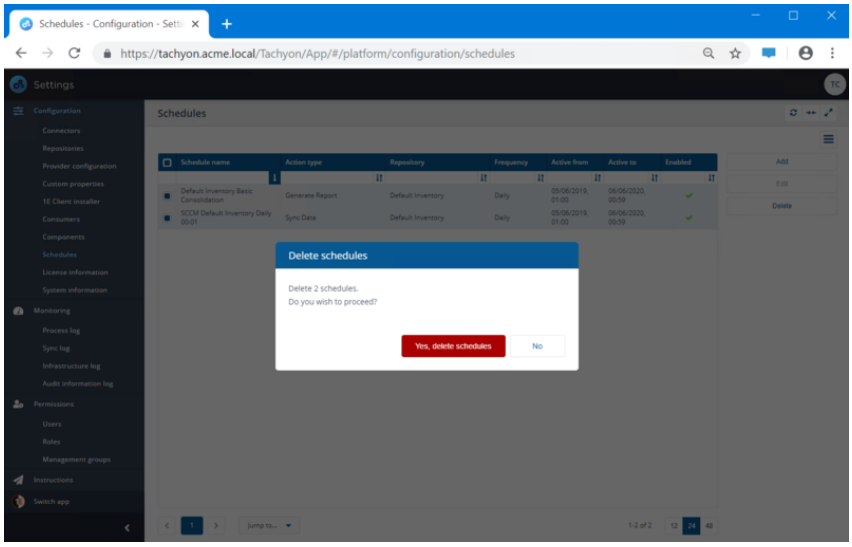
A primary reason to edit an existing schedule is to temporarily disable it so that it can be edited and re-enabled at a later date. For example if you know you have a planned maintenance task you might want to temporarily disable the schedules during the maintenance and then re-enable them once the maintenance has finished.



1.7.2.8.4 Deleting a Schedule

You can delete a particular schedule when it is no longer needed. To do this:

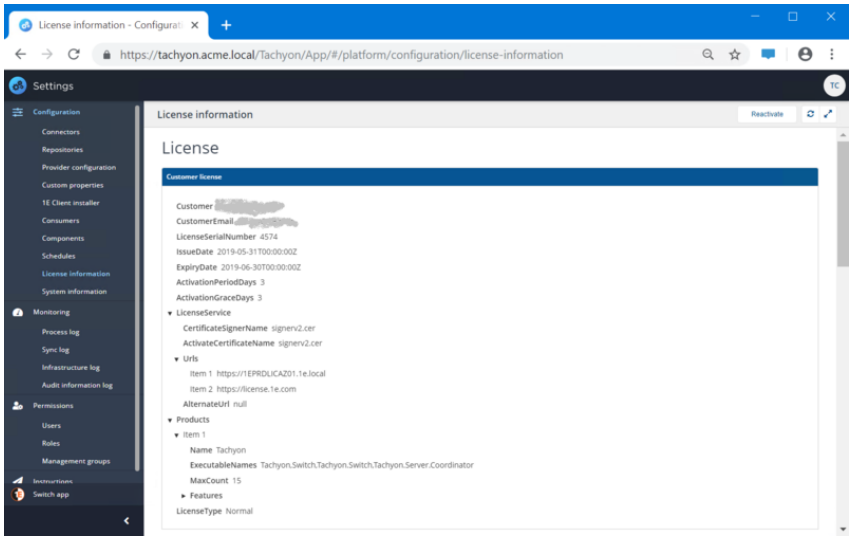
1. Navigate to the **Settings→Configuration→Schedules** page.
2. Check the checkbox next to the one schedule you want to delete (you can delete multiple schedules in a single action by checking multiple schedules).
3. Click the **Delete** button.
4. In the **Delete schedule(s)** popup you will be asked if you want to proceed.
5. To proceed and delete the selected schedule(s) click the **Yes, delete schedule(s)** button.



1.7.2.9 License information page

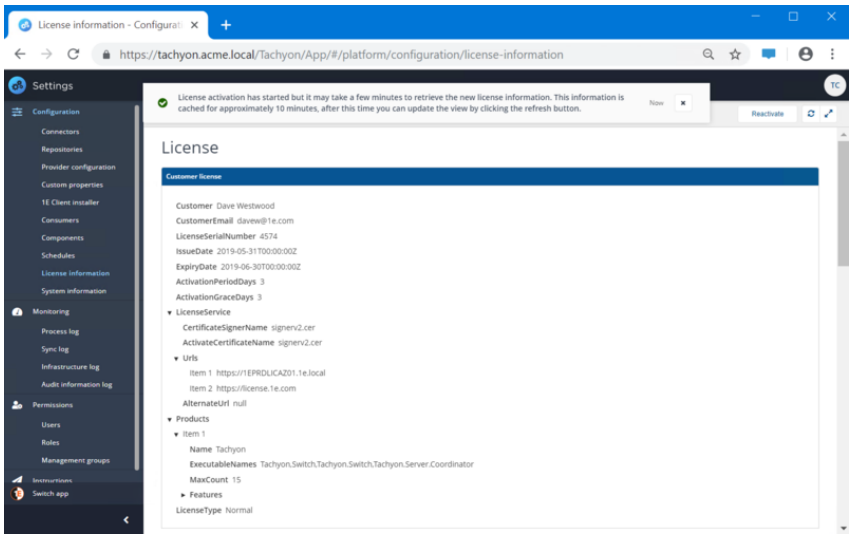
The **License information** page shows details of the current license status and lets you reactivate your license if any changes have been made.

In the Products section, under Features, you can see which consumers you are able to use, and which type of instructions you can run according to their prefix pattern. Available consumers and prefixes are listed below under License requirements for consumer applications.



1.7.2.9.1 Reactivating licenses

You can reactivate a license after it has been updated by 1E by clicking the **Reactivate** button. It takes a few minutes to retrieve the new license information and the page caches its displayed information for around 10 minutes. After this time you can update the view by clicking the **Refresh** button, which updates the information displayed on the page and in the lower right-hand corner of the browser.



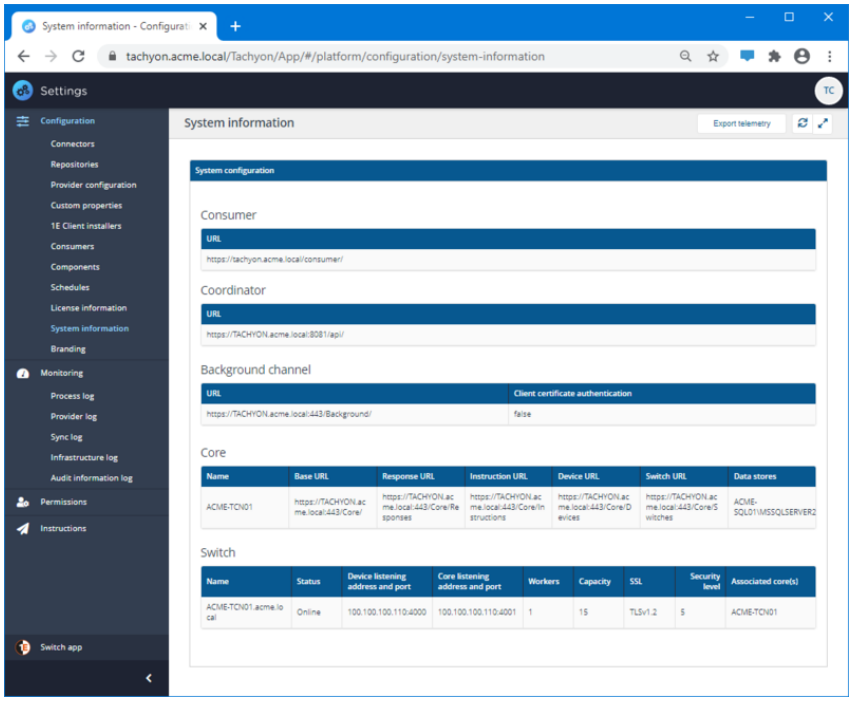
1.7.2.9.2 License requirements for consumer applications

For any application, tool or feature to use instructions, its consumer and prefix pattern must be registered in your license.

For full details about the License requirements for consumer applications, refer to License requirements.

1.7.2.10 System information page

The **System information** page lets you review the configuration of Tachyon components used for Tachyon real-time features. There are no configuration options.



1.7.2.10.1 System information

The information on this page is described in the following table:

Field	Description
Consumer	Displays the URL for the consumer API. For example: **https://TACHYON.acme.local/Consumer/**
Coordinator	Displays the URL for the coordinator API. For example: **https://TACHYON.acme.local:8080/api/**
Background Channel	Displays a list of configured background channels, showing the following information:

Field	Description

Column	Description
URL	Displays the URL for the background channel. This is set in the Tachyon clients so that they can communicate with this background channel. For example: **https://TACHYON.acme.local:443/background**
Client Certificate Authentication	Indicates whether client certificate authentication is required by the background channel. This may be **true** (client certificates are required) or **false** (client certificates are not required).

Core

Displays a list of the configured cores, showing the following information:

Column	Description
Name	The name used by the Master to identify the core. For example: **ACME-TCN01**
Base URL	The base URL for the core. For example: **http://ACME-TCN01.acme.local:80/CoreInternal/**
Response URL	The responses URL for the core. For example: **http://ACME-TCN01.acme.local:80/CoreInternal/Responses**
Instruction URL	The instructions URL for the core. For example: **http://TACHYON.acme.local:443/Core/Instructions**
Device URL	The devices URL for the core. For example: **http://ACME-TCN01.acme.local:80/CoreInternal/Devices**

Field	Description	
	Switch URL	The switches URL for the core. For example: **http://TACHYON.acme.local:443/Core/Switches**
	Data stores	The SQL instance where the core data is stored. For example: **ACME-SQL01**
Switch	Displays a list of the configured switches, showing the following information:	

Column	Description
Name	The name of the Switch Host. For example: **ACME-TCN01.acme.local**
Status	The current status for the switch. This may be one of **Online** or **Offline**
Device listening address and port The port on the IP address the switch listens on for Tachyon client connections. For example: **4000**	The address the switch listens on for Tachyon client connections. For example: **100.100.100.110:4000**
Core listening address and port The port the switch listens on for core prompts. For example: **4001**	The address the switch listens on for core prompts. For example: **100.100.100.110**

Field	Description	
	Workers	The workers the switch is configured to use. In combination with **Slots**, this value specifies the number of devices the switch can support. For example: **1**
	Capacity	The number of slots available to the switch. In combination with **Workers**, this value specifies the number of devices the switch can support. For example: **15**
	SSL	The security protocol used when communicating with this switch. This should be set to **TLSv1.2** unless advised by 1E.
	Security Layer	Shows the security level used by the switch when communicating with the Tachyon clients. By default this is set to: **5**
	Associated Core(s)	Specifies the cores this Switch is associated with by name. For example: **ACME-TCN01**

1.7.2.10.2 Export telemetry

The **Export telemetry** button triggers a collection process for Server telemetry data and exports a CSV file. The contents of the file are not encrypted.

If you have disabled automated sending of Server telemetry to 1E, and you contact 1E Support for assistance with any problems, you may be asked use the **Export telemetry** button, and then send the CSV file to 1E.

Telemetry helps 1E to continually improve your experience with Tachyon. Only summarized statistical information is collected, which enables 1E to see how customers use features of the application. No personally identifiable data is collected. 1E use this information to:

- Understand how the product is being used to influence future development decisions
- Plan supported platforms (OS, SQL etc. versions) over time
- Deliver a smooth upgrade experience as we can focus testing on implemented scenarios
- Improve system performance

- Identify early warning signs of potential issues such as excessive growth of database tables, instruction failures etc. so we can proactively address them.

Server telemetry reports how the platform is used and data is compressed, encrypted and sent to 1E through email on a configurable schedule. Full details of the Server telemetry data sent to 1E is provided in Server telemetry data.

User Interface telemetry reports how the user interface is used, and data is sent directly from administrator browsers to the 1E Cloud.

1.7.2.11 Branding page

The **Branding** page lets you customize the appearance of the portal and emails to match your corporate style.

1.7.2.11.1 Branding

To view this page and make changes to the appearance of the Tachyon Portal, you need a user with one of the following roles assigned:

- **Infrastructure Administrator**
- **Full Administrator**.

The fields on this page are described in the following table:

Field	Description
Company Name	Set this to the name for your corporation. This name is reserved for use in a future Tachyon application.
Portal Description	Set this to the description for your corporation. This text string can be up to 50 characters long. The contents of this field will appear on the Tachyon Portal landing page.
Company Logo	This field is a drop site where you can drag and drop your company logo. You can also use a local file browser dialog to locate the file by clicking on the **Browse** button in the field. The logo you provide must be .png or .jpg file at least 200 x 200 pixels and square. The maximum size is 100 kB. When uploaded, the logo will appear on the Tachyon Portal landing page and **Switch app** control menu.

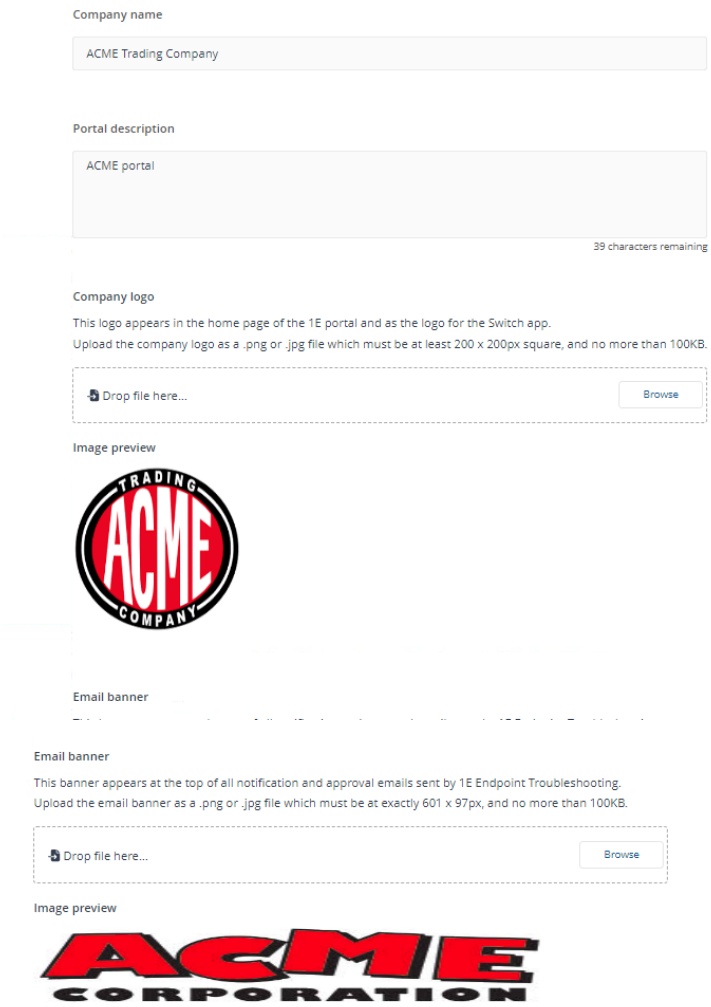
Field	Description
Email Banner	This field is a drop site where you can drag and drop your corporation email banner. You can also use a local file browser dialog to locate the file by clicking on the **Browse** button in the field. The logo you provide must be .png or .jpg ifle and exactly 601 x 97 pixels. The maximum size is 100 kB. When uploaded this banner will appear at the top of all Tachyon emails: verification, approval etc.

1.7.2.11.2 Setting the brand

The pictures show the **Branding** page filled out for the fictional ACME Trading Company Corporation with the following settings:

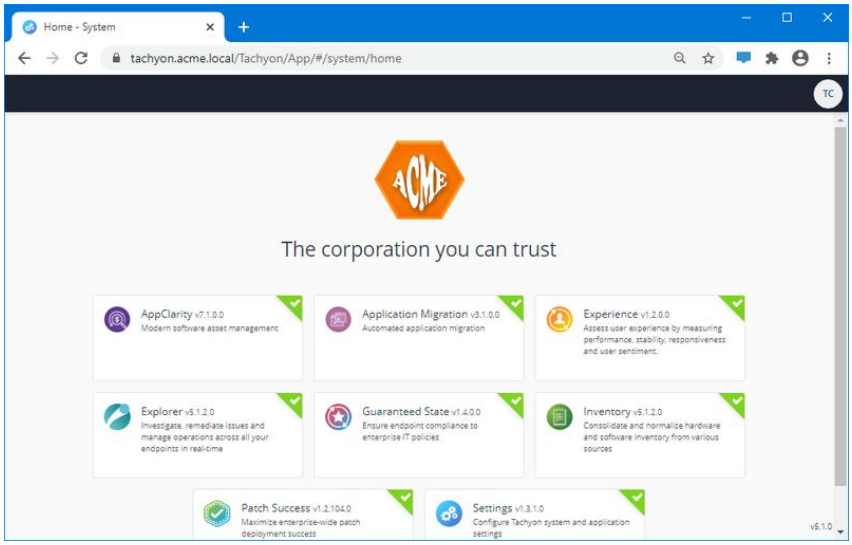
Field	Setting
Company Name	ACME Trading Company
Portal Description	ACME portal
Company Logo	ACME Logo.png
Email Banner	ACME Banner.png

After clicking **Save**, you are prompted to refresh the browser window.



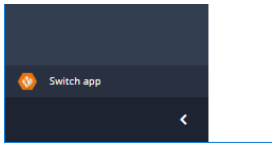
1.7.2.11.2.1 Tachyon Portal with branding

After refreshing the browser, if you navigate to the landing page you will see the new logo and description applied, as shown.



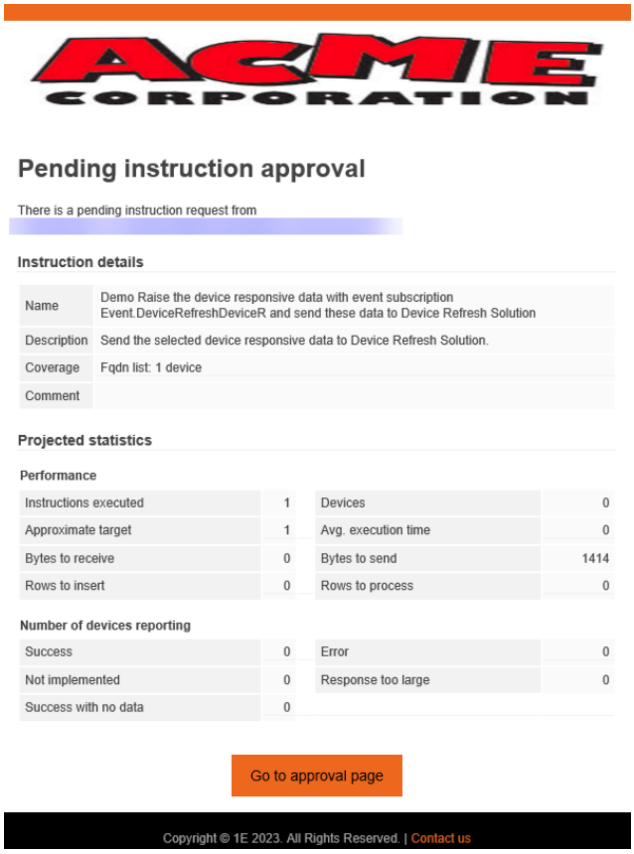
1.7.2.11.2.2 The Switch App menu with branding

The Switch App menu is displayed after you navigate to any of the installed applications. You will see your new logo appear next to the menu title. The picture shows the new logo applied.



1.7.2.11.2.3 A Tachyon email with branding

When Tachyon sends an email it will also apply the banner added and saved on the **Branding** page. The picture shows the ACME banner applied to an authentication email.



1.7.2.11.3 Resetting the branding to the default values

If at any time you want to revert Tachyon to using the default logos and text:

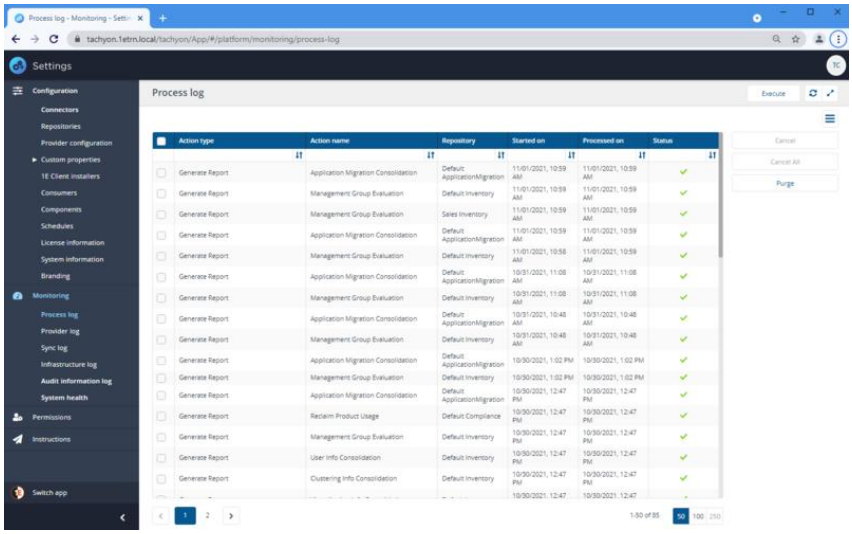
1. Navigate to the **Settings→Configuration→Branding** page.
2. Click on the **Reset** button to display the **Update - Branding** popup.
3. Here you are asked if you want to proceed? To reset the branding click **Yes, Reset & Save**, otherwise click **No**.
4. Clicking on **Yes, Reset & Save** resets the fields of the **Branding** page to their default values.
5. To view the reset you will need to refresh the browser again.

1.7.3 Monitoring Menu

Viewing Tachyon logs.

1.7.3.1 Process log page

The **Process log** page lets you view the progress of queued actions, cancel actions that are pending and purge process log history.



1.7.3.1.1 The Process log table

Column	Description
Action type	The type of action queued. For example **CleanSync** and **Sync Data** might be two actions executed when executing an overall connector sync data action.
Action name	The name of the action being executed. For example **CleanSync - SCCM** and **Sync Data - SCCM** might be two actions executed when executing an overall Configuration Manager sync data action.
Repository	The name of the repository (if any) the action is being performed on. For example **Default Inventory**.
Started on	The date and time the action started.
Processed on	The date and time the action finished.
Status	This indicates the current state for the action and ultimately whether it succeeded, failed or was cancelled. This may be one of the following:

Status	Description
	The action succeeded.
	The action is in progress.
	The action is queued.

Column	Description
	The action has been cancelled.
	The action failed.

1.7.3.1.2 Execute an action

The **Execute** button allows you to *manually* run an action. To *schedule* an action, please refer to Schedules page.

1. Click the **Execute** button.
2. In the **Execute action** popup subsequently displayed, use the **Repository** menu to select the inventory repository you want to populate.
3. Once the repository has been selected you can then select the action to run. In the case of inventory repositories the actions will be restricted to inventory related actions. For a connector you will be looking for an action with the form **Sync Data - <connector name>**.
4. For inventory syncs (where you sync a connector) you have additional options to check as shown in the example picture opposite:

   Warning

   Clean Sync causes deletion of existing data previously imported by the selected combination of **action** and **repository**. Data imported by any other connector actions is left intact and consolidated with new data. To clear all data from a repository, please refer to Clearing data from a repository.

   If **Clean Sync** checkbox is not checked then an incremental sync occurs, consolidating new data with old. An incremental sync is quicker than a clean sync.

   Clean Sync will prevent the Management Groups feature and applications such as Patch Success from working until the sync is complete and new data has been consolidated. This operation should only be performed if you need a clean sync or are experiencing problems with sync times taking too long.

   Note

   Run AI action will cause the AI action to run, this is only available if AI Powered Auto-curation has been enabled. The **Run AI action** checkbox is also available if the selected Action is **Generate Report - Basic Inventory Consolidation**. For detail on how to enable AI Powered Auto-curation the information is on the AI Powered Auto-curation page.

   Note

   Data to Sync allows you to select some or all categories of data supported by the connector.
5. Click the **Execute** button in the **Execute action** popup to start the sync.

6. A popup appears momentarily informing you that the Sync has started and you can monitor progress in the **Process log**.

7. When the sync starts a number of actions are queued to be performed on the selected repository. To check the progress of the sync actions:

    a. Navigate to the **Monitoring→Process log** page.

    b. Here you can see the sequence of actions that have been queued for the selected repository related to the **Sync Data** action selected.

    c. When each action has finished running you'll see a check icon

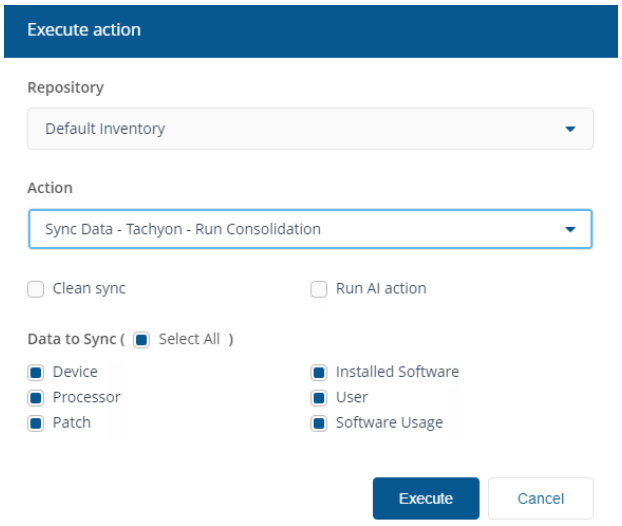
    appear in the **Status** column if it succeeds or a failed icon

    if it fails.

8. Once all the actions have succeeded you can check the results. To do this:

    a. Navigate to the **Monitoring→Sync log** page.

    b. This displays the items that have been added to the selected repository as a result of running the sync.



Note

The **Execute** button is also available on the Connectors page: Execute a connector sync action.

1.7.3.1.3 Cancelling actions

You can use the **Cancel** button to cancel individual actions or the **Cancel All** button to cancel all running or stuck actions.

Note

Only Full Administrators have permission to use the **Cancel All** and **Purge** buttons.

The**Cancel**button is used to cancel multiple or individual pending queued actions, you can do this by:

1. Select the queued

   action(s) you want to cancel from the **Process log** table by checking the box at the left-hand end of each action's row.

2. If any of the selected actions is queued the **Cancel** button will be enabled.

3. Click the **Cancel** button.

4. The **Cancel actions** popup asks if you want to proceed.

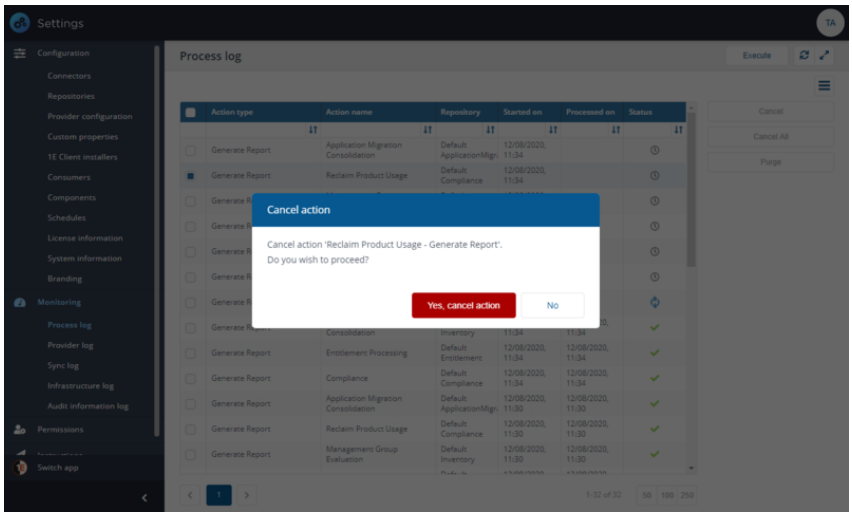
5. To proceed and cancel the selected queued actions click the **Yes, cancel actions** button.

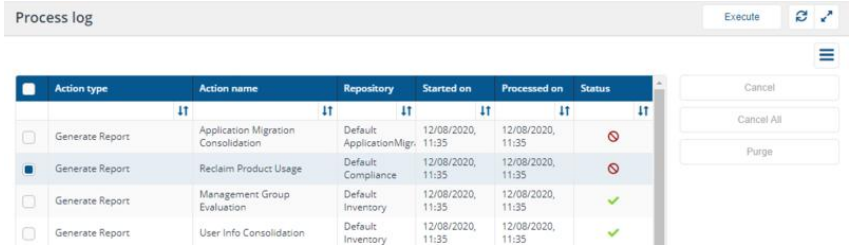
6. The actions will not longer be run and the status of the selected queued actions will change to cancelled

   .

Note

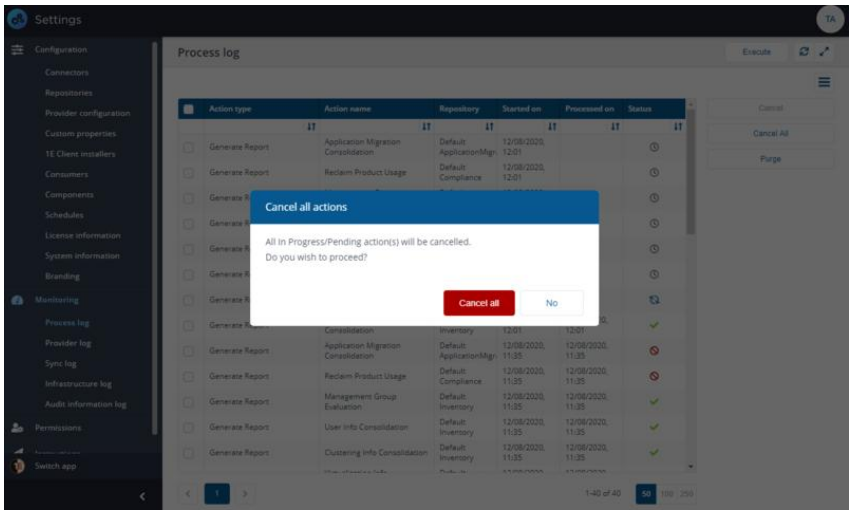
When one action is selected, all the dependent actions are also cancelled.

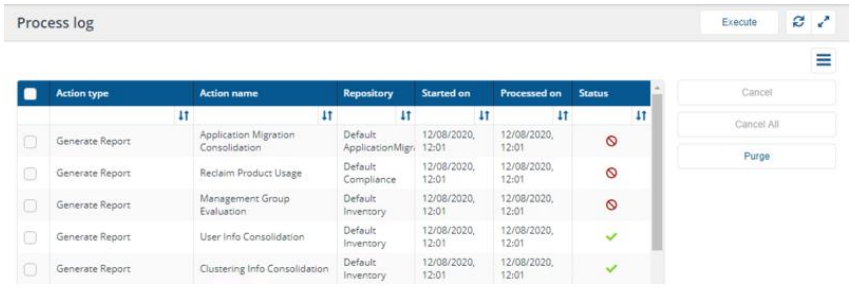




The **Cancel All** button can be used to cancel all currently running or stuck actions. You do not need to select an individual action before doing this.

You'll see a warning message if **Cancel All** is clicked, then all actions will be cancelled.





1.7.3.1.4 Purge logs

You can purge the entire Process Log history by:

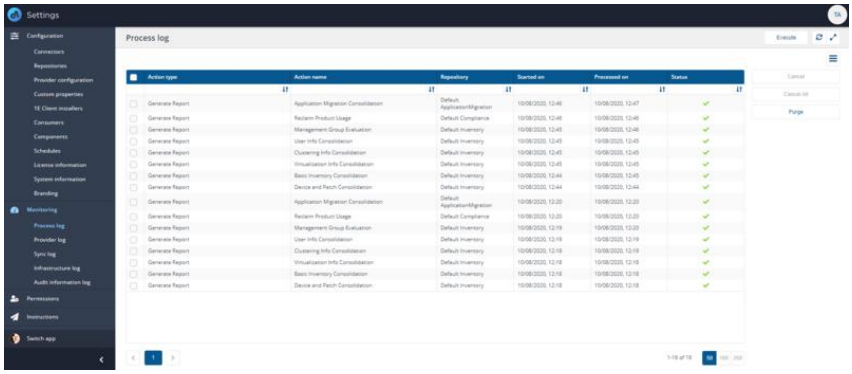
1. Clicking the **Purge** button.
2. The **Purge logs** popup asks if you want to proceed.
3. To proceed and purge the logs, click the **Yes, purge** button.
4. The Process log is then purged of all items.

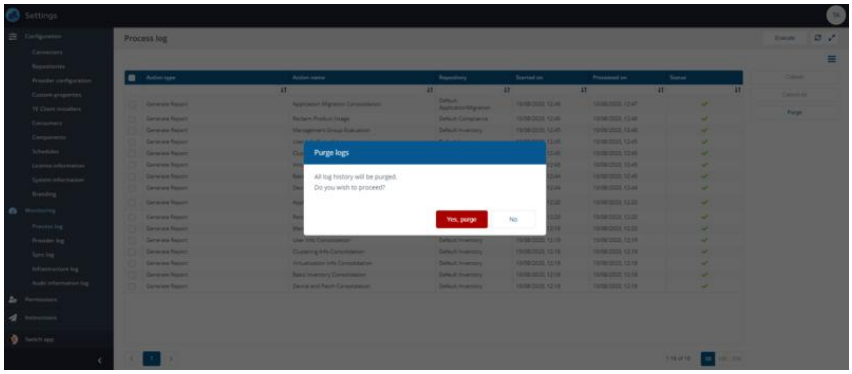
Note

If any **Action type** items are selected the **Purge** button will be disabled.

Note

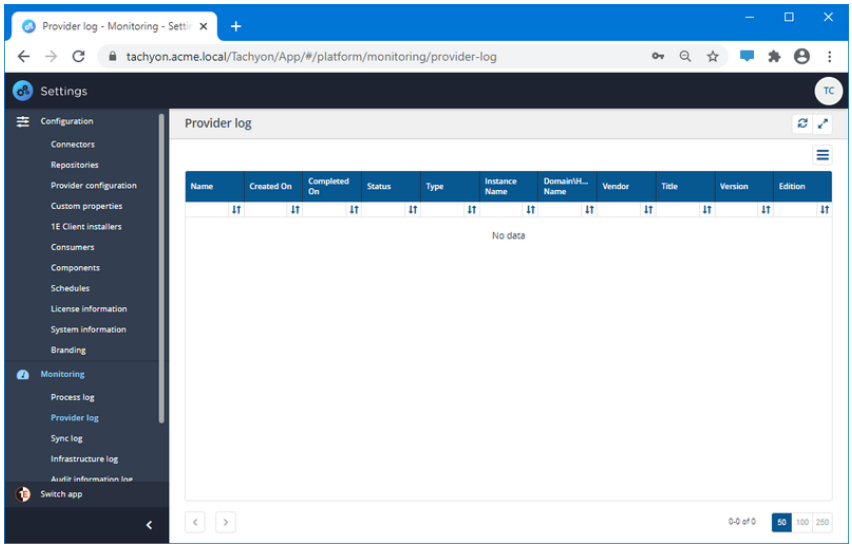
Only Full Administrators have permission to use the **Cancel All** and **Purge** buttons.





1.7.3.2 Provider log page

The **Provider log** page lets you view status log events related to Tachyon Provider operations.



1.7.3.2.1 The Provider log table

The columns in the **Provider log** are described in the following table:

Column	Description
Name	Shows the source of the Provider operation.
Created On	The date the Provider operation was created.
Completed On	The date the Provider operation completed.
Status	The current status of the Provider operation.

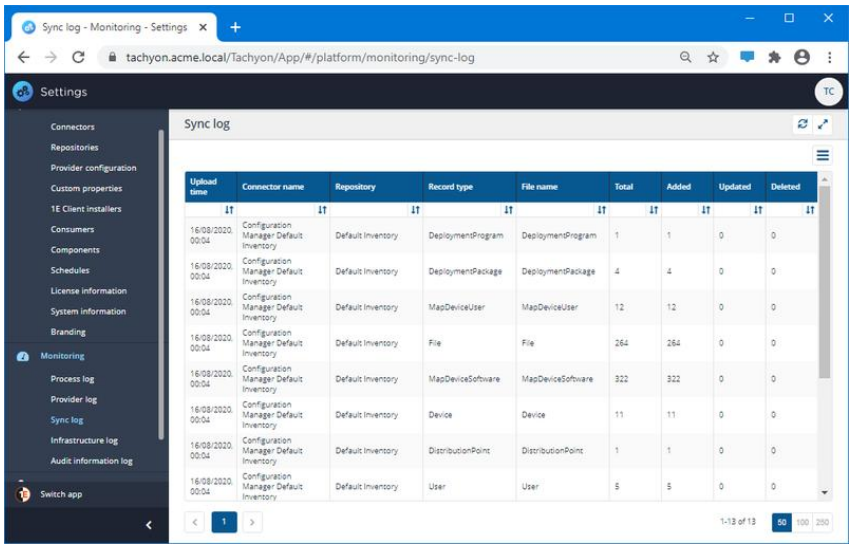
State	Description
NotStarted	The Provider operation does not yet have an assigned Provider. When one is found the operation state will be set to Pending.
InProgress	The Provider operation is currently being run.
Pending	The Provider operation has an assigned Provider but has not yet started to run.
Completed	The Provider operation has completed.
Failed	If a Provider operation is taking too long to complete it will be stopped and enter a Failed state. Provider operations in this state will then try to find another Provider to assign.
Cancelled	Cancelled Provider operations are stopped before they reach the Completed state, they take no further action and do not try to find another Provider to assign.

Type	The operation type.
Instance Name	The repository name where the Provider operation was created.
Domain\Host Name	The domain and device name where the Provider operation is run.
Vendor	The Vendor details for Product related Provider operations.
Title	The Title details for Product related Provider operations.
Version	The Version details for Product related Provider operations.

Column	Description
Edition	The Edition details for Product related Provider operations.

1.7.3.3 Sync log page

The **Sync log** page lets you review the records that have been added to repositories as a result of syncing connectors.



1.7.3.3.1 The Sync log table

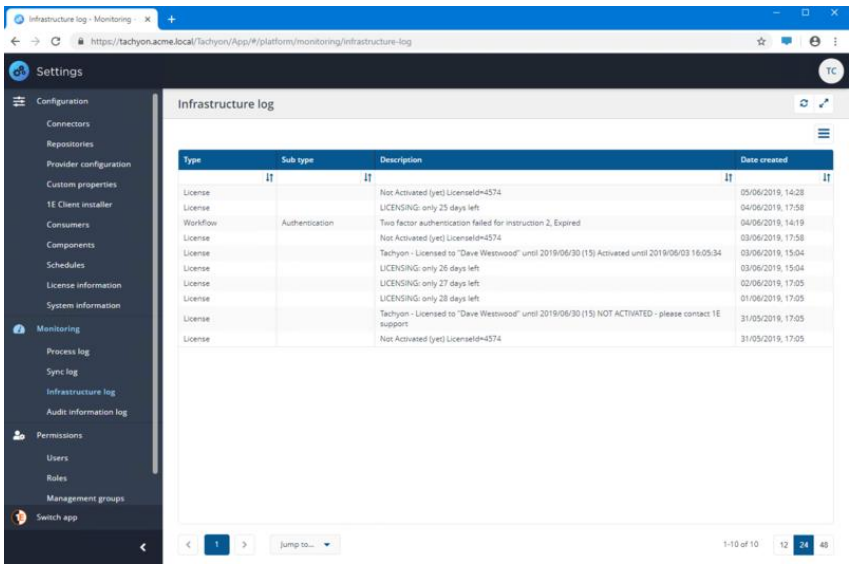
The **Sync log** table displays a list of records that have been uploaded to repositories by connectors. The columns displayed are described in the following table:

Column	Description
Upload time	The date and time the specific record type was uploaded.
Connector name	The name of the connector that uploaded the record type.
Repository	The name of the repository the record type was uploaded to.
Record type	The type of record uploaded.
File name	The file name created internally for this record type.
Total	The total number of records related to this record type sourced during the synchronization event.

Column	Description
Added	The number of records added to the platform for this record type.
Updated	The number of records that were updated as a result of uploading the record type.
Deleted	The number of records that were removed as a result of uploading the record type.

1.7.3.4 Infrastructure log page

The **Infrastructure log** page lets you view status log events related to the Tachyon infrastructure.



1.7.3.4.1 The Infrastructure log table

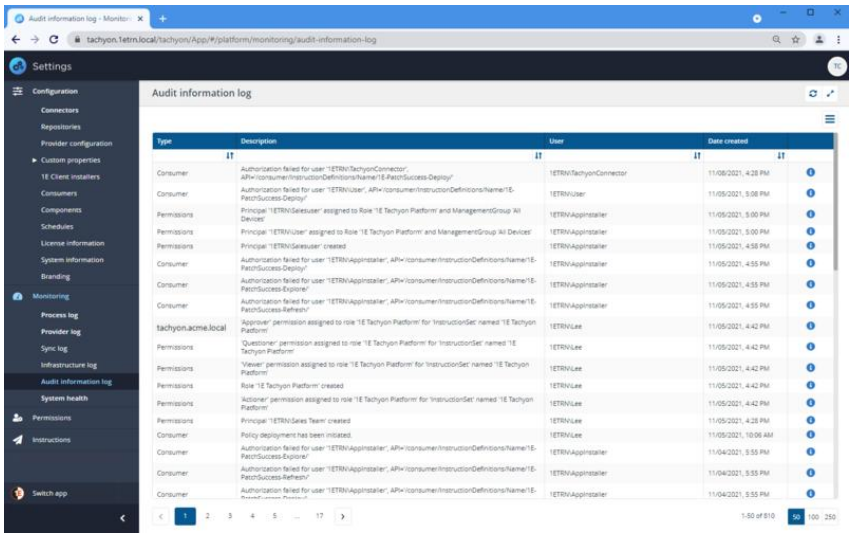
The columns in the **Infrastructure log** are described in the following table:

Column	Description
Type	Shows the type of event being logged. For example a **Workflow** event.
Sub type	Shows the sub type (if any) for more general type events. For example **Email Notification** is a sub type of a **Workflow** event.
Description	The description of the event. For example **Failure sending mail. Unable to connect to the remote server No connection could be**

Column	Description
	made because the target machine actively refused it shows a workflow event cause by a failure to connect to the specified mail server.
Date created	The date the event was created.

1.7.3.5 Audit information log page

The **Audit information log** page lets you view information on who is using Tachyon what actions they are performing.



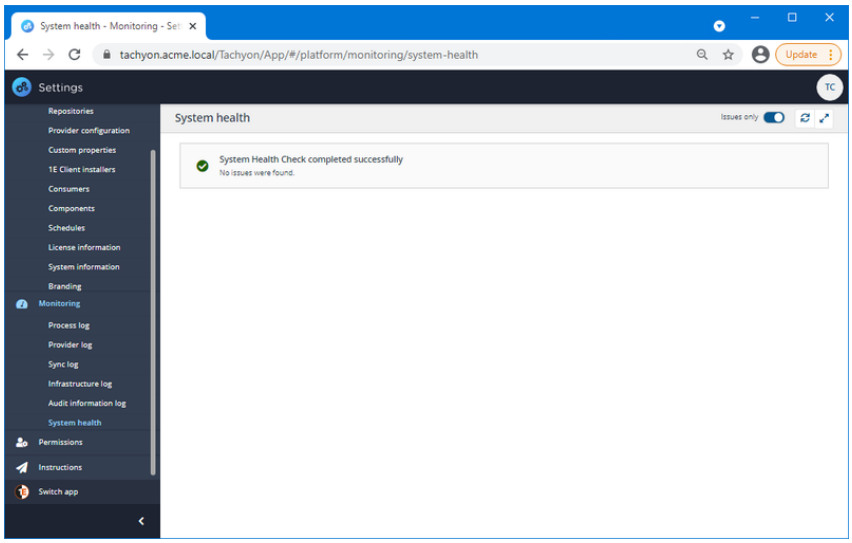
1.7.3.5.1 The Audit information log table

Column	Description
Type	The type of event. For example **Instruction Onboarding** events let you know who has been loading instructions into Tachyon.
Description	Description of the actual event that occurred. For example **Instruction definitions added to Instruction set 'Verification'** lets you know that some instructions were added to a particular instruction set.
User	The user who performed the action being logged. For example **ACME\TCNInstaller01** identifies the user who added instruction definitions to an instruction set.

Column	Description
Date created	The date and time the logged action occurred.
Detail message	Clicking the icon displays the **Detail message** for that row as a pop-up. The popup provides additional information related to the log item.

1.7.3.6 System health page

The **System Health** page runs a comprehensive series of component checks. By default, it shows issues, but you can see a full list of green lights by toggling **Issues only**.



1.7.3.6.1 Looking at the health checks

1.7.3.6.1.1 Showing all the checks

By default, the System health page shows only the checks where issues have been identified, unless there are no issues, in which case it displays an all clear message. You can set the page to show all the checks by toggling the **Issues only** switch to off in the banner for the page. The picture shows this and the types of check that will be subsequently displayed.

1.7.3.6.1.2 Showing the check details

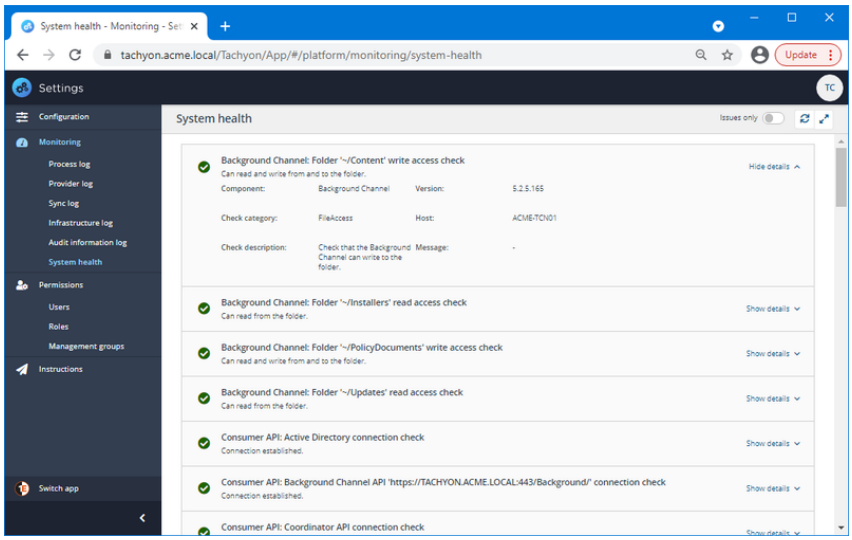
You can also expand each check to view the details related to it by clicking on the **Show details** link at the top-right of the check's entry in the System health table. The picture shows the **Background Channel Folder write access check** expanded.

When expanded you can see the following information for each check:

Information	Description
Component	The name for the component.
Version	The component version number.
Check category	The category the check belongs to.
Host	The host device the component is running on.
Check description	The description for the check being made.
Message	Any messages that have been generated by running the check.

Note

You will see four SLA Integrate errors after installation, which will disappear after you have installed a Connector.



1.7.3.6.2 The health checks

The following table provides an overview of all the health checks made by Tachyon:

Component	Check	Description
Background Channel	Folder '~/Content' write access check	Check that the Background Channel can write to the "Content" folder within the app pool user context.

Component	Check	Description
Folder '~/Installers' read access check	Check that the Background Channel can read from the "Installers" folder within the app pool user context.	
Folder '~/Policy Documents' write access check	Check that the Background Channel can write to the "PolicyDocuments" folder within the app pool user context.	
Folder '~/Updates' read access check	Check that the Background Channel can read from the "Updates" folder within the app pool user context.	
Consumer API	Active Directory connection check	Check that Consumer API can connect to Active Directory. *Uses the configured GC or LDAP connection string.*
Background Channel API connection check(s)	Check that Consumer API can connect to Background Channel API. *Uses the URL(s) stored in the TachyonMaster database.*	
Coordinator API connection check	Check that Consumer API can connect to Coordinator API. *Uses the OperationalSafeGuardsUrl application setting.*	
Core API '<Core server>'	Check that Consumer API can connect to Core API.	

Component	Check	Description
connection check(s)	*Uses the URL(s) stored in the TachyonMaster database.*	
Tachyon Master database connection check	Check that Consumer API can connect to the TachyonMaster database. *Uses the configured connection string (TachyonMaster) within the app pool user context.*	
TachyonResponse database connection check(s)	Check that Consumer API can connect to the TachyonResponse database(s). *Uses the stored connection strings within the TachyonMaster database under the app pool user context.*	
Coordinator service Agent Deployment module	Background Channel API connection check	Check that Coordinator Agent Deployment module can connect to Background Channel API. *Uses the URL(s) stored in the TachyonMaster database.*
Coordinator service Licensing module	Check license service URL	Verify that license service URL is from a trusted issuer.
Check license validity	Verify license expiry date.	

Component	Check	Description
Check trust with licensing component	Verify trust between coordinator and licensing component by comparing signatures between the licensing module DLL and licensing DLL.	
Coordinator service Management Groups module	Management Group API connection check	Check that Coordinator Management Groups module can connect to SLA Management Group API using the configured URL. *Uses the SLAEndpoint module setting.*
Coordinator service Policy module	Background Channel API connection check	Check that Coordinator Policy Module can connect to Background Channel API. *Uses the URL(s) stored in the TachyonMaster database.*
Coordinator service	Active Directory connection check	Check that Coordinator can connect to Active Directory. *Uses the configured GC or LDAP connection string.*
Coordinator certificate check	Check that Coordinator has a valid certificate used for the SSL API communication.	
SMTP connection check	Check that Coordinator can connect to the SMTP server using the "EHLO" command. *Only shown if SMTP emails has been enabled.*	

Component	Check	Description
Tachyon Master database connection check	Check that Coordinator can connect to the TachyonMaster database. *Uses the configured connection string (TachyonMaster) within the app pool user context.*	
Website application authentication check	Check that Consumer API site has Windows authentication enabled and that Anonymous authentication is disabled.	
Website certificate binding check	Check that Consumer API has a valid certificate binding.	
Core	TachyonMaster database connection check	Check that Core can connect to TachyonMaster database. *Uses the configured connection string (TachyonMaster) within the app pool user context.*
TachyonResponse database connection check(s)	Check that Core can connect to TachyonResponse database(s). *Uses the stored connection strings within the TachyonMaster database under the app pool user context.*	
SLA Admin	Consumer API connection check	Check that SLA Admin can connect to the Consumer API. *Uses the PermissionCheckerRootUrl application setting.*

Component	Check	Description
SLA Platform API connection check	Check that SLA Admin can connect to the SLA Platform API.	
SLA-Data database connection check	Check that SLA Admin can connect to the SLA-Data database. *Uses the configured connection string (DefaultCustomerConnection) within the app pool user context.*	
SLA-Shared database connection check	Check that SLA Admin can connect to the SLA-Shared database. *Uses the configured connection string (DefaultSharedConnection) within the app pool user context.*	
SLA Engine	1ECatalog database connection check	Check that SLA Engine can connect to the 1ECatalog database. *Uses the BaseUri application setting to request the 1ECatalog connection string from the SLA Platform API. The database connection check is performed within the service user context.*
Catalog API connection check	Check that SLA Engine can connect to the Catalog API. *Uses the URL retrieved from the SLA-Data.Component table for 1E Catalog within the service user context.*	

Component	Check	Description
Consumer API connection check	Check that SLA Engine can connect to the Consumer API. *Uses the TachyonConsumerRootUrl application setting.*	
SLA Platform API connection check	Check that SLA Engine can connect to the SLA Platform API. *Uses the BaseUri application setting.*	
SLA-Data database connection check	Check that SLA Engine can connect to the SLA-Data database. *Uses the configured connection string (DefaultCustomerConnection) within the service user context.*	
SLA-Shared database connection check	Check that SLA Engine can connect to the SLA-Shared database. *Uses the configured connection string (DefaultSharedConnection) within the service user context.*	
SLA Integrate Agent service *(part of SLA Integrate services)*	Folder '<ConnectorsRoot>' write access check	Check the SLA Integrate Agent can write to the 'dir-connectors' folder within the service user context.

Component	Check	Description
Folder '<Installer Root>' write access check	Check the SLA Integrate Agent can write to the 'dir-job-output' folder within the service user context.	
Folder '<JobOutputRoot>' write access check	Check the SLA Integrate Agent can write to the 'dir-job-output' folder within the service user context.	
SLA Integrate Manager connection check	Check that the SLA Integrate Agent can connect to the SLA Integrate Manager. *Uses the rest-api-address application setting.*	
SLA Platform API connection check	Check that the SLA Integrate Agent can connect to the SLA Platform API. *Uses the rest-api-address application setting to request the SLA Platform API address from the SLA Integrate Manager.*	
SLA Integrate Manager service *(part of SLA Integrate services)*	Folder '<InstallerRoot>' write access check	Check the SLA Platform Integrate Manager can write to the 'dir-installers' folder within the service user context.

Component	Check	Description
Folder '<JobOutputRoot>' write access check	Check the SLA Platform Integrate Manager can write to the 'dir-job-output' folder within the service user context.	
SLA Platform API connection check	Check that SLA Integrate Manager can connect to the SLA Platform API. *Uses the sla-data-address application setting.*	
SLA-Integrate database connection check	Check the SLA Integrate Manager service can connect to the SLA-Integrate database. *Uses the configured connection string (default) within the service user context.*	
SLA Platform Integrate Agent	Check at least one SLA Platform Integrate Agent has reporting health status.	
SLA Platform API *API includes the UI* *The following are not checked:* • *SLA I*	1ECatalog database connection check	Check that SLA Platform API can connect to the 1ECatalog database. *Uses the configured connection string (DefaultCatalogConnection) within the app pool user context.*

Component	Check	Description
nventory • *SLA Operations Provider API*		
Consumer API connection check	Check that SLA Platform API can connect to Consumer API. *Uses the PermissionCheckerRootUrl application setting.*	
SLA-Data database connection check	Check that SLA Platform API can connect to the SLA-Data database. *Uses the configured connection string (DefaultCustomerConnection) within the app pool user context.*	
SLA-Shared database connection check	Check that SLA Platform API can connect to the SLA-Shared database. *Uses the configured connection string (DefaultSharedConn*	

Component	Check	Description
	ection) within the app pool user context.	
SLA Engine	Check the SLA Engine has reported health status.	
Switch *Switch Host is not checked*	Core Connect (Device)	Check if this Switch can connect to core Device endpoint.
Core Connect (Instructions)	Check if this Switch can connect to core Instructions endpoint.	
Core Connect (Policy Response)	Check if this Switch can connect to core Policy Response endpoint.	
Core Connect (Policy)	Check if this Switch can connect to core Policy endpoint.	
Core Connect (Response)	Check if this Switch can connect to core Response endpoint.	
Core Connect (Switch)	Check if this Switch can connect to core Switch endpoint.	
Recent administrative events.	Check if this Switch has had any recent errors or warnings (since last instruction poke)	

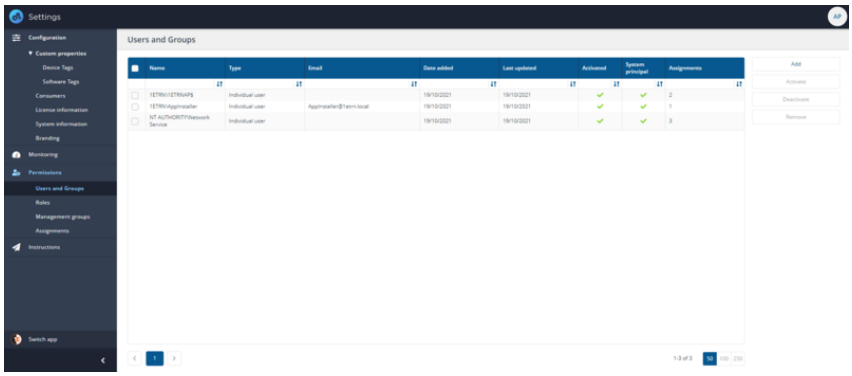
1.7.4 Permissions Menu

Configuring Tachyon users, roles, and management groups.

1.7.4.1 Users and Groups page

The **Users and Groups** page lets you view and manage current Tachyon users, from this page you can:

- Add new users and groups
- Reactivate deactivated users and groups
- Deactivate selected users and groups
- Remove users and groups
- View the details for particular users, groups and set their roles.



1.7.4.1.1 How to define Tachyonusers and set their access rights

Tachyon users are added using their Active Directory properties, fetched by Tachyon through a direct search of Active Directory. A Tachyon user may be defined as either a domain account or a security group. When using security groups, we recommend the use of Universal groups, as these will be compatible with any potential future changes to your AD infrastructure. Refer to Active Directory for more details.

Once a user or group has been added to Tachyon, you can then set any Tachyon roles to define what access they have to Tachyon features.

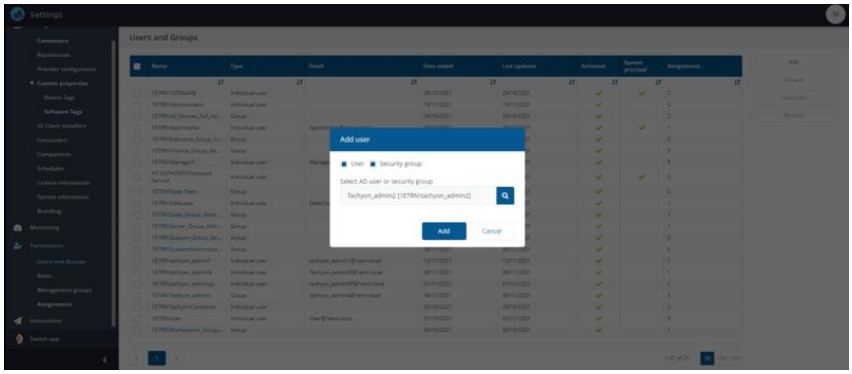
The following sections outline the steps to create a user and assign their access rights, for more details please see Configuring Access Rights - tutorial, which provides a step-by-step worked example.

1.7.4.1.1.1 Adding Tachyon users

1. Log on to the Tachyon portal using a user account with the **Full Administrator**, or the **Installer** role if it is a new installation.
2. Navigate to the **Settings**→**Permissions**→**Users and Groups** page.
3. Click on the **Add** button, doing this displays the **Add user** popup.

4. In the **Select AD user or security group** field, type the name, or part of the name, for the Active Directory user or security group that you want to add, then click the search icon.

5. Select the Active Directory user or security group from the list of matching names displayed in the drop-down list and click **Add**.



1.7.4.1.1.2 Adding Tachyon roles to users or groups

Once added to Tachyon, you can use **Assignments** to edit the roles for a Tachyon user or group:

1. On the **Settings→Permissions→Users and Groups** page, click on the **Assignments** link for the user or group you want to add the role to, this displays the Assignments page focused on the selected user.

2. On the Assignments page, the focus is on **Users and Groups**.

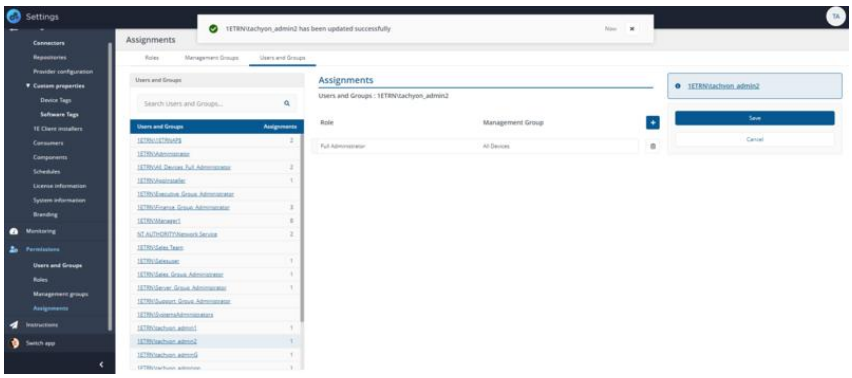
3. Click the plus sign button to add a **Role** and your choice of associated **Management Group**.

4. Once you've selected your Tachyon Roles and Management Groups, click the **Save** button.

Refer to the Assignments page for details about the Assignments page and walkthroughs of how to use the feature.

Refer to the Management Groups page for details about how you can use Management Groups to determine:

- Targets for questions, actions and reporting
- User permissions for targeting to particular devices based on management group membership.



1.7.4.1.2 Deactivating or removing Tachyon users or groups

Tachyon lets you add Active Directory users or security groups as users. It also provides a means for deactivating and removing those users. It's worthwhile discussing when you should use deactivate and when you should use remove.

1.7.4.1.2.1 Deactivating Tachyon users or groups

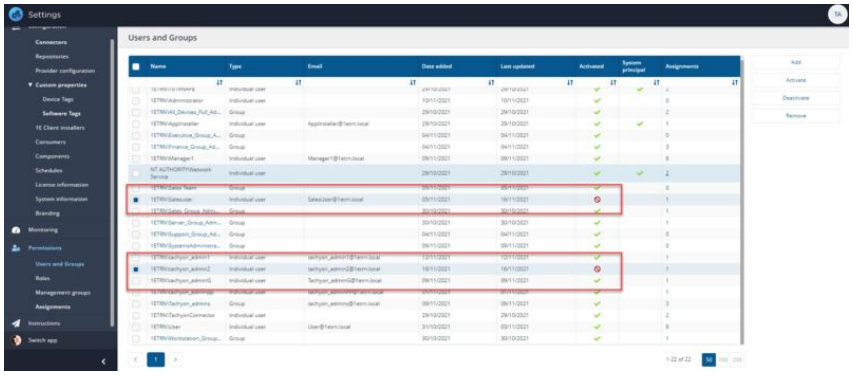
You can deactivate existing users if you need to temporarily prevent them from using the Tachyon portal without permanently removing all of their set roles.

To deactivate a user:

1. Navigate to the **Settings→Permissions→Users and Groups** page.
2. Check the checkbox at the left-hand end of one or more users you want to deactivate.
3. Click the **Deactivate** button.
4. The icon in the **Activation** column will change to

   , indicating that the user is now deactivated.
5. After deactivating, the selected user will no longer be able to perform further actions in the Tachyon portal (for any current sessions) and will not be able to log in to the portal for any subsequent sessions.

Deactivated users can be re-activated at a later date and all of their set roles will be re-instated. This does not affect any other Tachyon roles associated with the user or group by virtue of their membership of other Tachyon groups.



1.7.4.1.2.2 Re-activating Tachyon users or groups

You can re-activate currently deactivated users or groups to grant them access to the Tachyon portal.

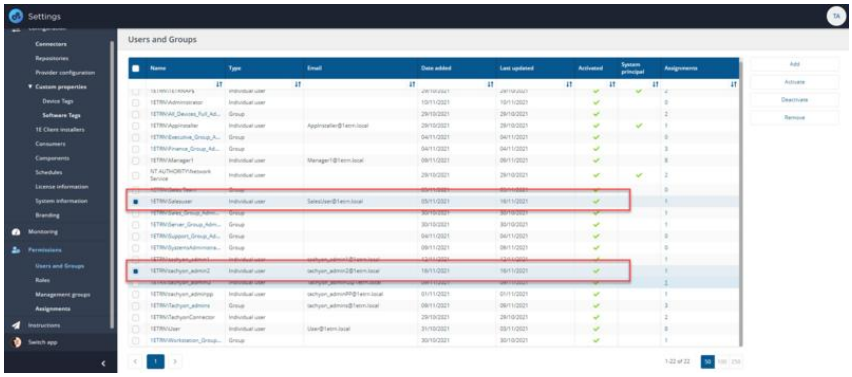
To re-activate a user:

1. Navigate to the **Settings→Permissions→Users and Groups** page.
2. Check the checkbox at the left-hand end of the user entry you want to re-activate.

3. Click the **Activate** button.
4. The icon in the **Activation** column will change to

   ✔

   , indicating that the user is now activated.
5. After activating, the selected user will be able to log in to the Tachyon portal and perform their permitted functions as before.



1.7.4.1.2.3 Removing users

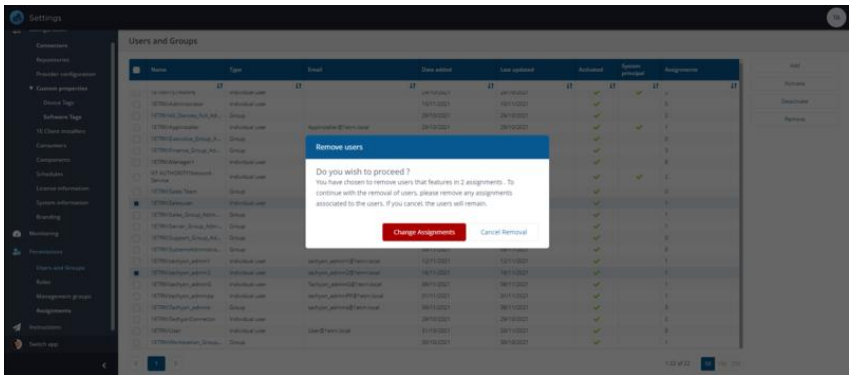
Use remove to delete the particular associations for the specific user or group with their roles. This does not affect any other roles associated with the user or group by virtue of their membership of other groups.

You can permanently remove one or more users or groups if they are no longer needed. Doing this removes any associations to roles.

To remove a user:

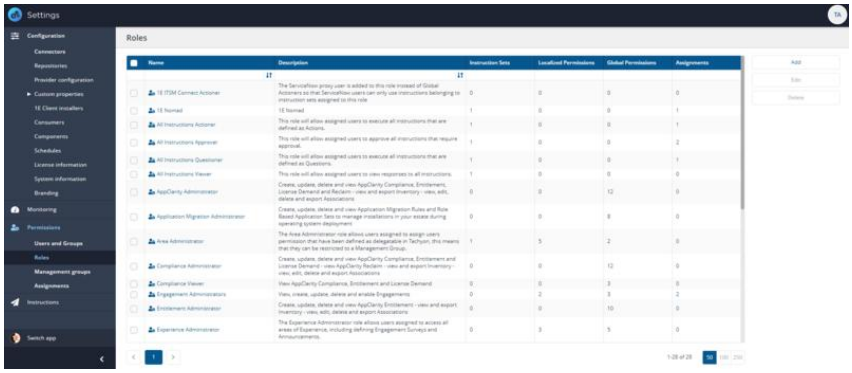
1. Navigate to the **Settings→Permissions→Users and Groups** page.
2. Check the checkbox at the left-hand end of the users you want to remove.
3. Click the **Remove** button.
4. A **Remove group** or **Remove user** popup will be displayed asking if you want to proceed with the removal of the selected group or user.
5. To proceed and remove them from Tachyon, you will need to remove any associated assignments, click the **Change Assignments** or **Cancel Removal** button.
6. The **Change Assignments** button launches the **Assignments** page, select the user or group you want to remove and delete any assignments they have using the trash can icon, click **Save**.
7. Navigate back to the **Users and Groups** page, re-select the user or group you want to remove, click **Remove**.
8. Click the **Yes, remove group** or **Yes, remove user** button, depending on whether it was a group or user being removed.

From this point on, all the associations for that user or group and their roles will be removed from Tachyon. If you did want to add them back in at a later date, you would have to rebuild them step by step.



1.7.4.2 Roles page

The **Roles** page lets you view system roles and currently defined custom roles. From here you can edit Role permissions and go into each role to set its users and group assignments and any associated management groups.



1.7.4.2.1 Tachyon roles

There are two types of roles that can be applied to the Tachyon users, system roles, and custom roles.

Tip

On the Roles page, you can see at a glance which Tachyon roles are system or custom roles, by using the icon in the **Name** column:

- System roles are indicated by an icon with a padlock

- Custom roles are indicated by an icon with a cog wheel

1.7.4.2.1.1 System and custom roles

Refer to Roles and Securables for a complete reference for the following:

- Platform system roles.
- The custom roles used by 1E applications.
- For customers upgrading from Tachyon Platform 5.2 or earlier, a list of role names that are automatically renamed.

1.7.4.2.2 Recommendations for using the Full Administrator role

The **Full Administrator** role can be used to provide across-the-board permissions to a user. While this may be convenient in certain circumstances, you should be aware that this is a powerful role and should be used with appropriate caution.

1.7.4.2.2.1 Using Full Administrator in a lab environment

To get things up and running quickly in a lab environment, you may choose to make the Setup user account a Full Administrator during installation on the Identity Providers page in 1E Setup. This will help minimize the number of users required for an evaluation and reduce the initial configuration required.

If the Setup user account was not elevated during setup then it will only have limited access and as this is a system principal user the permissions are locked down by default. You can allow it to assume the Full Administrator role using the following steps:

1. Add an Azure Active Directory group to 1E permissions
2. Apply the 1E Full Administrator role to this group.
3. Add the Setup user account to the same Azure Active Directory group.

In the short term, it's fine to make use of full administrators in this way, but this practice is not really suitable for large-scale deployments and should be used with care for the following reasons:

- The Full Administrator role has permission to do everything in 1E. It has across-the-board permissions to all Instruction Sets and therefore can be used to run actions that can have a major impact on your network.
- The Full Administrator accounts receive emails for all the transactions that are performed by 1E.

1.7.4.2.3 Different approaches for defining permissions

1E provides a flexible system for defining permissions for the features. There are a number of different ways of approaching the task, here we outline the general choices that can be made for assigning 1E users to system and custom roles.

1.7.4.2.3.1 Managing access primarily using the Tachyon Permissions console

In this approach, Tachyon users are added individually using their Active Directory credentials. This approach is more secure than alternatives because all users, roles, and access rights are managed only through the Tachyon Permissions console.

1.7.4.2.3.2 Managing access using Active Directory

Using this approach, Tachyon users are added as Active Directory security groups. Tachyon roles are then associated with those groups, and management of the individual users who can access Tachyon is subsequently done only through Active Directory. There are broadly three options when using this approach:

1. A one-to-one approach where you create a Tachyon-specific role-based Active Directory group for each Tachyon role. For example, you could create a **TCNGApprovers** Active Directory security group, and add that group as a user in Tachyon, and then assign the **All Instructions Approver** role to the user.
2. A many-to-one approach, where you use one or more of your existing role-based Active Directory groups for each Tachyon role. For example, you could use the Active Directory groups for your desktop and help desk teams, create a Tachyon user for each group, and then assign the Tachyon role to all those Tachyon users.
3. A mixture of the above

Note

It is possible for an Active Directory user to be associated with roles for both running and approving actions. In practice, this is safe because Tachyon prevents users from being able to directly approve their own actions regardless of the roles they have been assigned.

1.7.4.2.4 Defining a custom Instruction set 1E role

If you want to base your 1E permissions around access to specific Instruction sets, you will need to create custom 1E roles. The Custom roles section lists built-in custom roles used by 1E Applications.

To create a custom role:

1. Navigate to the **Settings**→**Permissions**→**Roles** page.
2. Click the **Add** button to start the add role process.
3. In the **New Role** page subsequently displayed set the **Name** and **Description**.
4. With the **Instruction Sets** tab selected, select your required Instruction Sets from the list.
5. Set the Instruction set access rights by checking the required **Actioner**, **Approver**, **Questioner** and **Viewer** checkboxes.
6. When the associated rights have been set click **Save** to save your changes and automatically return to the **Roles** page.
7. You can now add assignments of users and groups and management groups to the new custom role by clicking the link in the **Assignments** column.
8. Click the **+** (plus icon) to add a new item and, from the **Users and Groups** drop-down menu either search for, or select the users or groups you want to associate the role with.

9. From the **Management Group** drop-down menu either search for, or select the management group you want to associate the role with. This can either be the built-in **All Devices** or a management group you have created in **Settings→Permissions→Management groups**.

10. Click the **Save** button to associate the selected options with the custom role.

The following rights can be set for an Instruction set, these relate to the primary operator roles of the 1E system:

Right	Description
Actioner	Able to run actions defined in the Instruction Set.
Approver	Able to approve actions defined in the Instruction Set for anyone other than self. If email is enabled, will receive an approval request email for each requested action in the Instruction Set.
Questioner	Able to ask questions defined in the Instruction Set.
Viewer	Able to view responses to questions run from the Instruction Set.

Note

For details about how to load Instruction Definitions into 1E and then create, populate and delete Instruction sets, refer to the Instructions Menu page.

1.7.4.3 Configuring Access Rights - tutorial

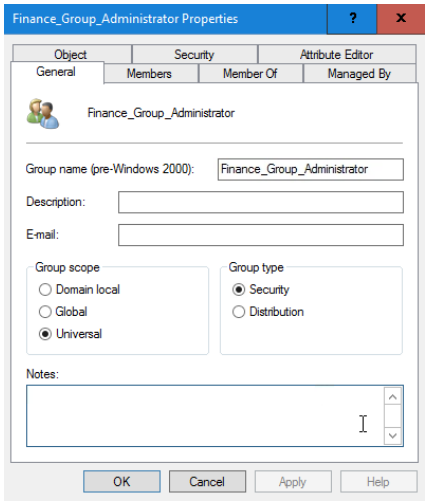
A quick tutorial on configuring access rights for Tachyon. Using a scenario where access to Tachyon will be managed through Active Directory groups, the tutorial illustrates the general setup required and the particular steps needed to add users.

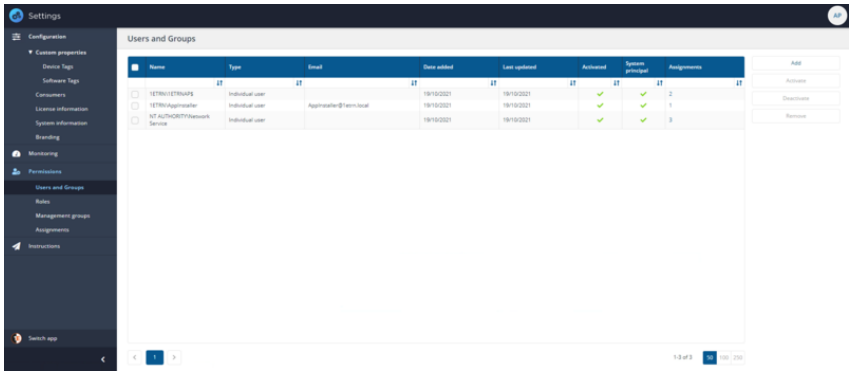
In this tutorial

In this tutorial we demonstrate a process for creating Active Directory (AD) managed permissions to the Tachyon portal. We use specifically created AD groups for each of the Tachyon system roles and create users for each one, we then define a custom role for a specific Instruction Set and create a user with an existing AD group that provides access to running actions in the Instruction Set.

1.7.4.3.1 Example AD group a Tachyon system role

As mentioned in Users and Groups page, we recommend that the AD security groups used for defining access to the Tachyon portal features are defined as **Universal** groups. The picture shows an example AD **Finance_Group_Administrator** security group intended for a **Group administrator** role. In our example, the **Finance_Group_Administrator** AD group is for workstation administrators of an AD OU called **Finance**.





1.7.4.3.2 1E roles

In this tutorial we will create an example 1E Azure Active Directory group user based on the possible roles given in the following 1E system and custom roles.

> **Tip**
>
> On the Roles page, you can see at a glance which 1E roles are system or custom roles, by using the icon in the **Name** column:

- System roles are indicated by an icon with a padlock

- Custom roles are indicated by an icon with a cog wheel

1.7.4.3.2.1 System and custom roles

Refer to Roles and Securables for a complete reference for the following:

- Platform system roles.
- The custom roles used by 1E applications.
- For customers upgrading from Tachyon Platform 5.2 or earlier, a list of role names that are automatically renamed.

1.7.4.3.3 Creating 1E users or groups

The general steps for creating a new user or group are as follows:

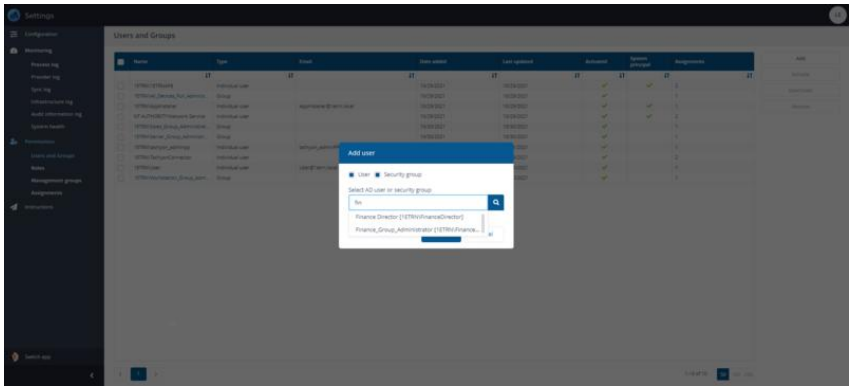
1.7.4.3.3.1 Adding 1E users

1. Log on to the 1E portal using a 1E user account with the **Full Administrator**, or the **Installer** role if it is a new 1E installation.
2. Navigate to the **Settings→Permissions→Users and Groups** page.
3. Click on the **Add** button, doing this displays the **Add user** popup.
4. In the **Select user or group** field, type the name, or part of the name, for the user or group that you want to add, then click the search icon.
5. Select the user or group from the list of matching names displayed in the drop-down list and click **Add**.

On the **Settings→Permissions→Users and Groups** page, after clicking the **Add** button, the **Add user** popup is displayed.

In the **Select user** edit field we type **FIN** because it is the first few characters of our group in our environment.

We then select the **Finance_Group_Administrator** group from the list. Once the group has been selected we click **Add** to create the new 1E user.



We then click the new **Finance_Group_Administrator** account's **Assignments** link to display the details for that group on the **Assignments** page.

> **Tip**
>
> Clicking the name of the group displays any AD accounts you have added to the Universal group using **Active Directory Users and Computers**.

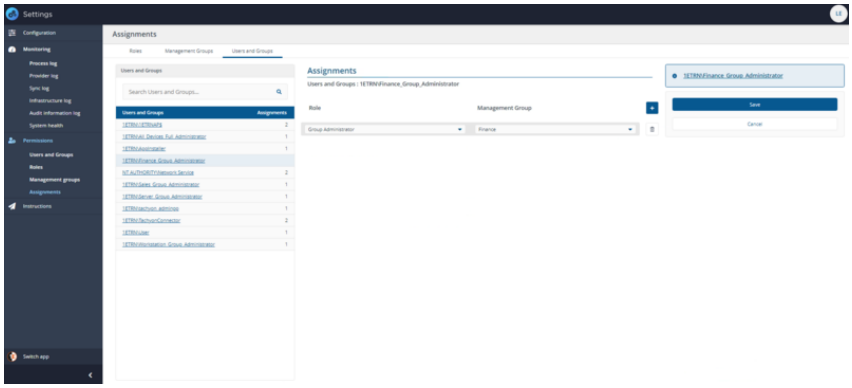
From here we can add assignments to our group account and the Management Group they will apply to.

In this case we choose the **Group Administrator** role for our **Finance** Management Group. We do not want our administrators for the Finance division to work on servers, or on devices belonging to other departments who have their own administrators, once we are satisfied with the changes, we click **Save**.

> **Note**

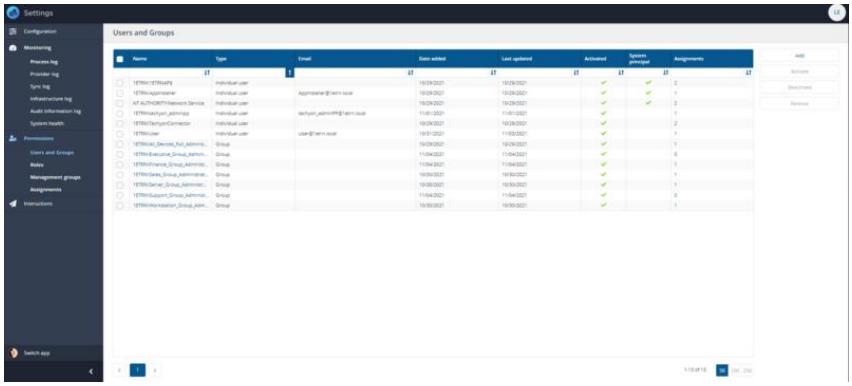
Refer to the Roles page for details about creating custom roles and a list of all built-in custom roles used by Tachyon Applications.

After the new user or group has just been added, 1E will display notifications for a short while showing the actions that have just been successfully performed.



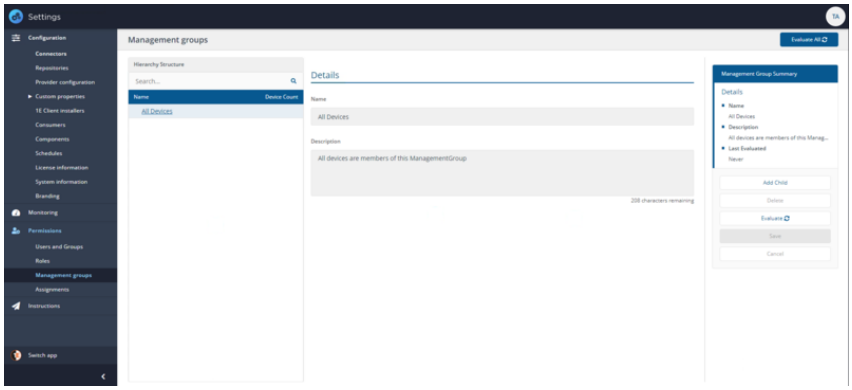
In the tutorial we then repeat the process of finding groups, adding 1E roles and saving for each of the 1E system roles. The purpose of this is that subsequently, specific user access to 1E can be managed through your Identity Provider using membership of selected groups and avoiding the necessity of managing the users through 1E.

The result of adding the groups can be seen in the picture.



1.7.4.4 Management Groups page

Management Groups are containers used to group devices and the software installed on those devices. Management Groups are defined using configurable rules that look at various properties of the devices and their installed software, these are then evaluated to determine the group membership. This means that Management Group membership adapts to changes to the devices and software in your environment.



1.7.4.4.1 Management Groups overview

Management Groups are used by 1E to determine:

- The targets for questions, actions, and reporting
- User permissions for targeting to particular devices based on Management Group membership.

In terms of permissions for determining how 1E users interact with the devices in your network, Management Groups work alongside Instruction sets.

In 1E, Management Groups are created in two different ways:

- **Rule based** - the page lets you add, edit, delete and evaluate Management Groups that are based on rules
- **Direct based** - these use scripts to create Management Groups by importing lists of devices using FQDN names only, this type of Management Group has no associated rules and cannot be edited and evaluated from the Management Groups page. 1E recommends using the 1E PowerShell Toolkit.

Both types of Management Group have the following properties:

- Each device known to 1E can be assigned to any number of Management Groups.
- Roles can be associated with specific Management Groups, so that users with those roles will only be able to target the devices in their Management Groups
- Management Groups can only contain devices, and they are completely independent of any other Management Group, even if they contain the same devices
- Each Management Group must have a unique name which is not case-sensitive.

Note

Please note the following considerations:

- Devices not assigned to any child Management Group will still be accessible, as all devices are members of the default **All Devices** Management Group
- Child Management Groups can only be created under the default **All Devices** Management Group

- The maximum number of child Management Groups are four (Five, including **All Devices**)
- However, there is no current limit on the number of child or "sibling" Management Groups which can be created.

1.7.4.4.1.1 Permissions

The following roles can add Users and Groups, Roles, Management Groups, Assignments, and Delegation:

- Full Administrator
- Group Administrator - cannot create roles unless they are delegated.

You can find out more about the system and custom roles available in 1E on the Roles page.

1.7.4.4.1.2 Connectors

Management Groups use device data stored in an Inventory repository, which is populated using one or more inventory connectors, as described in Connectors page. This is sufficient for inventory-based applications like AppClarity, Application Migration, and Patch Success.

If you want client-based applications like Explorer, Experience and Guaranteed State to use the Management Groups, then you must add a Tachyon Connector, which synchronizes its own data with inventory data. The username and password you provide for the Connector must be a valid user and belong to the **Management Group Administrator** role. Please refer to the Tachyon connector page for more details. You only require to configure the connector, you do not need to schedule or run the Tachyon connector unless you also want to collect data from clients.

> **Note**
>
> To take advantage of your Configuration Manager database and pull in its inventory and usage data, you'll need to configure a System Center Configuration Manager connector in your Tachyon system.

1.7.4.4.2 Creating direct-based Management Groups

Direct-based Management Groups are created using scripts. Two sample PowerShell scripts are provided.

- Each script creates a new log file in the same folder, with file name format as **<scriptname>_<ddMMyyyyhhmmss>.log** which must be deleted manually.
- If a Management Group already exists with the same name, the script will delete and recreate it, only with the new devices provided
- If the file or collection includes a device that is not present in the Tachyon Inventory repository, then it is ignored, and logged
- After a successful run, the script triggers a Management Group sync.

Once imported into Tachyon, your direct-based Management Groups will be added as child groups of the default **All Devices** Management Group.

1.7.4.4.2.1 Prerequisites

- User must have read/write permission in the folder where the PowerShell script is present
- User must use **UseCustomCredentials** parameter if the current logged-in user does not have permission in Tachyon to create Management Groups
- If Windows Task Scheduler is used to run a script, then the scheduled task should provide the current logged-in user.

1.7.4.4.2.2 Create Direct-based Management Groups from a file

Note

This script has changed to support an API change in Platform 8.1

Create-DirectManagementGroupUsingFile.ps1, to view and copy the script, click **Read more...**

Create-DirectManagementGroupUsingFile.ps1

```
<#
.SYNOPSIS
1E Tachyon – Create Direct Management Group
Copyright © 1e Ltd 2022 - all rights reserved
http://www.1e.com

Version 2.0

Disclaimer
Your use of this software is at your sole risk. All software is provided "as-is
", without any warranty, whether express or implied, of accuracy, completeness,
fitness for a particular purpose, title or non-infringement, and none of the so
ftware is supported or guaranteed by 1E. 1E shall not be liable for any damages
you may sustain by using this software, whether direct, indirect, special, inci
dental or consequential, even if it has been advised of the possibility of such
damages.

If you have an issue using this software, please ensure you are using an unmodi
fied version before contacting 1E Support.


.DESCRIPTION
This script reads the Device FQDN list in files and creates Direct Membership M
anagement Groups through SLA/Tachyon APIs. If the group does not exist
it is created and devices are added. If the group exists, the existing devices
are deleted and new devices are added.


.PARAMETER TachyonApiBaseUrl
Mandatory parameter.  The header name used to access the Tachyon web service.
Should match the header listed in the IIS bindings on the Tachyon server.

.PARAMETER FolderPath
Mandatory parameter.  The name of the input folder which contains the files to
```

```
be used in creating Direct Membership Management Groups. These files contain
the list of devices to be used in creating Management Groups.  The File name sh
ould be same as the name of Name of Management Group. Also, the first line
of the file should contain the description of Management Group to be created, f
rom next line onwards every line contains the Device FQDN.

.PARAMETER UseCustomCredentials
Optional switch.  If UseCustomCredentials is used, User will be prompted to ent
er the credentials, otherwise the script will use default credentials.


.EXAMPLE
.\Create-DirectManagementGroupUsingFile.ps1 -TachyonApiBaseUrl https://tachyon.
lab.local -FolderPath C:\Temp\MgFolder

Scenario:
A Tachyon server is accessed using URL https://tachyon.lab.local/Tachyon using
default credentials.  The files containing the Device FQDN list
is in the directory C:\Temp\MyFolder.

.EXAMPLE
..\Create-DirectManagementGroupUsingFile.ps1 -TachyonApiBaseUrl https://tachyon
.lab.local -FolderPath C:\Temp\MgFolder -UseCustomCredentials

Scenario:
A Tachyon server is accessed using URL https://tachyon.lab.local/Tachyon using
different credentials other than current default credentials.
The files containing the Device FQDN list is in the directory C:\Temp\MyFolder.

#>

param(
    [Parameter(Mandatory=$true, HelpMessage="Enter Tachyon API Base URL e.g. :
https://tachyon.testlab.com")]
    [ValidateNotNullOrEmpty()]
    [string] $TachyonApiBaseUrl,

    [Parameter(Mandatory=$true, HelpMessage="Enter Folder Path which contains f
iles containing Device FQDN list")]
    [ValidateNotNullOrEmpty()]
    [string] $FolderPath,

    [Parameter(Mandatory=$false, HelpMessage="To use Custom Credentials other t
han windows default credentials")]
    [Switch] $UseCustomCredentials
)

$ScriptVersion = "2.0" # Update the script version here

function Write-Log {
```

```
    [CmdletBinding()]
    Param(
          [parameter(Mandatory=$true)]
          [String]$Path,

          [parameter(Mandatory=$true)]
          [String]$Message,

          [parameter(Mandatory=$true)]
          [String]$Component,

          [Parameter(Mandatory=$true)]
          [ValidateSet("Debug", "Info", "Message", "Warning", "Error")]
          [String]$Type
    )

    switch ($Type) {
        "Info" { [int]$Type = 1 }
        "Warning" { [int]$Type = 2 }
        "Error" { [int]$Type = 3 }
        "Debug" { [int]$Type = 4 }
        "Message" { [int]$Type = 5 }
    }

    # Create a log entry
    $Content = "<![LOG[$Message]LOG]!>" +`
        "<time=`"$(Get-Date -Format "HH:mm:ss.ffffff")`" " +`
        "date=`"$(Get-Date -Format "M-d-yyyy")`" " +`
        "component=`"$Component`" " +`
        "context=`"$([System.Security.Principal.WindowsIdentity]::GetCurrent().
Name)`" " +`
        "type=`"$Type`" " +`
        "thread=`"$([Threading.Thread]::CurrentThread.ManagedThreadId)`" " +`
        "file=`"`">"

    try {
        # Write the line to the log file
        Add-Content -Path $Path -Value $Content
    }
    catch {
        Write-Host "User does not have access to write log at path $Path"
        Write-Host $Message
    }

    if ($Type -eq 1) {
        Write-Host $Message -ForegroundColor Yellow
    }

    if ($Type -eq 3) {
```

```
        Write-Host $Message -ForegroundColor Red
    }

    if ($Type -eq 5) {
        Write-Host $Message
    }
}

function Invoke-DirectMgApi{
    [CmdletBinding()]
    Param(
          [parameter(Mandatory=$true)]
          [String]$uri,

          [parameter(Mandatory=$true)]
          [String]$payload,

          [parameter(Mandatory=$false)]
          [System.Management.Automation.PSCredential]$credential
    )

    $hdrs = @{
        "Accept" = "application/json"
        "Content-type" = "application/json"
        "X-Tachyon-Consumer" = "Platform"
    }

    try {
        $stopwatchApi =  [system.diagnostics.stopwatch]::StartNew()

        $Content = "Invoking API"
        Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation
.MyCommand.Name -Type Message

        [Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType
]::Tls -bor [Net.SecurityProtocolType]::Tls11 -bor [Net.SecurityProtocolType]::
Tls12

        if($credential){
            $response = Invoke-RestMethod -Method POST -Uri $uri -Body $payload
-Credential $credential -Headers $hdrs
            $Content = "Response from API : $response"
            Write-Log -Path $LogFilePath -Message $Content -Component $MyInvoca
tion.MyCommand.Name -Type Message
        }
        else {
            $response = Invoke-RestMethod -Method POST -Uri $uri -Body $payload
-UseDefaultCredentials -Headers $hdrs
            $Content = "Response from API : $response"
            Write-Log -Path $LogFilePath -Message $Content -Component $MyInvoca
```

```
tion.MyCommand.Name -Type Message
        }

        $stopwatchApi.Stop()

        $Content = "Time taken by API : $($stopwatchApi.Elapsed.TotalSeconds) s
econds"
        Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation
.MyCommand.Name -Type Message
    }
    catch {
        $err = $_

        $Content = "An error occured : $($err.Exception)"
        Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation
.MyCommand.Name -Type Error

        $Content = "Error Details : $($err)"
        Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation
.MyCommand.Name -Type Debug
    }
}

# Get the Current Directory
$CurrentDirectory = $PSScriptRoot

if ($UseCustomCredentials -eq $true) {
    $cred = Get-Credential
}

$LogFilePath = Join-Path $PSScriptRoot "$($MyInvocation.MyCommand.Name)_$(Get-D
ate -Format ddMMyyyyHHmmss).log"

$Content = "************************************************"
Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation.MyComma
nd.Name -Type Debug

$Content = "Starting script"
Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation.MyComma
nd.Name -Type Debug

$Content = "************************************************"
Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation.MyComma
nd.Name -Type Debug

$Content = "Running Script Version: " + $ScriptVersion
Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation.MyComma
nd.Name -Type Debug

# Get the Current Directory
```

```
$Content = "Current Directory is " + $CurrentDirectory
Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation.MyComma
nd.Name -Type Debug

$Content = "Tachyon API Base URL: " + $TachyonApiBaseUrl
Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation.MyComma
nd.Name -Type Message

$Content = "Folder Path containing Device list files: " + $FolderPath
Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation.MyComma
nd.Name -Type Message

$Content = "Verifying Folder Path : $FolderPath"
Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation.MyComma
nd.Name -Type Debug

if (!(Test-Path $FolderPath)) {
    $Content = "Folder path does not exist : $FolderPath"
    Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation.MyC
ommand.Name -Type Error

    exit
}

$Content = "Fetching all supported files from folder"
Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation.MyComma
nd.Name -Type Debug
$files = Get-ChildItem -Path $FolderPath -Filter *.txt

$Content = "Total Files in folder $FolderPath : $($files.Count)"
Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation.MyComma
nd.Name -Type Debug

foreach($file in $files)
{
    $fileFullPath = $file.FullName

    $Content = "Reading File : $fileFullPath"
    Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation.MyC
ommand.Name -Type Message

    $stopwatchFileRead =  [system.diagnostics.stopwatch]::StartNew()

    $fqdnList = New-Object System.Collections.Generic.List[System.Object]

    foreach($line in [System.IO.File]::ReadLines($fileFullPath))
    {
        if($line -ne ""){
            $fqdnList.Add($line.Trim())
```

```
        }
    }

    if($fqdnList.Count -lt 2){
        $Content = "No device present in file"
        Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation
.MyCommand.Name -Type Error

        Continue
    }

    #File name is Management Group Name
    $MGName = $file.BaseName

    #First line of the file is the Management Group Description
    $MgDescription = $fqdnList[0]

    #Removing the first line from collection as it's MG description
    $fqdnList.RemoveAt(0)

    $uploadModelObject = [PSCustomObject]@{
        Name     = $MGName
        Description = $MgDescription
        Devices    = $fqdnList
    }

    $payload = ConvertTo-Json $uploadModelObject

    $stopwatchFileRead.Stop()

    $Content = "Time taken in reading file : $($stopwatchFileRead.Elapsed.Total
Seconds) seconds"
    Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation.MyC
ommand.Name -Type Debug

    $Content = "Creating Management Group -"
    Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation.MyC
ommand.Name -Type Info

    $Content = "  Name : $MGName"
    Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation.MyC
ommand.Name -Type Message

    $Content = "  Description : $MgDescription"
    Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation.MyC
ommand.Name -Type Message

    $Content = "  Total Devices in file : $($fqdnList.Count)"
    Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation.MyC
ommand.Name -Type Message
```

```
    #trimming any white space if any in the begining or end in url
    $TachyonApiBaseUrl = $TachyonApiBaseUrl.Trim()

    $uri = "$TachyonApiBaseUrl/admin/managementgroups/upload"

    $Content = "URI : $uri"
    Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation.MyC
ommand.Name -Type Debug

    Invoke-DirectMgApi -uri $uri -payload $payload -Credential $cred

}

$Content = "Complete"
Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation.MyComma
nd.Name -Type Message
```

```
.\Create-DirectManagementGroupUsingFile.ps1 -TachyonApiBaseUrl https://tachyon.
testlab.com -FolderPath C:\Temp\DeviceFolder -UseCustomCredentials
```

Parameter name	Mandatory	Description
TachyonApiBaseUrl	Yes	Platform base URL, for example: https://tachyon.lab.local
FolderPath	Yes	Folder path which contains files containing Device FQDN list
UseCustomCredentials	No	Use custom credentials (the script will prompt) otherwise current windows credentials will be used to call APIs.

1. Create a folder which will contain text files to create Management Groups. This is the FolderPath passed as a parameter in the PowerShell script.
2. Create text files in the above folder with the name same as Management Group(e.g. ManagementGroupName.txt)
   - Enter **Management Group Description** in first line
   - Enter one or more **Device FQDN** from second line onwards, one device per line.
3. Optionally add more files if you want to create multiple Management Groups.
4. Execute the PowerShell script.

Note

To ensure all devices are present in the Tachyon Inventory repository, ensure you have configured a Connectors page for the inventory source you are using to create your device lists.

1.7.4.4.2.3 Create Direct-based Management Groups from a Configuration Manager collection

Note

This script has changed to support an API change in Platform 8.1

Create-DirectManagementGroupUsingCmCollection.ps1, to view and copy the script, click **Read more...**

Create-DirectManagementGroupUsingCmCollection.ps1

```
<#
.SYNOPSIS
1E Tachyon – Create Direct Management Group
Copyright © 1e Ltd 2022 - all rights reserved
http://www.1e.com

Version 2.0

Disclaimer
Your use of this software is at your sole risk. All software is provided "as-is
", without any warranty, whether express or implied, of accuracy, completeness,
fitness for a particular purpose, title or non-infringement, and none of the so
ftware is supported or guaranteed by 1E. 1E shall not be liable for any damages
you may sustain by using this software, whether direct, indirect, special, inci
dental or consequential, even if it has been advised of the possibility of such
damages.

If you have an issue using this software, please ensure you are using an unmodi
fied version before contacting 1E Support.


.DESCRIPTION
This script reads the memberships of ConfigMgr Collections (Both Direct and Que
ry based membership) and creates Direct Membership Management
Groups through SLA/Tachyon APIs. If the group does not exist it is created, and
devices are added. If the group exists, the existing devices
are deleted and new devices are added. The script is designed to run from the C
onfigMgr server It queries WMI and gets the information
necessary to connect to the ConfigMgr's site namespace.


.PARAMETER TachyonApiBaseUrl
Mandatory parameter.  The header name used to access the Tachyon web service.
Should match the header listed in the IIS bindings on the Tachyon server.

.PARAMETER FilePath
Mandatory parameter.  The name of the input file which contains the list of col
lections to be used in creating Direct Membership Management Groups.  Each line
in file
contains Collection Name, Management Group Name, and Management Group Descripti
on; all three values separated by a comma.
```

```
e.g.
Collection 1,Management Group 1, Management Group 1 Description
Collection 2,Management Group 2, Management Group 2 Description

.PARAMETER UseCustomCredentials
Optional switch.  If UseCustomCredentials is used, User will be prompted to ent
er the credentials, otherwise the script will use default credentials.

.EXAMPLE
.\Create-DirectManagementGroupUsingCmCollection.ps1 -TachyonApiBaseUrl https://
tachyon.lab.local -FilePath C:\Temp\Collection.txt

Scenario:
A Tachyon server is accessed using URL https://tachyon.lab.local/Tachyon using
default credentials.  The file containing the list of collections to process
is in the location C:\Temp\Collection.txt.

.EXAMPLE
..\Create-DirectManagementGroupUsingCmCollection.ps1 -TachyonApiBaseUrl https:/
/tachyon.lab.local -FilePath C:\Temp\Collection.txt -UseCustomCredentials

Scenario:
A Tachyon server is accessed using URL https://tachyon.lab.local/Tachyon using
different credentials other than current default credentials.
The file containing the list of collections to process is in the location C:\Te
mp\Collection.txt.

#>


param(
    [Parameter(Mandatory=$true, HelpMessage="Enter Tachyon API Base URL e.g. :
https://tachyon.testlab.com")]
    [ValidateNotNullOrEmpty()]
    [string] $TachyonApiBaseUrl,

    [Parameter(Mandatory=$true, HelpMessage="Enter File Path which contains col
lection details in csv format. The file should contain Collection Name, Managem
ent Group Name, and Management Group Description")]
    [ValidateNotNullOrEmpty()]
    [string] $FilePath,

    [Parameter(Mandatory=$false, HelpMessage="To use Custom Credentials other t
han windows default credentials")]
    [Switch] $UseCustomCredentials
)

$ScriptVersion = "2.0" # Update the script version here

function Write-log {
```

```
    [CmdletBinding()]
    Param(
          [parameter(Mandatory=$true)]
          [String]$Path,

          [parameter(Mandatory=$true)]
          [String]$Message,

          [parameter(Mandatory=$true)]
          [String]$Component,

          [Parameter(Mandatory=$true)]
          [ValidateSet("Debug", "Info", "Message", "Warning", "Error")]
          [String]$Type
    )

    switch ($Type) {
        "Info" { [int]$Type = 1 }
        "Warning" { [int]$Type = 2 }
        "Error" { [int]$Type = 3 }
        "Debug" { [int]$Type = 4 }
        "Message" { [int]$Type = 5 }
    }

    # Create a log entry
    $Content = "<![LOG[$Message]LOG]!>" +`
        "<time=`"$(Get-Date -Format "HH:mm:ss.ffffff")`" " +`
        "date=`"$(Get-Date -Format "M-d-yyyy")`" " +`
        "component=`"$Component`" " +`
        "context=`"$([System.Security.Principal.WindowsIdentity]::GetCurrent().
Name)`" " +`
        "type=`"$Type`" " +`
        "thread=`"$([Threading.Thread]::CurrentThread.ManagedThreadId)`" " +`
        "file=`"`">"

    try {
        # Write the line to the log file
        Add-Content -Path $Path -Value $Content
    }
    catch {
        Write-Host "User does not have access to write log at path $Path" -Fore
groundColor Yellow
        Write-Host $Message
    }

    if ($Type -eq 1) {
        Write-Host $Message -ForegroundColor Yellow
    }
```

```
    if ($Type -eq 3) {
        Write-Host $Message -ForegroundColor Red
    }

    if ($Type -eq 5) {
        Write-Host $Message
    }
}

function Invoke-DirectMgApi{
    [CmdletBinding()]
    Param(
          [parameter(Mandatory=$true)]
          [String]$uri,

          [parameter(Mandatory=$true)]
          [String]$payload,

          [parameter(Mandatory=$false)]
          [System.Management.Automation.PSCredential]$credential
    )

    $hdrs = @{
        "Accept" = "application/json"
        "Content-type" = "application/json"
        "X-Tachyon-Consumer" = "Platform"
    }

    try {
        $stopwatchApi =  [system.diagnostics.stopwatch]::StartNew()

        $Content = "Invoking API"
        Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation
.MyCommand.Name -Type Message

        [Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType
]::Tls -bor [Net.SecurityProtocolType]::Tls11 -bor [Net.SecurityProtocolType]::
Tls12

        if($credential){
            $response = Invoke-RestMethod -Method POST -Uri $uri -Body $payload
-Credential $credential -Headers $hdrs
            $Content = "Response from API : $response"
            Write-Log -Path $LogFilePath -Message $Content -Component $MyInvoca
tion.MyCommand.Name -Type Message
        }
        else {
            $response = Invoke-RestMethod -Method POST -Uri $uri -Body $payload
-UseDefaultCredentials -Headers $hdrs
            $Content = "Response from API : $response"
```

```
            Write-Log -Path $LogFilePath -Message $Content -Component $MyInvoca
tion.MyCommand.Name -Type Message
        }

        $stopwatchApi.Stop()

        $Content = "Time taken by API : $($stopwatchApi.Elapsed.TotalSeconds) s
econds"
        Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation
.MyCommand.Name -Type Message
    }
    catch {
        $err = $_

        $Content = "An error occured : $($err.Exception)"
        Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation
.MyCommand.Name -Type Error

        $Content = "Error Details : $($err)"
        Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation
.MyCommand.Name -Type Debug
    }
}

function Connect-ConfigMgrModule{
    try {
        # Load CM PowerShell Module

        if (-Not (Test-Path "HKLM:\SOFTWARE\Wow6432Node\Microsoft\ConfigMgr10\A
dminUI")) {
            $Content = "Configuration Manager not found. Pleaes verify if the m
achine has Configuration Manager installed."
            Write-Log -Path $LogFilePath -Message $Content -Component $MyInvoca
tion.MyCommand.Name -Type Error
            exit
        }

        $CMConsolePath = (Get-ItemProperty -Path "HKLM:\SOFTWARE\Wow6432Node\Mi
crosoft\ConfigMgr10\AdminUI" | Select-Object -expandProperty AdminUILog).Replac
e("\AdminUILog\", "")
        if ($CMConsolePath) {
            Import-Module -Name "$CMConsolePath\bin\ConfigurationManager.psd1"
            $Content = "Loaded ConfigurationManager.psd1 module"
            Write-Log -Path $LogFilePath -Message $Content -Component $MyInvoca
tion.MyCommand.Name -Type Debug
        }
        else {
            $Content = "ConfigurationManager.psd1 module not found. Pleaes veri
fy if the machine has Configuration Manager installed."
            Write-Log -Path $LogFilePath -Message $Content -Component $MyInvoca
```

```
tion.MyCommand.Name -Type Error
            exit
        }

        # Get the CM Site Code
        $CMSiteCode = Get-WMIObject -Namespace root\sms -Class SMS_ProviderLoca
tion | Select-Object -expandproperty SiteCode

        if ($CMSiteCode -eq "") {
            $Content = "Sitecode could not be determined."
            Write-Log -Path $LogFilePath -Message $Content -Component $MyInvoca
tion.MyCommand.Name -Type Error
            exit
        }

        $Content = "ConfigMgr Site Code: " + $CMSiteCode
        Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation
.MyCommand.Name -Type Message

        $CMLocation = $CMSiteCode + ":"

        $Content = "Setting Location : $CMLocation"
        Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation
.MyCommand.Name -Type Debug

        Push-Location

        Set-Location -Path $CMLocation
    }
    catch {
        $err = $_

        $Content = "An error occured while loading configuration manager module
: $($err.Exception)"
        Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation
.MyCommand.Name -Type Error

        $Content = "Error Details : $($err)"
        Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation
.MyCommand.Name -Type Debug

        exit
    }


}

function Read-ConfigMgrDeviceCollection{
    [CmdletBinding()]
    Param(
```

```
        [parameter(Mandatory=$true)]
        [hashtable]$collectionList
    )

    try {
        $stopwatch =  [system.diagnostics.stopwatch]::StartNew()

        $arrCMCollList = Get-CMDeviceCollection | Select-Object -Property Colle
ctionID,Name
        ForEach ($CMCollection IN $arrCMCollList){
            $CMCollName = $CMCollection.Name

            $Content = "Retrieved Collection Name from ConfigMgr: " + $CMCollNa
me
            Write-Log -Path $LogFilePath -Message $Content -Component $MyInvoca
tion.MyCommand.Name -Type Debug

            $CMCollId = $CMCollection.CollectionID

            If ($collectionList.ContainsKey($CMCollName)){

                $arrCollectionMembership = Get-CMCollectionMember -CollectionId
$CMCollID | Select-Object -expandProperty Name
                If ($null -ne $arrCollectionMembership){
                    $Content = "Fetching Devices from Collection : " + $CMCollN
ame
                    Write-Log -Path $LogFilePath -Message $Content -Component $
MyInvocation.MyCommand.Name -Type Message

                    $MgName = $collectionList["$CMCollName"][0]
                    $MgDescription = $collectionList["$CMCollName"][1]

                    #Create File to save the device list, which later will be u
sed to create MG
                    $MGFileName = $MgName + ".txt"
                    $MGFilePath = Join-Path $FolderPath $MGFileName
                    if (!(Test-Path $MGFilePath)){
                        $Content = New-Item -itemType File -Path $FolderPath -N
ame $MGFileName
                        Write-Log -Path $LogFilePath -Message $Content -Compone
nt $MyInvocation.MyCommand.Name -Type Debug

                        $Content = "Created file $MGFilePath"
                        Write-Log -Path $LogFilePath -Message $Content -Compone
nt $MyInvocation.MyCommand.Name -Type Debug

                        Add-Content -Path "$MGFilePath" -Value "$MgDescription"

                        $Content = "Added description $MgDescription"
                        Write-Log -Path $LogFilePath -Message $Content -Compone
```

```
nt $MyInvocation.MyCommand.Name -Type Debug
                    }

                    ForEach ($CollMember IN $arrCollectionMembership){
                        $deviceDetails = Get-CMDevice -Name $CollMember -Resour
ce | Select-Object Name,FullDomainName
                        $deviceFullName = $deviceDetails.Name + "." + $deviceDe
tails.FullDomainName

                        $Content = "Adding device: " + $deviceFullName + " to M
G File: " + $MgName
                        Write-Log -Path $LogFilePath -Message $Content -Compone
nt $MyInvocation.MyCommand.Name -Type Debug

                        Add-Content -Path "$MGFilePath" -Value "$deviceFullName
"
                    }
                }

            }
        }

        $stopwatch.Stop()

        $Content = "Time taken in reading devices from Collection : $($stopwatc
h.Elapsed.TotalSeconds) seconds"
        Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation
.MyCommand.Name -Type Message

        Pop-Location

        $Content = "Update location back to local drive"
        Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation
.MyCommand.Name -Type Debug

        $Content = "**********************"
        Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation
.MyCommand.Name -Type Message
    }
    catch {
        $err = $_

        $Content = "An error occured while fetching devices : $($err.Exception)
"
        Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation
.MyCommand.Name -Type Error

        $Content = "Error Details : $($err)"
        Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation
.MyCommand.Name -Type Debug
```

```
        exit
    }


}

# Get the Current Directory
$CurrentDirectory = $PSScriptRoot

#Temp Folder to contain list of devices which will be used to create MG
$MGFolderName = "MGDeviceList"
$FolderPath = Join-Path $CurrentDirectory $MGFolderName

if ($UseCustomCredentials -eq $true) {
    $cred = Get-Credential
}


$LogFilePath = Join-Path $CurrentDirectory "$($MyInvocation.MyCommand.Name)_$(G
et-Date -Format ddMMyyyyHHmmss).log"


$Content = "************************************************"
Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation.MyComma
nd.Name -Type Debug

$Content = "Starting Script"
Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation.MyComma
nd.Name -Type Debug

$Content = "************************************************"
Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation.MyComma
nd.Name -Type Debug

$Content = "Running Script Version: " + $ScriptVersion
Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation.MyComma
nd.Name -Type Debug

$Content = "Current Directory is: " + $CurrentDirectory
Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation.MyComma
nd.Name -Type Debug

$Content = "Tachyon API Base URL: " + $TachyonApiBaseUrl
Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation.MyComma
nd.Name -Type Message

$Content = "File Path containing CM Collection list: " + $FilePath
Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation.MyComma
nd.Name -Type Message
```

```
$Content = "Temp Folder Path to save Device List: " + $FolderPath
Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation.MyComma
nd.Name -Type Message


$Content = "Verifying File Path : $FilePath"
Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation.MyComma
nd.Name -Type Debug

if (!(Test-Path $FilePath)) {
    $Content = "File path does not exist : $FilePath"
    Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation.MyC
ommand.Name -Type Error

    exit
}

try {
    if (!(Test-Path $FolderPath)) {
        $Content = "Creating temp folder : $FolderPath"
        Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation
.MyCommand.Name -Type Debug

        $Content = New-Item -Path "$CurrentDirectory" -Name $MGFolderName -Item
Type "directory"
        Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation
.MyCommand.Name -Type Debug
    }
    else{
        $Content = "Deleting existing MG files from $FolderPath"
        Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation
.MyCommand.Name -Type Debug

        # Delete Collection Membership List Files
        Remove-Item -Path "$FolderPath\*.*"
    }
}
catch {
    $Content = "User does not have permission to create : $FolderPath"
    Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation.MyC
ommand.Name -Type Error

    exit
}

# Read Collection Details from File
$Content = "Reading collection details from $FilePath"
Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation.MyComma
nd.Name -Type Message
```

```
$collectionList = @{}

foreach($line in [System.IO.File]::ReadLines($FilePath))
{
    if($line -ne ""){
        $collectionDetails = $line.Split(",")
        if($collectionDetails.Count -lt 3){
            $Content = "Input data not in correct format. It should contain <Co
llectionName>,<MGName>,<MGDescription>"
            Write-Log -Path $LogFilePath -Message $Content -Component $MyInvoca
tion.MyCommand.Name -Type Error
            exit
        }
        $collectionList.Add($collectionDetails[0],@($collectionDetails[1],$coll
ectionDetails[2]))
    }
}

if($collectionList.Count -lt 1){
    $Content = "No collection details present in file"
    Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation.MyC
ommand.Name -Type Error

    exit
}

#Loading Config Manager Powershell Modules
Connect-ConfigMgrModule

#Read Device Collections from Config Manager and prepare device list in temp fo
lder which will be used to create
Read-ConfigMgrDeviceCollection -collectionList $collectionList

$Content = "Verifying Folder Path : $FolderPath"
Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation.MyComma
nd.Name -Type Debug

if (!(Test-Path $FolderPath)) {
    $Content = "Folder path does not exist : $FolderPath"
    Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation.MyC
ommand.Name -Type Error

    exit
}

$Content = "Fetching all files from folder"
Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation.MyComma
nd.Name -Type Debug
$files = Get-ChildItem -Path $FolderPath -Filter *.txt
```

```
$Content = "Total Files in folder $FolderPath : $($files.Count)"
Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation.MyComma
nd.Name -Type Debug

foreach($file in $files)
{
    $fileFullPath = $file.FullName

    $Content = "Reading File : $fileFullPath"
    Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation.MyC
ommand.Name -Type Message

    $stopwatchFileRead =  [system.diagnostics.stopwatch]::StartNew()

    $fqdnList = New-Object System.Collections.Generic.List[System.Object]

    foreach($line in [System.IO.File]::ReadLines($fileFullPath))
    {
        if($line -ne ""){
            $fqdnList.Add($line)
        }
    }

    if($fqdnList.Count -lt 2){
        $Content = "No device present in file"
        Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation
.MyCommand.Name -Type Error

        Continue
    }

    #File name is Management Group Name
    $MGName = $file.BaseName

    #First line of the file is the Management Group Description
    $MgDescription = $fqdnList[0]

    #Removing the first line from collection as it's MG description
    $fqdnList.RemoveAt(0)

    $uploadModelObject = [PSCustomObject]@{
        Name     = $MGName
        Description = $MgDescription
        Devices    = $fqdnList
    }

    $payload = ConvertTo-Json $uploadModelObject
```

```
    $stopwatchFileRead.Stop()

    $Content = "Time taken in reading file : $($stopwatchFileRead.Elapsed.Total
Seconds) seconds"
    Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation.MyC
ommand.Name -Type Debug

    $Content = "Creating Management Group -"
    Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation.MyC
ommand.Name -Type Info

    $Content = "  Name : $MGName"
    Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation.MyC
ommand.Name -Type Message

    $Content = "  Description : $MgDescription"
    Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation.MyC
ommand.Name -Type Message

    $Content = "  Total Devices in file : $($fqdnList.Count)"
    Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation.MyC
ommand.Name -Type Message

    #trimming any white space if any in the begining or end in url
    $TachyonApiBaseUrl = $TachyonApiBaseUrl.Trim()

    $uri = "$TachyonApiBaseUrl/admin/managementgroups/upload"

    $Content = "URI : $uri"
    Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation.MyC
ommand.Name -Type Debug

    Invoke-DirectMgApi -uri $uri -payload $payload -Credential $cred
}

$Content = "Complete"
Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation.MyComma
nd.Name -Type Message
```

```
.\Create-DirectManagementGroupUsingCmCollection.ps1 -TachyonApiBaseUrl https://
tachyon.testlab.com -FilePath C:\Temp\Collection.txt -UseCustomCredentials
```

Parameter name	Mandatory	Description
TachyonApiBaseUrl	Yes	Platform base URL, for example: https://tachyon.lab.local">https://tachyon.lab.local
FilePath	Yes	File path, which contains details of CM Collections.

Parameter name	Mandatory	Description
UseCustomCredentials	No	Use custom credentials (the script will prompt) otherwise current windows credentials will be used to call APIs.

1. Create a text file which will be passed as a parameter in PowerShell script.
2. In the file enter the following as a comma separated single line:
   Collection name, Management Group Name, Management Group Description
3. Optionally, enter more lines in the same format if you want to create multiple Management Groups.
4. Execute the PowerShell script.

Note

This script is designed to be run on the Configuration Manager Site server.

To ensure all CM devices are present in the Tachyon Inventory repository, ensure you have a System Center Configuration Manager connector and run its Data Sync action to populate the repository.

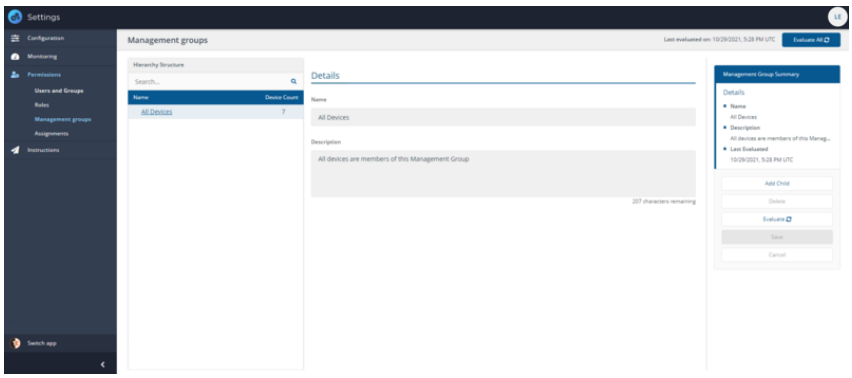
1.7.4.4.3 Working with direct-based Management Groups

Given the information provided in Creating direct-based Management Groups we can now give an example of how direct-based Management Groups can be added.

1.7.4.4.3.1 Before adding the direct-based Management Groups

In our example, we do not have any Management Groups except the default **All Devices** group with a total of all seven devices in our network, as shown in the picture opposite.

Once imported into Tachyon, your direct-based Management Groups will be added as child groups of the default **All Devices** Management Group.

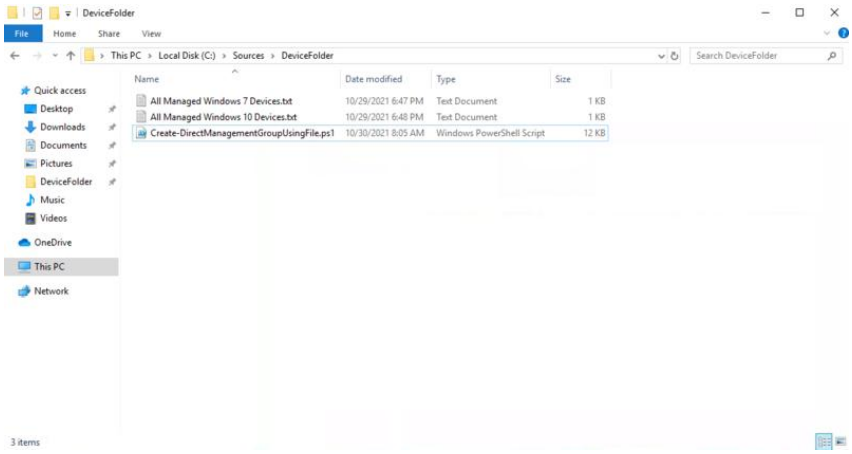


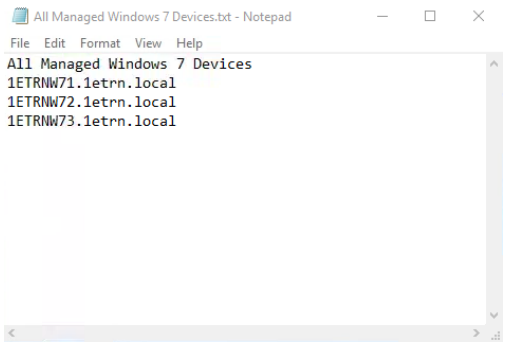
1.7.4.4.3.2 The device files

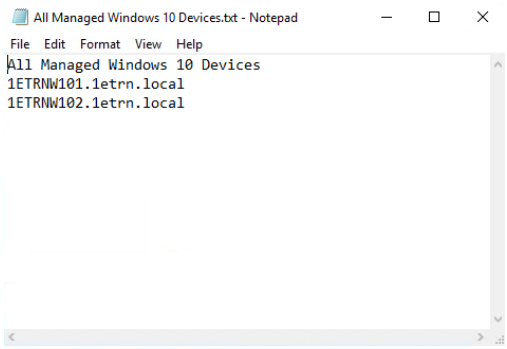
We've created a **C:\Sources\DeviceFolder** folder and added two files,
All Managed Windows 10 Devices.txt and **All Managed Windows 7 Devices.txt** that contain a list of device FQDN on separate lines.

We have also added the **Create-DirectManagementGroupUsingCmCollection.ps1** script to this folder, in our example we'll run the script from the same folder as the text files.

> **Tip**
>
> Unlike Rule based Management Groups, once a direct based Management Group is added to Tachyon, you cannot later change the name.
>
> To distinguish your direct-based Management Groups from your rule based groups, you should give them a meaningful naming convention, for the purposes of our example we have just used All Managed Windows as a prefix to indicate them.







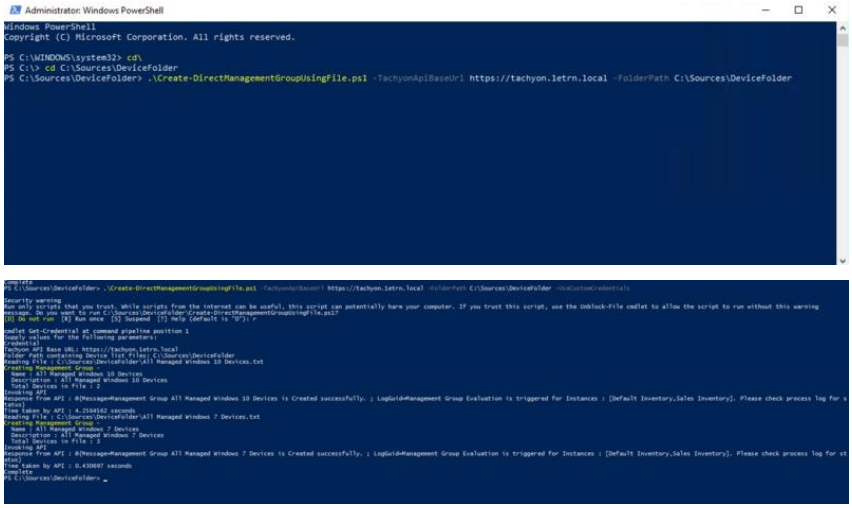
1.7.4.4.3.3 Running the script to populate the direct-based Management Groups

With the device files in place, in our example, we run the **Create-DirectManagementGroupUsingFile.ps1** file with the following command-line:

```
.\Create-DirectManagementGroupUsingFile.ps1 -TachyonApiBaseUrl https://tachyon.
testlab.com -FolderPath C:\Temp\DeviceFolder -UseCustomCredentials
```

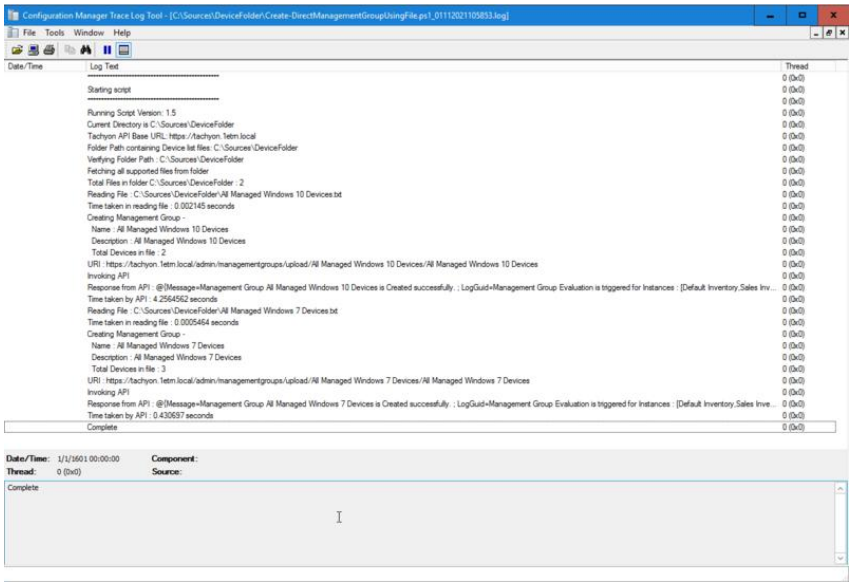
Where the **TachyonApiBaseUrl** is set to our example instance of **https://tachyon.1etrn.local** and the **-FolderPath** is set to the **C:\Sources\DeviceFolder** we set up earlier.

We don't bother with the **UseCustomCredentials** setting as the account we are running the script with has administrator permissions in Tachyon.



1.7.4.4.3.4 Checking the log file for Create-DirectManagementGroupUsingFile.ps1

After running the script you will find a log file is created in the same directory where the **Create-DirectManagementGroupUsingFile.ps1** is located. In our example we can see that the script completed without errors.



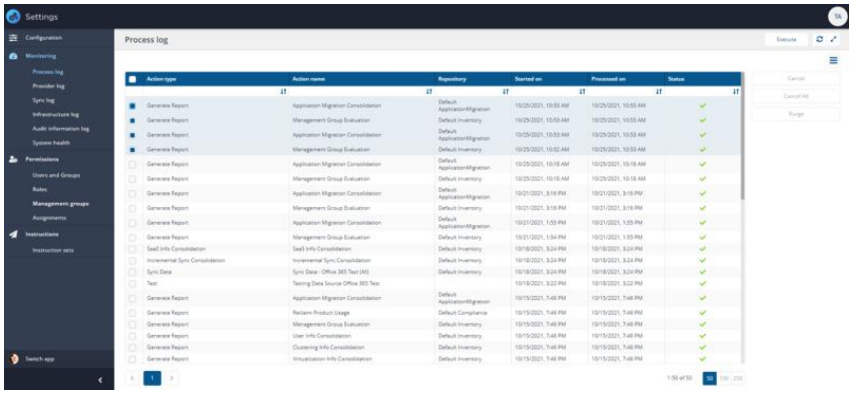
1.7.4.4.3.5 The reports for creating and enabling the direct-based Management Groups

When the direct-based Management Groups are added to Tachyon some reports will run to enable the Management Groups to be used.

If more than one direct-based Management Groups are being added you will see two **Management Group Evaluation** reports run on the default **Inventory** repository. You will also see an additional Management Group Evaluation report run on each additional non-default inventory repositories you have in your system.

If you have Application Migration installed you will also see two **Application Migration Consolidation** reports run on the default **ApplicationMigration** repository.

In our example we have Application Migration installed, so we see four reports run when the DB Management Groups are added. Two **Management Group Evaluation** reports and two **Application Migration Consolidation** reports, as can be seen in the picture.

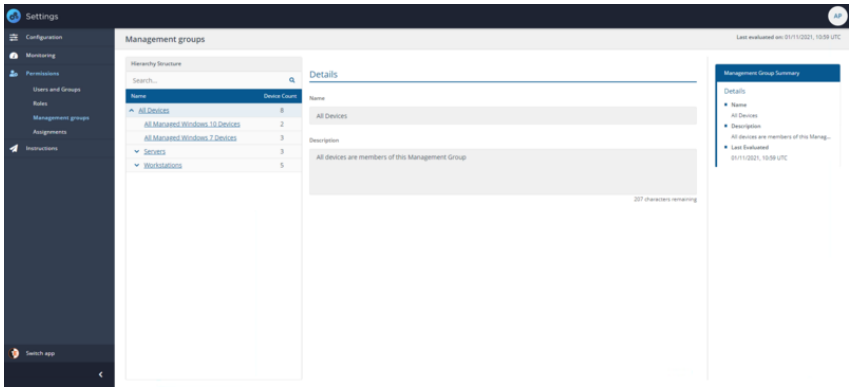


1.7.4.4.3.6 The direct-based Management Groups added

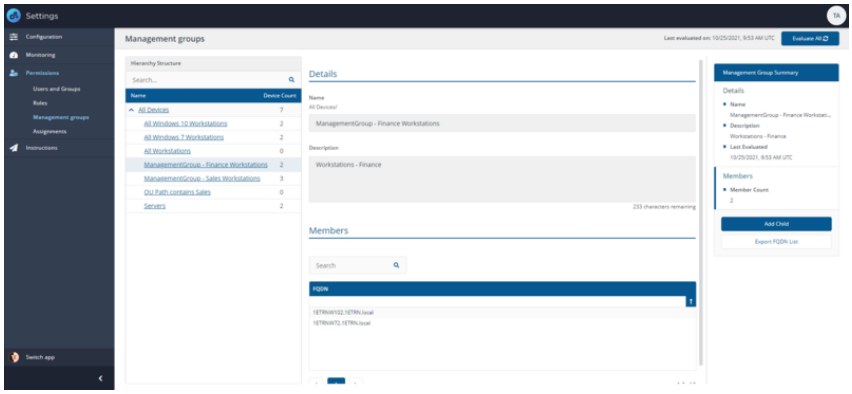
After running the script, two new direct-based Management Groups get added:

- **All Managed Windows 10 Devices.txt**
- **All Managed Windows 7 Devices.txt**

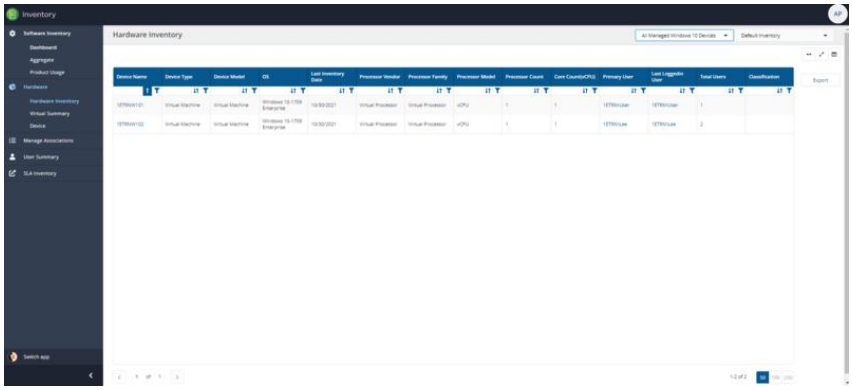
You can drill down to see the details of a Management Group by clicking the **Name** link.



Clicking on the **All Managed Windows 10 Devices.txt** Management Group name link displays the details for that Management Group. Here, you can view group members, export the membership as a .TSV file or add Child Management Groups as required.



You can use the **Inventory→Hardware Inventory** page with the Management Group selector set to the name of the Management Group, to view every device contained in the new Management Group.



1.7.4.4.4 Working with rule-based Management Groups

Rule-based Management Groups are defined and maintained in the **Settings**→Permissions→Management Groups page. They use device inventory data gathered from data sources by connectors and use Management Groups to control how instructions are applied in Tachyon applications. All child Management Groups must be created under the default **All Devices** Management Group.

You can easily create complex Management Group definitions by building rules for them, you'll find this in the **Rules** section of each Management Group. In the Rules section, you can define parameters that determine what devices are members of your Management Groups. The rules you create can be as simple as defining membership according to the OU path in your AD, or as complex as adding groups of rules that narrow membership down to details like **Processor Matched Threads per Core**. You can also use device or software tags that you have created to define Management Group membership, or a combination of all these parameters.

By default, in a new installation of Tachyon, all devices are members of the **All Devices** group. If you have upgraded from a previous version of Tachyon, your previously created Management Group will be preserved and will become a child Management Group of **All Devices** Management Group.

You can create **Child** Management Groups and nest them into a **Hierarchy Structure** where child Management Groups inherit rules from their parent groups.

Using child Management Groups you could create by hand a Management Group structure which mirrors your Configuration Manager collections, or divide your Management Groups by device type, for example into servers

and workstations. You can use the delegation feature to create Management Groups that mirror your organizational structure with associated delegated roles.

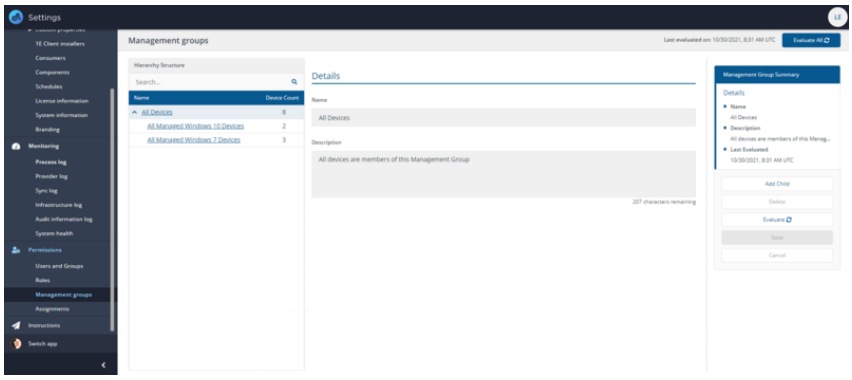
To find out how to use scripts to import a Management Group structure from a file or from Configuration Manager collection, refer to Creating direct-based Management Groups.

Note

Refer to Management Groups - tutorial for a conceptual example of how you might create a **Hierarchy Structure**, and for details about how you can use the delegation feature.

The following sections walk through the basic steps required to:

- Creating a rule-based Management Group
- Editing a rule-based Management Group
- Deleting a Management Group
- Evaluating Management Group membership.



1.7.4.4.4.1 Creating a rule-based Management Group

In this example we will create a Management Group for devices that are based in a different office location, this location contains Windows 7 devices and is named Sales. The new Management Group is going to be a child group of the **All Devices** group.

To create the rule-based Management Group:

1. Navigate to the **Settings**→**Permissions**→**Management Groups** page.
2. Click the **Add Child** button to display the new Management Group template.
3. Enter a suitable **Name** for the Management Group. For example **Sales**.
4. Add a **Description**, it's a good idea to use a description that provides an outline of the rules that are used to populate the Management Group. For example **OU Path Contains Sales.**
5. To add each rule:
    a. Click on the **Add rule** button. The first one is already added, all you need to do is fill out the parts of the rule.
    b. First, you select the rule name and description, for example, **OU Path**.

c. You then select the condition. For example **Contains**.

d. To complete the rule you then set the value. For example **Sales**.

e. Click **Save**.

6. Repeat step 5 for each rule you want to define.

7. When you have more than one rule added, you can:

   a. Use the gripper icon at the right-hand end of the rule to change the order the rules are applied by dragging the rule to a new place in the list.

   b. Change the conjunction operator at the left-hand end of the rule to select between **AND** and **OR**.

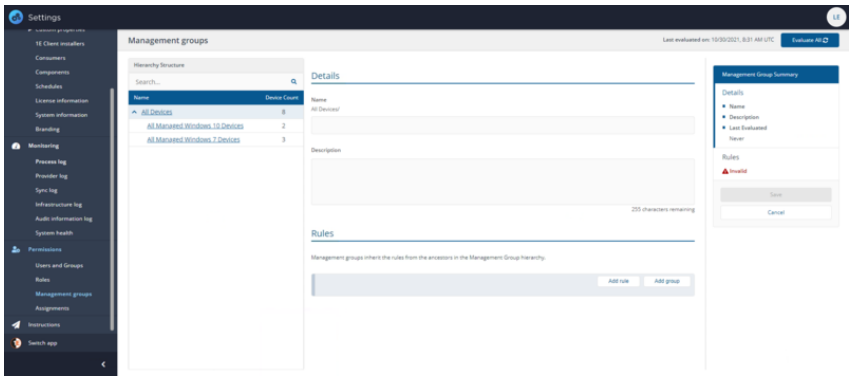
8. When you have finished adding the rules, you need to decide whether you want the Management Group membership to be evaluated immediately on adding the Management Group. If you are just adding one Management Group, it makes sense to click the **Evaluate** button. If you are adding a number of Management Groups, it may be a good idea to leave Click the **Evaluate All** button at the top of the page.

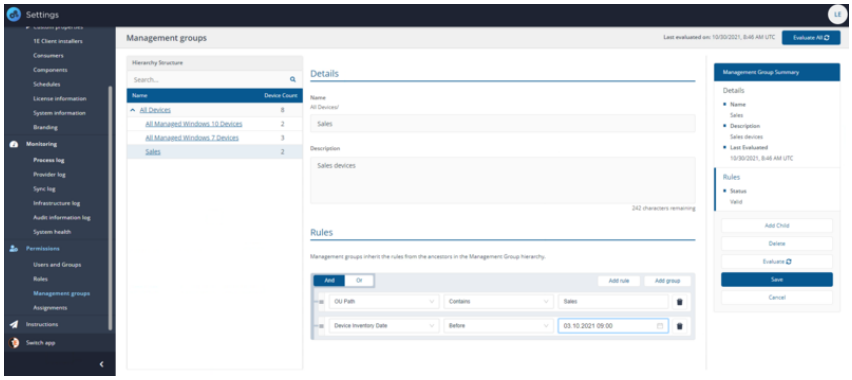
9. If you click **Evaluate All** and there is more than one inventory repository an additional control will be displayed prompting you to select which repository you want to evaluate the Management Group rules against.

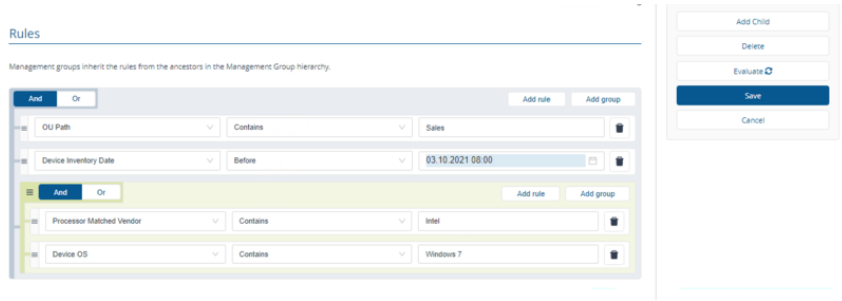
The Management Group will be added to the **Hierarchy Structure**.

Tip

You can create nested groups of rules using the **Add group** button. For example, we want to narrow the devices in the Sales group to those devices with an Intel processer and an OS of Windows 7 as we want to upgrade this legacy OS.



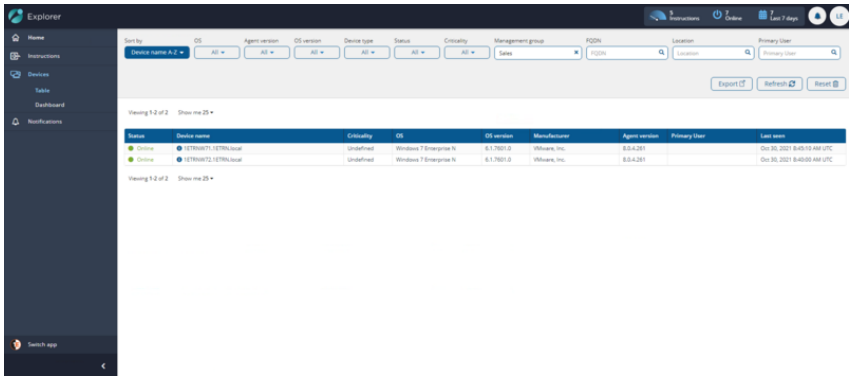




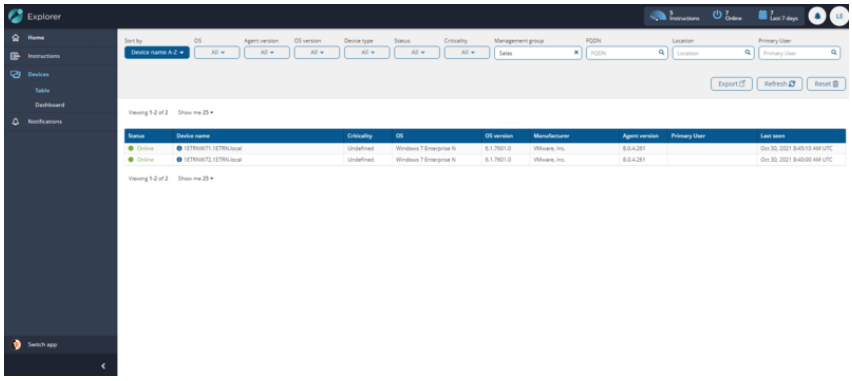
If you selected to evaluate rules immediately, the rules you set for the Management Group will be evaluated against the selected inventory repository.

To check how many devices are in the Management Group, switch to the **Inventory** app, select the Management Group name from the drop-down.

The picture shows the details for the **OU Path contains Sales** Management Group, showing that it contains **2** devices.



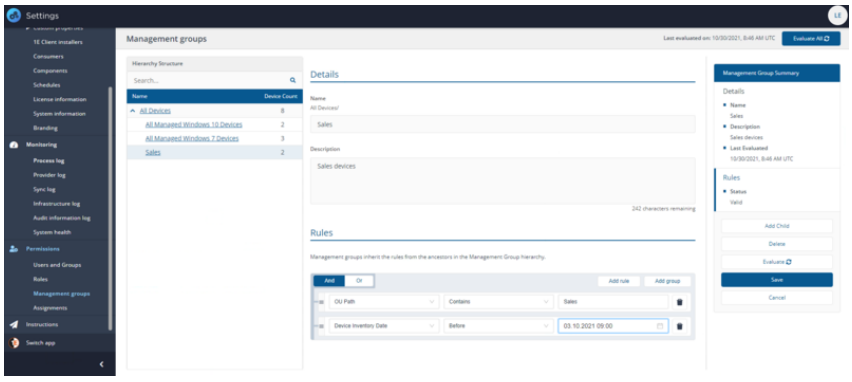
Once the Management Group rules have been evaluated, you should then be able to check the devices in Explorer contained in the group using the **Explorer→Devices→Table** page. The picture shows the **Devices** table with the **Management Group** filter set to **Sales**.



1.7.4.4.4.2 Editing a rule-based Management Group

To edit an existing rule-based Management Group:

1. Navigate to the **Settings**→**Permissions**→**Management Groups** page.
2. In the **Management Groups** table, locate the Management Group you want to edit and click the title at the left-hand end of its row in **Hierarchy Structure**.
3. Here you can edit the **Name**, **Description** and **Rules** that define the Management Group.
4. When you've finished editing, before you click the **Save** button you can click **Evaluate**, enables any modifications you've made to the rules to take effect right away. If you don't check the box, the rules won't be run, but you'll be able to evaluate the Management Groups later.

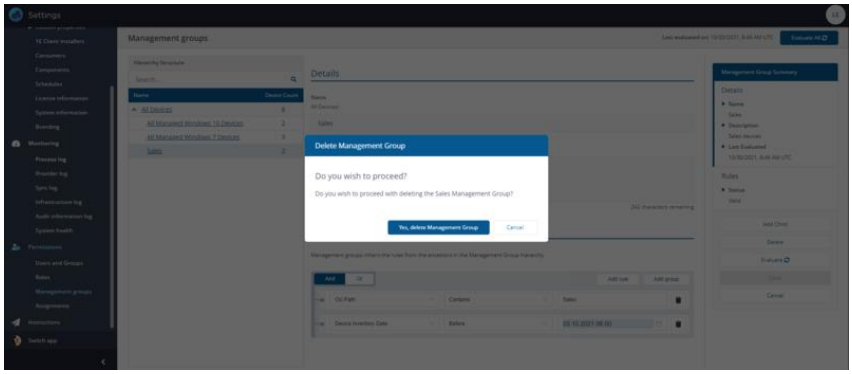


1.7.4.4.4.3 Deleting a Management Group

The following applies to rule-based and direct-based Management Groups.

To delete an existing Management Group:

1. Navigate to the **Settings**→**Permissions**→**Management Groups** page.
2. In the **Management Groups** table, locate the Management Group you want to delete and click the title at the left-hand end of its row in **Hierarchy Structure.**
3. Click the **Delete** button. This displays the **Delete Management Group** popup.
4. Here you are asked if you want to proceed with the delete process. Click the **Yes, delete Management Group** button to confirm the deletion, or **No** to cancel.



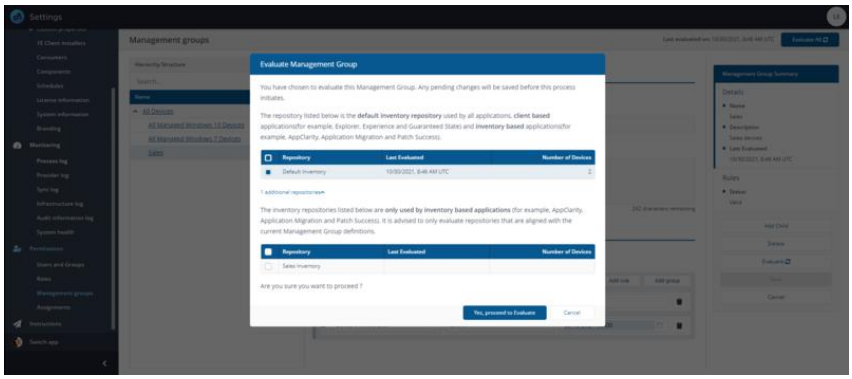
1.7.4.4.4.4 Evaluating Management Group membership

You can select to evaluate the Management Groups at any time.

Note

When a parent Management Group gets evaluated, all child Management Groups also get evaluated.

1. Navigate to the **Settings→Permissions→Management Groups** page.
2. Click the **Evaluate** button.
3. If there is only one inventory repository, the evaluation will be queued immediately. If there is more than one inventory repository, the **Evaluate Management Groups** popup will be displayed, and you will need to select a **Repository** then click the Evaluate button before the evaluation is queued.
4. When an evaluation is queued you will see a **Management Group Evaluation** action appear on the **Settings→Monitoring→Process** log page. From there you can view the progress of the evaluation.
5. When this action has run, Explorer will reflect any changes that have been made to the Management Group memberships.



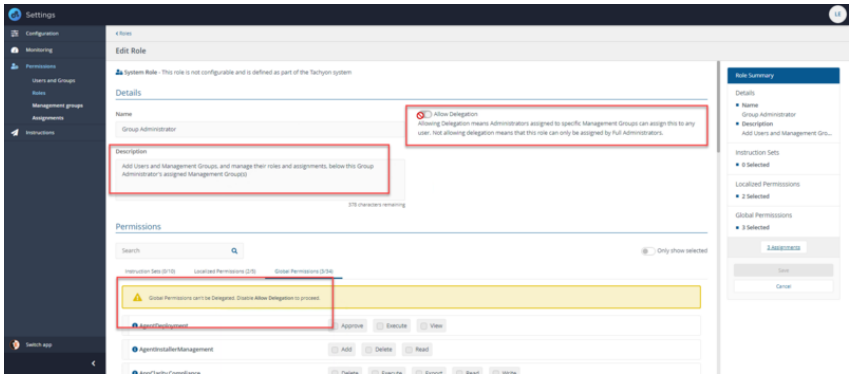
1.7.4.4.4.5 Delegation in Tachyon

Delegation in Tachyon is, a concept where an administrator can delegate some of their own responsibility to other users and limit the area where they can use that responsibility. In Tachyon, a Full administrator can create and modify Roles. They can also assign any Role to a Tachyon user or group using Management Groups, there are exceptions, like the **Group Administrator** Role which cannot be assigned to **All Devices**.

For example, a local security administrator with the **Group Administrator** role cannot create or modify Roles, but they can assign any Role that is marked as delegatable to a Management Group they have the security permission on, or any of its child Management Groups.

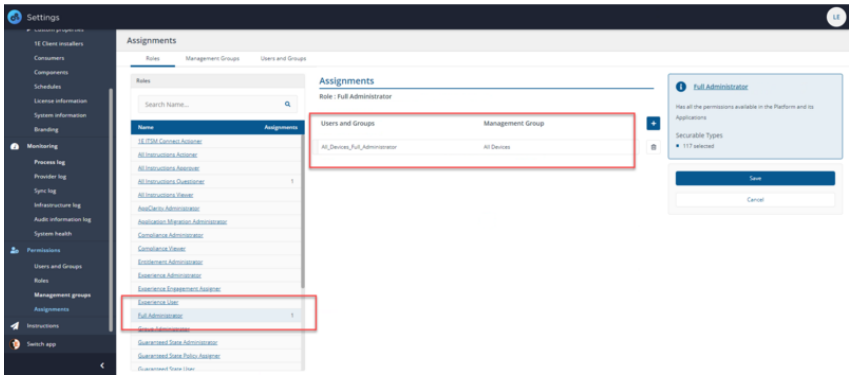
The exception is that a local security administrator cannot assign a Role that has the same security permission using the same Management Group they have permissions on. Instead, they have to use a child Management Group of the one they have security permissions on.

Essentially, a local security administrator cannot create an assignment that would result in another Tachyon user or group having the same security permissions as they do.



1.7.4.4.4.5.1 Delegation example

In our example we have a new Tachyon installation with only a few assignments, the one shown in the picture is of the **Full Administrator** role which is assigned to the group **All_Devices_Full_Administrator** and is assigned to **All Devices**. We have used a group to control the assignment instead of an individual user account.



In our example, we want to use the delegation feature of Tachyon and use the Group Administrator role to delegate some tasks to a child Management Group of **All Devices** called **Servers** to another administrator.

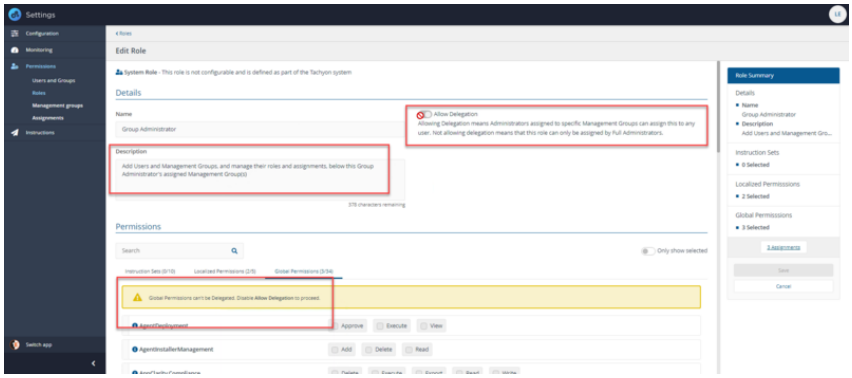
We'll assign the **Group Administrator** role to a Universal AD group called **Server_Group_Administrator** which we have added to Tachyon using the Users and Groups page.

To add the new assignment:

1. On the **Settings**→**Permissions**→**Assignments** page, we click on the title of the role to configure, in this case **Group Administrator** this displays the **Assignments** page focused on that role.

2. Clicking the plus sign button allows us to add our group, **Server_Group_Administrator** and the associated Management Group, **Servers**.

3. Once we've selected the group and Management Group, we click the **Save** button.



When a user in the **Server_Group_Administrator** group signs in to Tachyon, they will be able to create a child Management Group. For example a subset of the **Servers** Management Group for application servers called **App servers**, other Management Groups at the same level are locked because the **Server_Group_Administrator** has not been applied to those Management Groups.

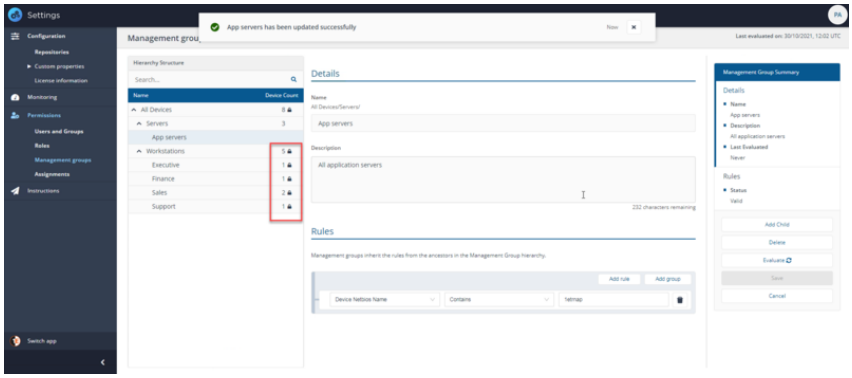
If, for example, our **Server_Group_Administrator** now wants to add a user with the **All Instructions Questioner** role to the new **App servers** Management Group, they can now do so.

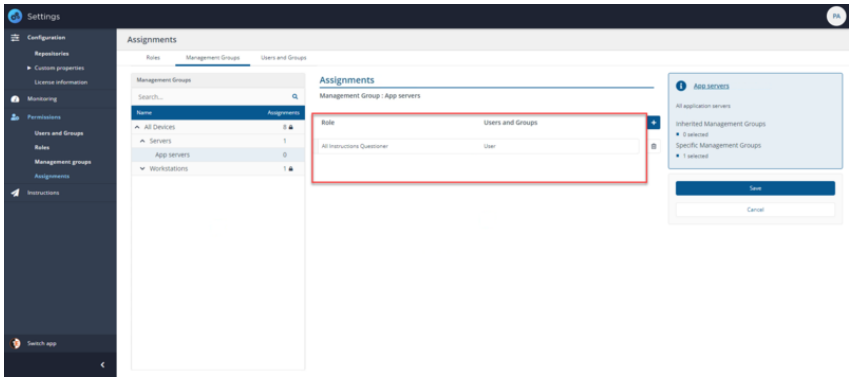
Note

For a complete reference table of Tachyon roles, please refer to the Roles and Securables page.

This page contains a full list of roles, their associated permissions, whether each role is delegatable and notes indicating if the role is new or renamed for the release.

Role	Description
System roles	System roles are built-in and are not configurable, however they can be assigned to users the same as any other role.
Custom roles	Custom roles can be used to define who is able to use specific Instruction Sets to ask questions, run actions or approve actions.
Securables and operations	A Permission is one or more Operations for a Securable. The remit for a Securable is either Localized or Global. A Role that has only Localized permissions can be delegated.





1.7.4.4.5 Management Group rules and conditions

In computing, a Boolean result means an expression is either true (1) or false (0). That is, expressions such as A AND B or A OR B give you a true or false result. Boolean expressions can be much more complex, and you can use brackets (groupings) to keep the same operators together, for example A AND B AND C. You would not write an expression such as A AND B OR C because it is ambiguous. It can be interpreted as either A AND (B OR C) or (A AND B) OR C.

When you are building rules, and you get different results to the ones you expect, write down each of your rules as A, B, C etc, and put them into a simple Boolean expression, like A OR (A AND B) = A.

This is perhaps the most important point to remember when building Management Group rules, and why it helps to write down what you are trying to achieve as a Boolean expression, then simplify it. The Rule examples section has some simple examples of how Boolean expressions translates to the rules you can apply to your own Management Groups.

1.7.4.4.5.1 Rule layout

The rows in the Rules section are laid out as follows:

Conjunction	Rule Name	Operators	Value	Delete	Gripper
When there is more than one rule, this field determines how it	Determines the type of information checked when	How the value compares against the type of information. This may be one of the following:	The value field is either	This field contains	This field lets you

<table>
<tr><th>Conjunction</th><th>Rule Name</th><th>Operators</th><th>Value</th><th>Delete</th><th>Gripper</th></tr>
<tr>
<td>is evaluated with the other rules. This may be one of:

<table>
<tr><th>Conjunction</th><th>Description</th></tr>
<tr><td>AND</td><td>This rule must be satisfied as well as any other rules.</td></tr>
<tr><td>OR</td><td>Either this rule must be satisfied or any other rules.</td></tr>
</table>
</td>
<td>evaluating the rule.

For example, selecting Device Computer Name will specify checking the set value against the information held internally for each device's computer name using the selected operand.

Please refer to List of available rules below.</td>
<td>
<table>
<tr><th>Operator</th><th>Attribute type</th><th>Comparison</th></tr>
<tr><td>Equal to</td><td>String, Date, Number, Yes/No</td><td>Your value is exactly equal to the device’s value.</td></tr>
<tr><td>Not Equal to</td><td>String, Date, Number</td><td>Your value is not equal to (different to) the device’s value.</td></tr>
<tr><td>Before</td><td>Date</td><td>Your date is before the device’s date.</td></tr>
<tr><td>After</td><td>Date</td><td>Your date is after the device’s date.</td></tr>
<tr><td>Begins with</td><td>String</td><td>The device’s value begins with your value.</td></tr>
<tr><td>Ends with</td><td>String</td><td>The device’s value ends with your value.</td></tr>
<tr><td>Less than</td><td>Number</td><td>Your value is less than the device’s value.</td></tr>
</table>
</td>
<td>a string, date, or numeric value, depending on the chosen rule name.

It may also be a Device tag. For more information about Deice tags, please refer to Device Tags page.</td>
<td>an icon that lets you delete the rule.</td>
<td>grab the rule and change its order where there is more than one rule.</td>
</tr>
</table>

Conjunction	Rule Name	Operators			Value	Delete	Gripper
		Less than or equal to	Number	Your value is **less than or equal to** the device's value.			
		Greater than	Number	Your value is **greater than** the device's value.			
		Greater than or equal to	Number	Your value is **greater than or equal to** the device's value.			
		Is one of	Tag	The specified Device tag exists on the device, and its value **is one of** the array of alternative values that you specified.			
		Is not one of	Tag	The specified Device tag exists on the device, and its value **is not one of** the array of alternative values that you specified.			

Conjunction	Rule Name	Operators			Value	Delete	Gripper
		Is Null	String, Date, Number, Tag	The device does not provide this information. If you have specified a Device tag, it does not exist on the device.			
		Is not Null	String, Date, Number, Tag	The device provides this information, but it can be any value. If you have specified a Device tag, it exists on the device, set to any value.			
		Contains	String	The device's value **contains** your text string.			
		Not Contains	String	The device's value **does not contain** your text string.			

1.7.4.4.5.2 Rule examples

The following examples may help to illustrate the logic underpinning the rules you can build and apply to the Management Groups in your environment.

1.7.4.4.5.2.1 Rule example 1

"Device Netbios Name begins with 1ETRNW" OR ("Device Netbios Name begins with 1ETRNW" AND "Device Netbios Name begins with 1ETRN")

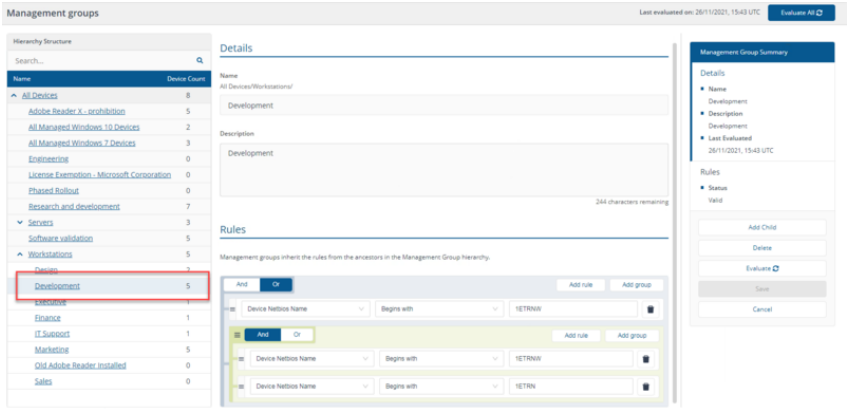
Is the same as saying:

"Device Netbios Name begins with 1ETRNW"

You could reduce this to the statement:

A OR (A AND B) = A

In our environment, this returns all five workstation devices with the NetBIOS name beginning 1ETRNW.

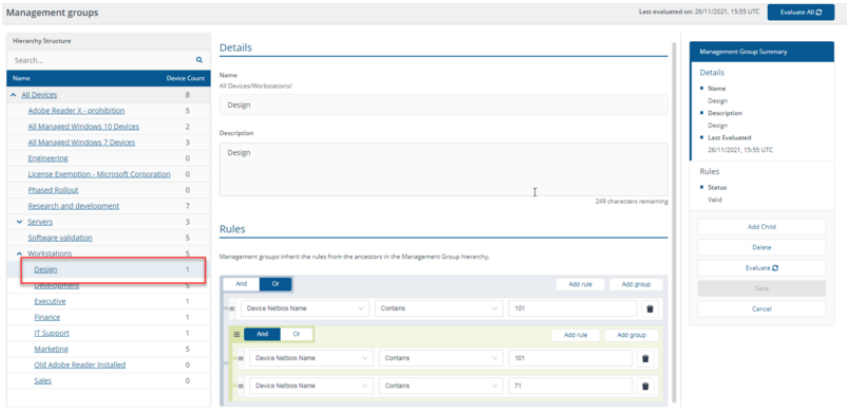


1.7.4.4.5.2.2 Rule example 2

"Device Netbios Name contains 101" OR ("Device Netbios Name Contains 101" AND "Device Netbios Name Contains 71")

Is the same as:

"Device Netbios Name Contains 101"



You could reverse the logic in the statement and say:

"Device Netbios name Contains 101" AND ("Device Netbios name Contains 101" OR "Device Netbios name Contains 71")

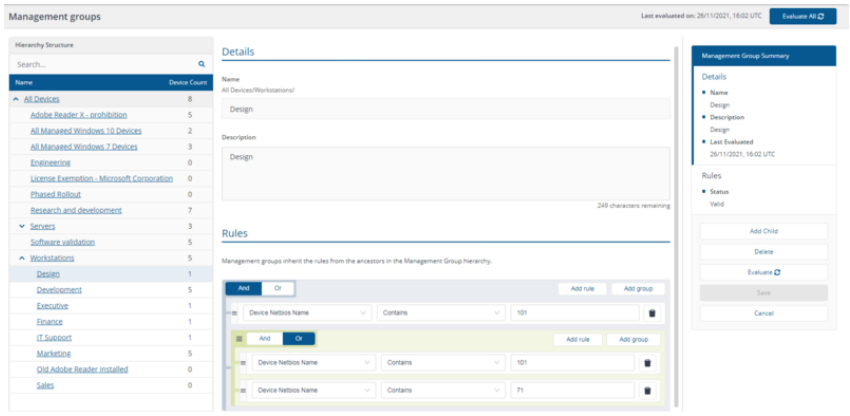
Which is the same as:

"Device Netbios Name Contains 101"

You could reduce this to the statement:

A AND (A OR B) = A

In our environment, this returns one workstation device with the NetBIOS name contains 101, which matches one device, 1ETRNW101.



1.7.4.4.5.2.3 Rule example 3

Management Group rules do not let you place a Boolean NOT operator around a grouping, but you can convert an expression into NOT rules, for example:

NOT ("Device Netbios Name Contains AP" OR "Device Netbios Name Contains CM")

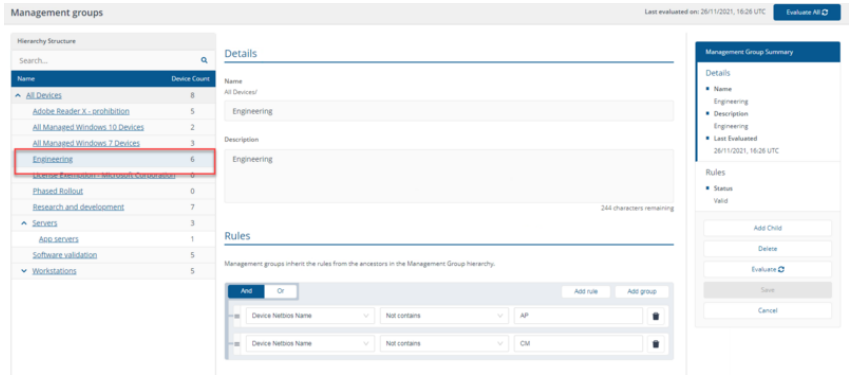
Using rules, you can express this as:

"Device Netbios Name Not contains AP" AND "Device Netbios Name Not contains CM"

You could reduce this to the statement:

NOT (A OR B) = (NOT A) AND (NOT B)

In our environment this returns the six devices where the NetBIOS name does not contain AP or CM, which are 1ETRNAP, our application server, and 1ETRNCM, our Configuration Manager server.



1.7.4.4.5.3 List of available rules

Rules used to create Management Groups, and connectors that provide the data to support the rules.

For details of how to create and use Management Groups, please refer to Management Groups page.

Warning

The number of rules that a single Management Group can contain is variable because of many factors including SQL Server version, server configuration and rule type used. 1E recommends not exceeding 10,000 rules per rule-based Management Group.

Rule name	Description	SCCM	ServiceNow	Tachyon	OracleLMS	BigFix	BigFixInv	Intune	vCenter	WSUS
Device ADSite Name	AD Site the device is connected to.	✓	✓							
Device Assigned Cores	Maximum number of assigned cores for the device. Derived from	✓	✓	✓	✓	✓			✓	
Device Classification	Classification of the device. For example, **Test**, **Production** or **Development**. **Note** **Production** is the default.	✓	✓		✓					
Device Computer Name	Hostname of the computer.	✓	✓	✓	✓	✓	✓	✓	✓	✓
Device Criticality	By default, Device Criticality is set as one of the following, as described in Using Device Criticality. • Undefined • Non-critical • Low • Medium • High	✓	✓	✓	✓	✓	✓	✓	✓	✓

Rule name	Description	SCCM	ServiceNow	Tachyon	OracleLMS	BigFix	BigFixInv	Intune	vCenter	WSUS
	• Critical.									
Device Domain Name	Domain the device is installed on.	✓	✓	✓			✓			
Device Inventory date	Date that the device was last updated.	✓	✓	✓	✓			✓	✓	✓
Device Matched Device Type	Normalized device type based on chassis type. For example **Desktop**.	✓	✓	✓	✓	✓		✓	✓	✓
Device Matched Family	Normalized family of the device. For example, **Aspire**.	✓	✓	✓	✓	✓			✓	
Device Matched Model	Normalized model of the device. For example, **A30**.	✓	✓	✓	✓	✓		✓	✓	✓
Device Matched Socket count	Normalized socket count of the device. For example, **1**.	✓	✓	✓	✓	✓		✓	✓	✓
Device Matched Vendor	Normalized vendor name of the device. For example, **Acer Inc.**.	✓	✓	✓	✓	✓		✓	✓	✓

Rule name	Description	SCCM	ServiceNow	Tachyon	OracleLMS	BigFix	BigFixInv	Intune	vCenter	WSUS
Device Netbios Domain name	NetBIOS version of the device's domain name.	✓	✓	✓						
Device Netbios Name	NetBIOS version of the device name.	✓	✓	✓					✓	
Device OS	The normalized product title of the OS that is running on the device.	✓	✓	✓		✓	✓		✓	
Device Purchase date	Date that the device was purchased.	✓	✓							
Device Serial	Serial number of the computer.	✓	✓				✓	✓		
Device User Primary Username	The primary user of the device.	✓		✓						
OU Name (Deprecated)	Name of the OU that the device is in. For example **Sales**. **Note** All OUs with the same name will be used,	✓	✓							

Rule name	Description	SCCM	ServiceNow	Tachyon	OracleLMS	BigFix	BigFixInv	Intune	vCenter	WSUS
	therefore the **OU Path** rule should be used instead. The **OU Name** rule is deprecated and should be re-defined using **OU Path**. This rule is deprecated, which means it will continue to work until it is removed in a future version of Tachyon.									
OU Path	The name or path of the OU location in the AD hierarchy, using pipe | as the delimiter. For example, to get all the computers in **OU=Sales, OU=Workstations, DC=acme, DC=local** you can either specify **Sales** or - if there is more than one OU called **Sales** in the AD structure - specify the whole path **acme.local|Workstations|Sales**. Note that the DC and OU parts of a distinguished name are treated differently.	✓	✓							

Rule name	Description	SCCM	ServiceNow	Tachyon	OracleLMS	BigFix	BigFixInv	Intune	vCenter	WSUS
Processor Matched Chip Module Count	Normalized chip module count of the processor. For example, **1**.	✓	✓	✓	✓	✓				
Processor Matched Core Count	Normalized core count of the processor. For example, **2**.	✓	✓	✓	✓	✓			✓	
Processor Matched Family	Normalized family name of the processor. For example, **Athlon 64 X2**.	✓	✓	✓	✓	✓			✓	
Processor Matched Model	Normalized model name of the processor. For example, **3250e**.	✓	✓	✓	✓	✓			✓	
Processor Matched Processor Type	Normalized type of the processor. For example, **Desktop**.	✓	✓	✓	✓	✓			✓	
Processor Match	Normalized release date of the processor. For example, **31-03-2008**.	✓	✓	✓	✓	✓			✓	

Rule name	Description	SCCM	ServiceNow	Tachyon	OracleLMS	BigFix	BigFixInv	Intune	vCenter	WSUS
ed Release Date										
Processor Matched Speed MHz	Normalized speed of the processor. For example, **2.100**.	✓	✓	✓	✓	✓			✓	
Processor Matched Threads per Core	Normalized threads per core of the processor. For example, **1**.	✓	✓	✓	✓	✓			✓	
Processor Matched Vendor	Normalized vendor name of the processor. For example, **Advanced Micro Devices, Inc**.	✓	✓	✓	✓	✓			✓	
Product Catalog Colloquial Version	Software colloquial version contained in the inventory source. For example, **2012**. **Note** This will usually be blank.	✓	✓				✓	✓		
Product Catalo	Software edition contained in the inventory source. For example, **Standard**. **Note**	✓	✓	✓			✓	✓		

Rule name	Description	SCCM	ServiceNow	Tachyon	OracleLMS	BigFix	BigFixInv	Intune	vCenter	WSUS
g Edition	This will usually be blank in SCCM unless the relevant MOF extensions have been installed.									
Product Catalog Is Partial Version Matched	Flag that indicates whether the software title was partial matched or not (TRUE/**1**) or not (FALSE/**0**).	✓	✓	✓	✓	✓	✓	✓		
Product Catalog Matched Colloquial Version	Normalized software colloquial version. For example, **2016**.	✓	✓	✓	✓	✓	✓	✓		
Product Catalog Matched Edition	Normalized software edition. For example, **Standard**.	✓	✓	✓	✓	✓	✓	✓		
Product Catalog	Normalized software end of support date that of that	✓	✓	✓	✓	✓	✓	✓		

Rule name	Description	SCCM	ServiceNow	Tachyon	OracleLMS	BigFix	BigFixInv	Intune	vCenter	WSUS
Matched End of Support	version. For example, **31-10-2008**.									
Product Catalog Matched is Bundle	Flag indicating whether the normalized software is a bundle (TRUE/**1**) or not (FALSE/**0**).	✓	✓	✓	✓	✓	✓	✓		
Product Catalog Matched Is License Required	Flag indicating whether that normalized software title requires a license (TRUE/**1**) or not (FALSE/**0**).	✓	✓	✓	✓	✓	✓	✓		
Product Catalog Matched Release Date	Normalized software release date of that version. For example, **31-10-2008**.	✓	✓	✓	✓	✓	✓	✓		
Product Catalog Match	Normalized software title. For example, **Office**.	✓	✓	✓	✓	✓	✓	✓		

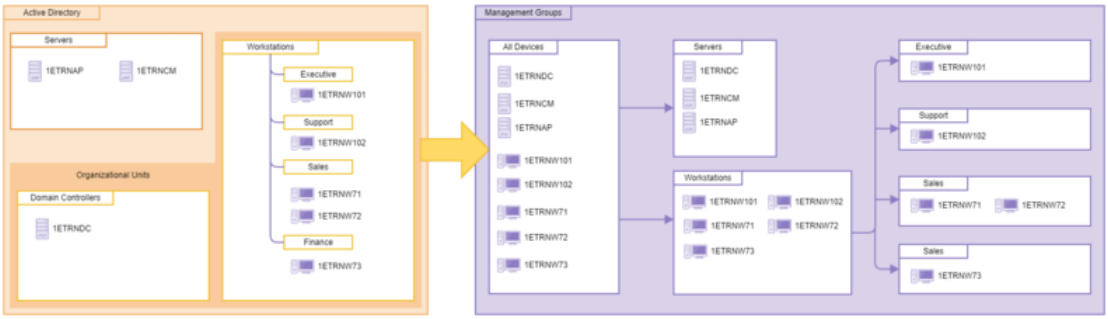
Rule name	Description	SCCM	ServiceNow	Tachyon	OracleLMS	BigFix	BigFixInv	Intune	vCenter	WSUS
ed Title										
Product Catalog Matched Vendor	Normalized software vendor name. For example, **Microsoft Corporation**.	✓	✓	✓	✓	✓	✓	✓		
Product Catalog Matched Version	Normalized software version. For example, **10.2.233**.	✓	✓	✓	✓	✓	✓	✓		
Product Catalog Title	Software title contained in the inventory source. For example, **Office Standard en_pack**.	✓	✓	✓	✓	✓	✓	✓		
Product Catalog UN Standard Product Service Code	UNSPC code of the normalized software title.	✓	✓	✓	✓	✓	✓	✓		
Product Catalo	Software vendor name contained in the inventory	✓	✓	✓		✓	✓	✓		

Rule name	Description	SCCM	ServiceNow	Tachyon	OracleLMS	BigFix	BigFixInv	Intune	vCenter	WSUS
g Vendor	source. For example, **Microsoft**.									
Product Catalog Version	Software version number contained in the inventory source. For example, **10.2.233**.	✓	✓	✓	✓	✓	✓	✓		
Product Install Date	Date that software installation was installed according to the inventory source.	✓		✓						
Product Instance Name	Instance name if used by a product, for example **MSSQLSERVER** for SQL Server.	✓	✓	✓	✓	✓				
Product Last Used date	Date that software installation was last run according to the inventory source.	✓		✓						
Product Usage Category	Usage category assigned to a specific installation of a normalized software title. Potential categories are: - Used - Unused - Rarely used - Unreported	✓	✓	✓	✓					

1.7.4.5 Management Groups - tutorial

In this tutorial

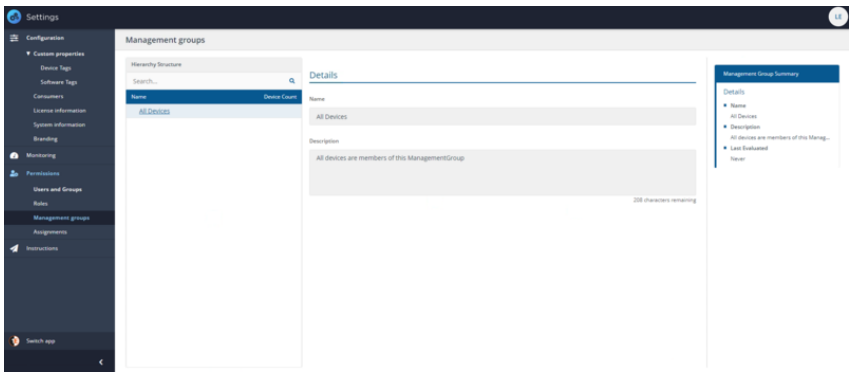
In this tutorial, we add a number of Management Groups for the ACME organization: one that uses the name of the devices and several that use the Organizational Unit (OU) the devices belong to. The following picture shows what we have in our example Active Directory and how this will appear as Management Groups in Tachyon. Here you can see there are two servers in the AD Computers group, an additional Domain Controller server and five workstations in the OU.



By the end of this example, you will have added six Management Groups in addition to the default All Devices Management Group:

- All Devices - this Management Group brings all devices into a single Management Group
- Servers, Workstations, Executive, Support, Sales and Finance - these Management Groups will use an OU rule to separate the devices according to the OU they belong to.

> **Note**
>
> If you want to take advantage of your Configuration Manager database, and pull in its inventory and usage data, so that you can mirror your Active Directory OU structure in your Management Groups, then you'll need to configure a System Center Configuration Manager connectorin your Tachyon system.

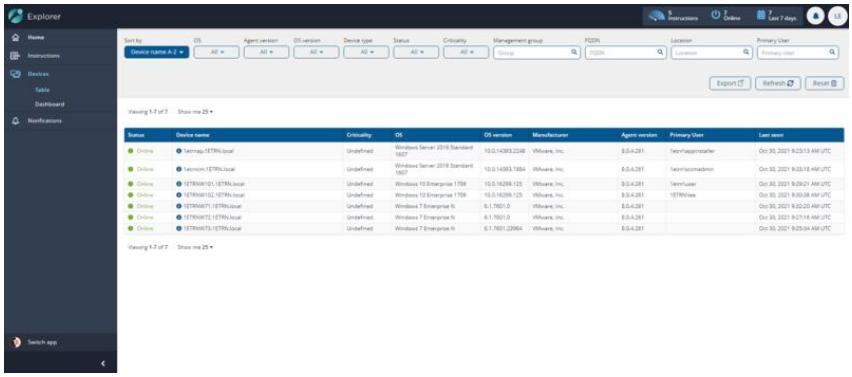


1.7.4.5.1 Without Management Groups

Before describing the process for creating the Management Groups, let's take a look at the Explorer application to see how things look without any Management Groups defined. The easiest way is to use the **Devices** table in Explorer:

1. Navigate to the **Explorer→Devices→Table** page.
2. On this page you will see all the devices with the Tachyon client installed. In our example, there are **7** connected devices.
3. Clicking on the **Management Group** filter edit field, you can see that no Management Groups are present.
4. Now switch to the **Settings** application using the **Switch app** menu.
5. Navigate to the **Settings→Configuration→Connectors** page.
6. Here you can check that a Tachyon connector has been added and tested.

If you have configured a connector, you can start adding Management Groups.



1.7.4.5.2 Adding example Management Groups

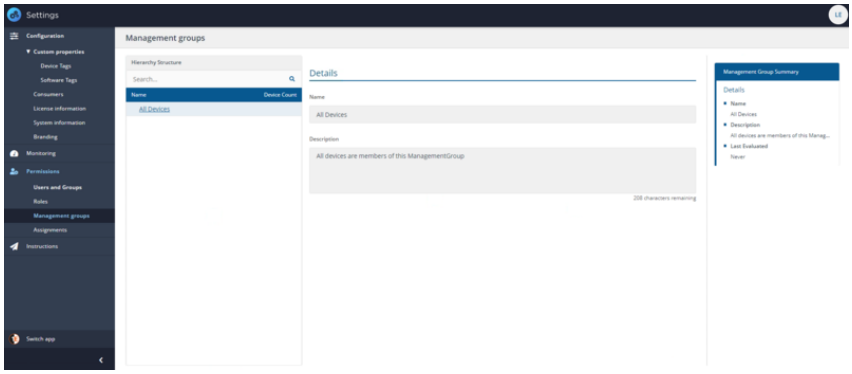
By default, in a new installation of Tachyon, all devices are members of the **All Devices** group. If you have upgraded from a previous version of Tachyon, your previously created Management Group will be preserved and will become a child Management Group of **All Devices** Management Group.

You can create **Child** Management Groups and nest them into a **Hierarchy Structure** where child Management Groups inherit rules from their parent groups.

Using child Management Groups you could create by hand a Management Group structure which mirrors your Configuration Manager collections, or divide your Management Groups by device type, for example into servers and workstations. You can use the delegation feature to create Management Groups that mirror your organizational structure with associated delegated roles.

To find out how to use scripts to import a Management Group structure from a file or from Configuration Manager collection, refer to Creating direct-based Management Groups.

Refer to the Roles page section for details about how you can use the delegation feature.



To add our Management Groups:

1. Navigate to the **Settings**→**Permissions**→**Management Groups** page.
2. To start creating groups click on the **Add Child** button to display the **Details** screen.
3. **Add Child** lets you set the following parameters for the Management Group:
   - **Name** - the name you will identify the group by
   - **Description** - the description for the group, use this to briefly describe the rules used to populate the Management Group
   - **Rules** - the rules that define the contents of the Management Group.
4. In our first Management Group, which will contain all the servers in the network, we set the following as shown in the first row of the table opposite :
   a. **Name** to **Servers**.
   b. **Description** to **All servers**.
   c. **Rules**: we set the first parameter to **Device OS**, the comparison operator to **Contains** and then the value to **Server**.
   d. Having made all the settings we then click on **Save** to save the Management Group.
   e. The last thing we could do is click **Evalute**. We don't do this immediately because we are going to create another 5 Management Groups, and we want to go straight onto doing that without waiting for the reports to run.
5. Our second group will contain all the devices in the **Workstations** OU and below. We make sure we select the **All Devices** level in our **Hierarchy Structure** as we want this OU to be a child of **All Devices**. We click on **Add** to start the process.
6. Set the following information for the second Management Group, as shown in the second row of the table opposite:
   a. **Name** to **Workstations**
   b. Description to **All workstations**
   c. **Rules**: this time we set the first parameter to **OU Path**, the comparison operator to **Contains** and the value to **Workstations**

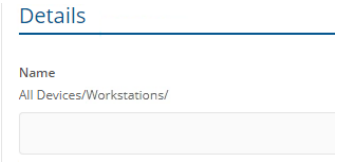
d. Having made all the settings we then click on **Add** to save the Management Group.

7. Repeat the steps outlined in step **6** for the remaining Management Groups but using the settings in the table opposite:

Note

The remaining four Management Groups are similar to our second Management Group in that they all use the **OU Path** property. The remaining Management Groups represent different departments in the organization and contain end user devices. These groups will be child Management Groups to the parent workstations Management Group, by creating a hierarchy in this way we can later delegate management responsibilities by assigning Tachyon users, groups and roles to them.

When creating Child Management Groups, check that you are creating that group in the correct part of your hierarchy. When you create a new group, it's place in the hierarchy is shown above the **Name** field.



Note

The **OU Path** rule was introduced in an accumulated hotfix to replace **OU Name** which was then deprecated (will be removed sometime in the future).

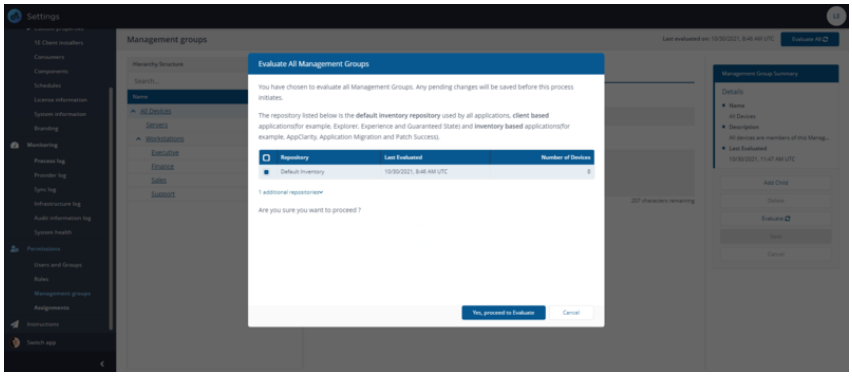
This tutorial uses **OU Path** in the same way as **OU Name**. However, **OU Path** also allows you to filter on *any* text in the OU path, using the pipe symbol | as a delimiter of different strings to search for, which must all be true to get a match. For example Workstations|Sales. **OU Path** allows you to be more explicit if you have OUs with the same name in different parts of your OU structure.

Child Management Group	Parameter	Value
Servers (steps 3 and 4)	Name	Devices
Description	All servers	
Rules	Device OS contains server	
Workstations (steps 5 and 6)	Name	Workstations
Description	OU Workstations	

Child Management Group	Parameter	Value
Rules	OU Path Contains Workstations	
Executive	Name	Executive Devices
Description	OU Executive	
Rules	OU Path Contains Executive	
Support	Name	Support
Description	OU Support	
Rules	OU Path Contains Support	
Finance	Name	Finance
Description	OU Finance	
Rules	OU Path Contains Finance	
Sales	Name	Sales
Description	OU Sales	
Rules	OU Path Contains Sales	

Having defined all the Management Groups we now need to evaluate all the rules.

1. Click on the **Evaluate All** button in the top right corner of the page, if you have more than one inventory in your Tachyon configuration you will be prompted to choose which repository you wish run evaluate your Management Groups against. Then click **Yes, proceed to Evaluate**.
2. To check the progress of the **Management Group Evaluation** action, navigate to the **Settings→Monitoring→Process log** page.
3. After a few seconds the **Status** column for the **Management Group Evaluation** action changes to display a green tick.

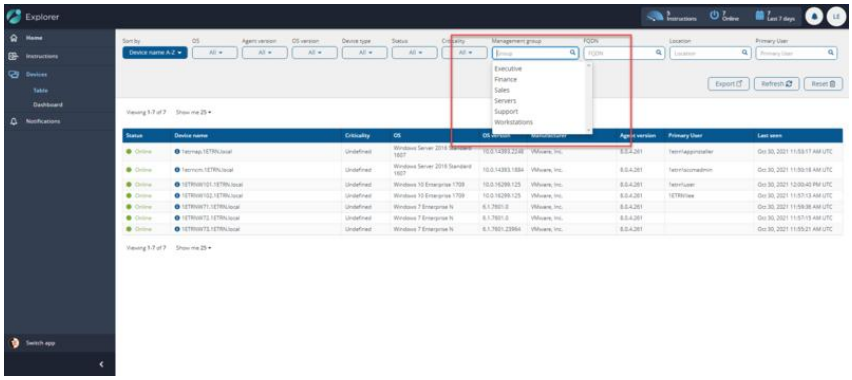


1.7.4.5.3 Checking the Management Groups in Explorer

The Management Group rules have now been evaluated and populated the Management Groups, it's now time to check how this has affected the **Devices** page in Explorer.

1. Navigate to **Explorer** using the **Switch app** menu.
2. Tachyonremembers that we were on the **Devices** page the last time we were in the Explorerapplication.
3. Click on the **Management Group** filter. A menu pops up displaying all 6 of the new Management Groups.
4. Selecting a Management Group from the menu filters the devices to show just the ones that belong to that Management Group.
5. Clicking on the **Sales** Management Group shows that it contains just 1 device.
6. Clicking on the **Workstations** Management Group shows that it contains 5 devices.
7. Clicking on **Executive** shows that it contains 2 devices.

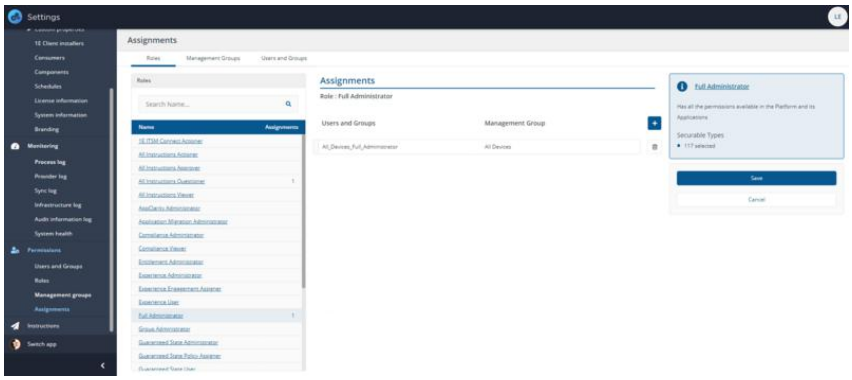
The example is now complete. We've created 6 new Management Groups, one of those with a rule that uses the OS type name and the other 5 using the OU the device belongs to. We've then evaluated the rules to populate the Management Groups with matching devices. At the same time, this has synchronized the information with the Explorer application, so we can now filter the devices displayed on the Devices table.



1.7.4.6 Assignments page

The **Assignments** page lets you view and manage current assignments for Tachyon roles, management groups, users and groups, from this page you can:

- View all current assignments
- Add new assignments
- Remove current assignments.

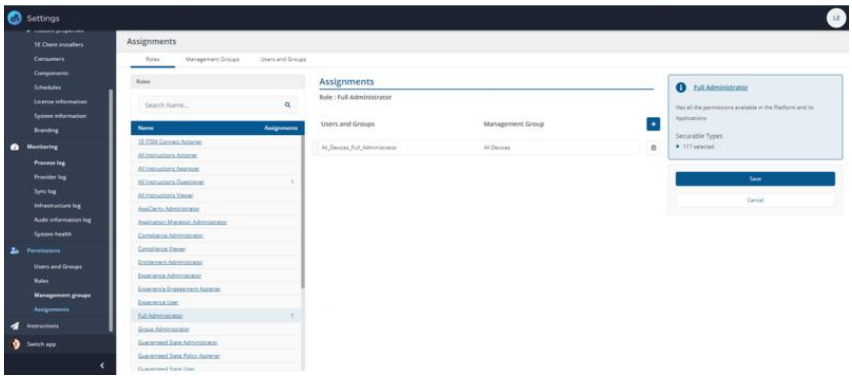


1.7.4.6.1 Roles assignments

Roles focus on all Tachyon roles, with the total of their current assignments listed next to each title. To add new assignments to a role, you can click on the role name. This displays that role's current assignments, with an information panel displaying a summary of that role and the securable types associated with that role.

In our example we have a new Tachyon installation with only a few assignments, the one shown in the picture is of the Full Administrator role which is assigned to the group **All_Devices_Full_Administrator** and is assigned to **All Devices**. We have used a group to control the assignment instead of an individual user account.

Refer to the Roles page for recommendations about how best to use roles, and for a full list of roles, permissions and if a role is delegatable.



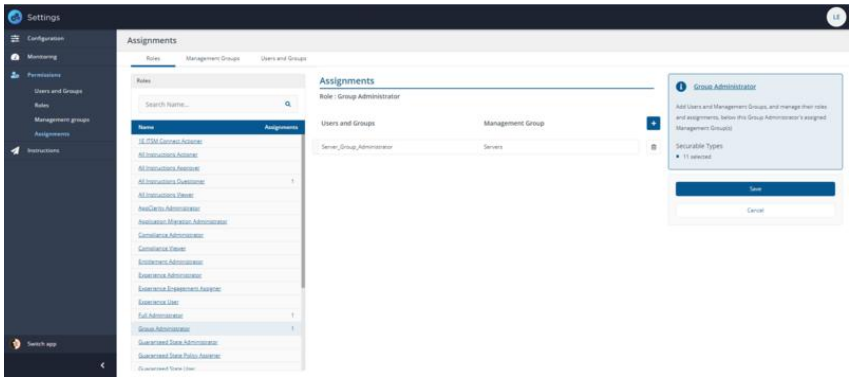
1.7.4.6.1.1 Example Role assignment

In our example, we want to use the delegation feature of Tachyon and use the Group Administrator role to delegate some tasks to a child management group of **All Devices** called **Servers** to another administrator.

We'll assign the **Group Administrator** role to a Universal AD group called **Server_Group_Administrator** which we have added to Tachyon using the Users and Groups page.

To add the new assignment:

1. On the **Settings→Permissions→Assignments** page, we click on the title of the role to configure, in this case **Group Administrator** this displays the **Assignments** page focused on that role.
2. Clicking the plus sign button allows us to add our group, **Server_Group_Administrator** and the associated management group, **Servers**.
3. Once we've selected the group and management group, we click the **Save** button.



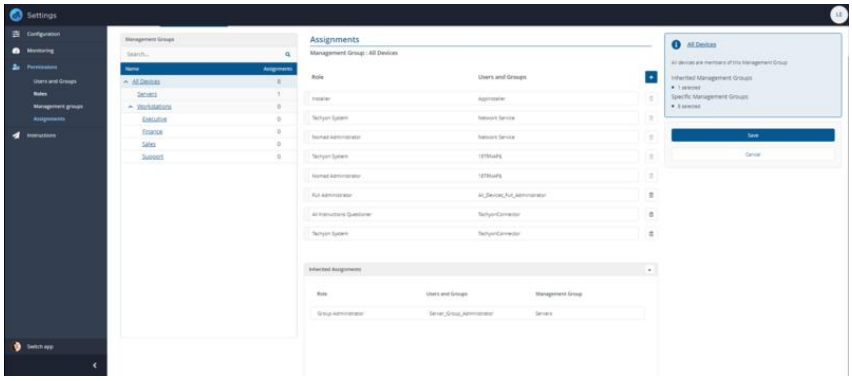
1.7.4.6.2 Management Groups assignments

The **Management Groups** tab focus on the management groups you have set up in your Tachyon installation, with the total of their current assignments listed next to each title. To add new assignments to a management group, you can click on the management group name. This displays that group's current assignments, with an information panel displaying a summary of that role and the assignments that are inherited with that group.

In our example we have a new Tachyon installation with only a few management groups, the one shown in the picture is of **All Devices** among the assignments is the group **All_Devices_Full_Administrator** and an inherited assignment **Server_Group_Administrator** from the management group **Servers**. We have used groups to control the assignments instead of individual user accounts.

Refer to the Roles page for recommendations about how best to use roles, and for a full list of roles, permissions and if a role is delegatable.

For recommendations about using and creating management groups refer to the Management Groups page and Management Groups - tutorial.



1.7.4.6.2.1 Example Management Group assignment

In our example, we want to use the delegation feature of Tachyon and use the **Group Administrator** role to delegate some tasks to a child management group of **All Devices** called **Workstations** to another administrator.

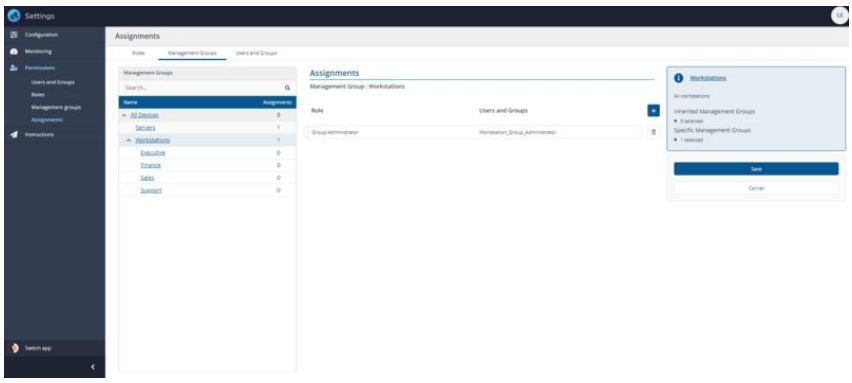
We'll assign the Group Administrator role to a Universal AD group called **Workstation_Group_Administrator** which we have added to Tachyon using the Users and Groups page.

To add the new assignment:

1. On the **Settings**→**Permissions**→**Assignments** page, we click on **Management Groups** and then the title of the group to configure, in this case **Workstations** this displays the **Assignments** page focused on that group.

2. Clicking the plus sign button allows us to add our group, **Workstation_Group_Administrator** and the associated delegatable role, **Group Administrator**.

3. Once we've selected the group and role, we click the **Save** button.



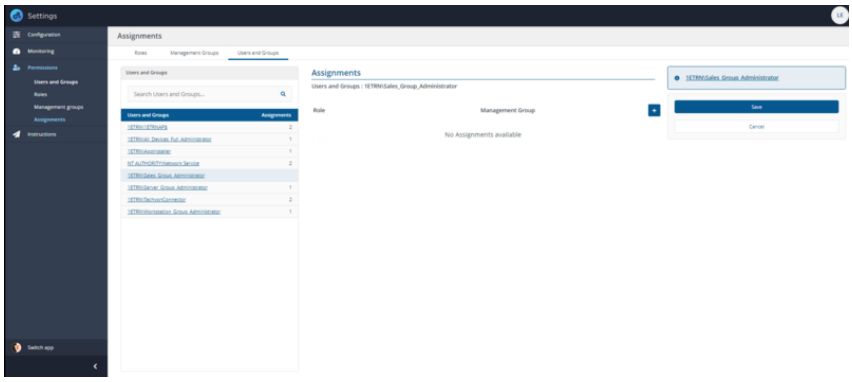
1.7.4.6.3 Users and Groups assignments

Users and Groups focuses on the users and groups you have set up in your Tachyon installation, with the total of their current assignments listed next to each title. To add new assignments, you can click on the user or group name. This displays that user or group's current assignments, with an information panel displaying a summary of that user or group.

In our example we have a new Tachyon installation with only a few groups and accounts, the one shown in the picture is of **All Devices** among the potential groups we can assign is the group **Sales_Group_Administrator**. We have used groups to control the assignments instead of individual user accounts.

Refer to the Users and Groups page for recommendations about how to define users and set their access rights and deactivating or removing Tachyon users or groups.

Refer to the Roles page for recommendations about how best to use roles, and the Roles and Securables page for a full list of roles and permissions.



1.7.4.6.3.1 Example Users and Groups assignment

In our example, we want to use the delegation feature of Tachyon and use the **Group Administrator** role to delegate some tasks to a child management group of **All Devices\Workstations** called **Sales** to another administrator.

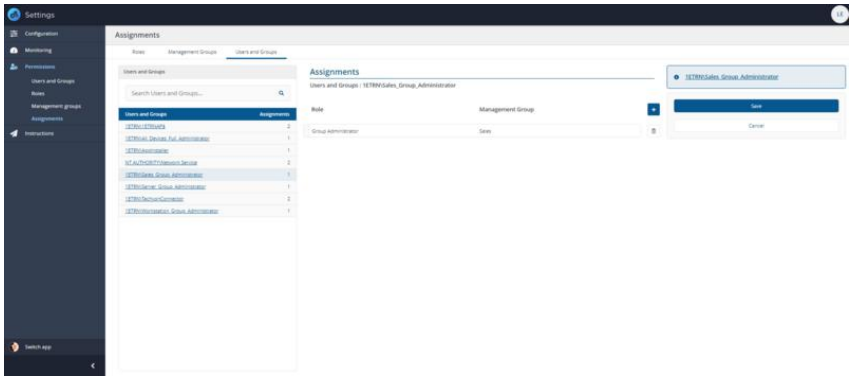
We'll assign the Group Administrator role to a Universal AD group called **Sales_Group_Administrator** which we have added to Tachyon using the Users and Groups page.

To add the new assignment:

1. On the **Settings**→**Permissions**→**Assignments** page, we click on **Users and Groups** and then the title of the group to configure, in this case **1ETRN\Sales_Group_Administrator** this displays the **Assignments** page focused on that group.

2. Clicking the plus sign button allows us to add the **Sales** management group and the associated role, **Group Administrator**.

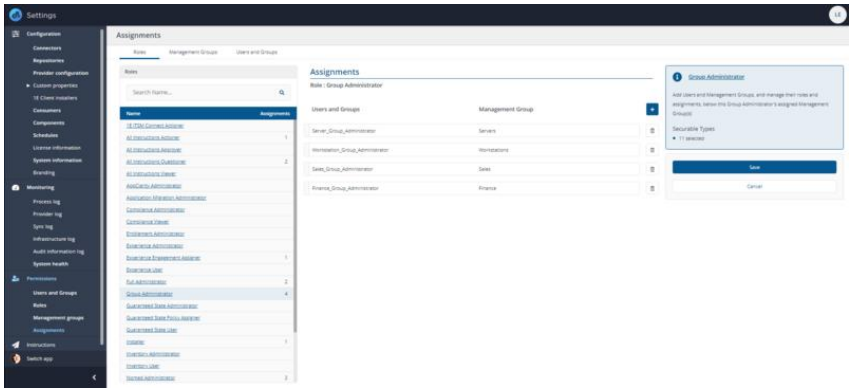
3. Once we've selected the group and role, we click the **Save** button.

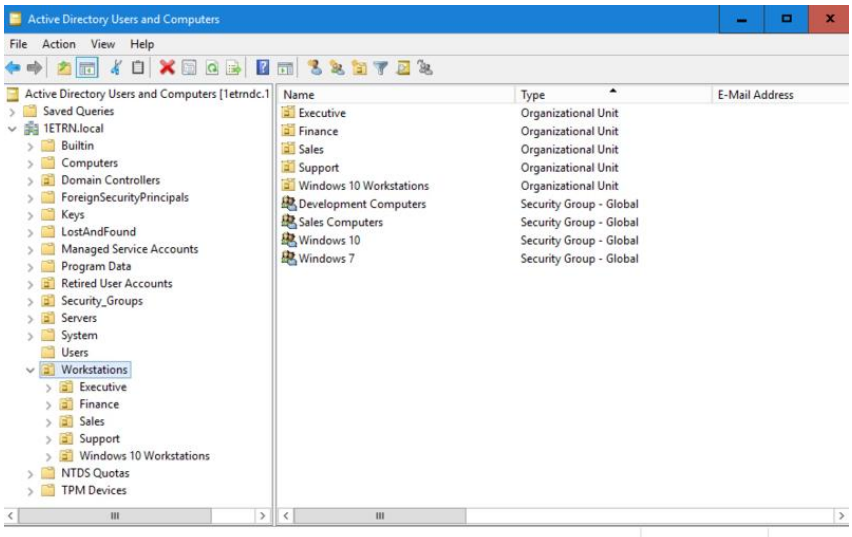


Using this type of structure, we can mirror the organization we have in our Configuration Manager collections or Active Directory.

Once we have completed assigning our **Group Administrator** role to our management groups and associated Tachyon groups, we can effectively delegate responsibility for groups of devices. In our example, this is based on department, where we have OUs in AD that represent different business functions and where we use different administrators to manage each department's devices.

This model could easily apply to organizations that have offices in different locations, whether that is in one country or many. Indeed, you could use management groups to manage different types of device or model or just by OS.





1.7.5 Instructions Menu

Loading and managing Tachyon Instruction sets.

1.7.5.1 Instruction sets page

How to load Instruction Definitions into Tachyon and then create, populate and delete Instruction sets.

The **Instruction sets** page enables users with the **Full Administrator** role, to add, remove and modify the product packs used by Tachyon. This page can be viewed by users with the **All instructions actioner** role.

You can perform these tasks:

- Adding Instruction Definitions into Tachyon
- Creating Instruction sets
- Moving Instructions to Instruction sets
- Deleting Instructions sets and Instructions
- Updating Instructions.

Note

You can create your own platform instructions using SCALE.

SCALE is a powerful, lightweight, cross-platform programming language which combines 1E Client Methods and Modules with SQL commands to enable you to create questions, actions, preconditions, checks, and fixes that can automate almost anything on a Windows, Linux or macOS device.

Refer to 1E SDK.

1.7.5.1.1 Instruction sets overview

Tachyon functionality is based around Instructions, until these are added to the system you will not be able to ask questions or perform actions. 1E provides instructions in zip files called Product Packs. A collection of Product Packs necessary for zip files available in the **Tachyon Platform** zip (available on the 1E Support Portal) and from the 1E Exchange (tachyonexchange.1e.com). Each Product Pack contains a related collection of Instruction Definitions. Product Packs and Instruction Definitions can be added to Tachyon by a **Full Administrator**.

When added into Tachyon, Instructions are immediately allocated to the built-in **Unassigned** Instruction set. Instruction sets provide a way of determining the permissions for the Instructions they contain, but the **Unsassigned** Instruction set is only intended as a staging area for newly loaded Instructions - and Instructions in this set cannot be used directly. An Instruction can only belong to a single Instruction set, so after loading it into Tachyon, and before it can be used, it must be moved to another Instruction set - one created by a **Full Administrator**.

Instruction sets created by a **Full Administrator** can be used as the basis for custom roles created by a **Full Administrator** or **Group Administrator**. These custom roles determine the permissions for the Instruction sets and all the Instructions they contain. This enables the administrator to complete the assignment of specific Instruction set roles to users and determine which Instructions they can action, approve, question or view.

Note

Custom roles cannot be defined for the **Unassigned** set and none of the global roles in Tachyon have permissions on the **Unassigned** set. So at least one Instruction set must be added and populated before you can begin to use Tachyon Instructions.

1.7.5.1.2 Adding Instruction Definitions into Tachyon

Instructions can be added to Tachyon from the Instruction sets page in **Settings**.

1.7.5.1.2.1 Uploading Product Packs

You upload Product Packs into the Settings application using the system file open dialog. To do this:

1. Navigate to the **Settings**→**Instructions**→**Instruction sets** page.
2. Click the **Upload** button on the header for the page.
3. In the **Open** dialog, locate and select the file(s) you want.
4. Click the **Open** button.
5. At this point all the Instructions from the selected Product Packs or Instruction Definition files will be uploaded into Tachyon and added to the default **Unassigned** Instruction set.

1.7.5.1.3 Creating Instruction sets

Instruction sets can be created in the following ways:

1.7.5.1.3.1 Creating an Instruction set from selected Instructions

To add an Instruction set from selected Instructions (as shown in the animation):

1. Navigate to the **Settings**→**Instructions**→**Instruction sets** page.
2. Select the Instructions you want to move to the new set by checking the checkbox at the left-hand end of the instruction's row.
3. Click the **Add New set** button.
4. In the **Add new instruction set** popup, enter a suitable name for the Instruction set.
5. You can optionally add a custom icon, in JPG or PNG format, that will be used when displaying the instruction:
    a. Click the **Choose File** button.
    b. In the **Open** dialog, locate and select the JPG or PNG file you want to use.
    c. Click **Open** to load the file into Tachyon.
    d. The file location and a preview of the file will be displayed in the popup.
6. Ensure that the **Include *n* selected instructions** checkbox is checked
7. Click the **Add** button

When familiarizing yourself with the new instructions contained in a Product Pack it can be convenient to create a matching Instruction set to hold all its instructions. You can then set permissions for all the instructions contained in the Product Pack in one go. Later on you can then add other Instruction sets and move the Instructions in order to refine the permissions for each instruction.

1.7.5.1.3.2 Creating an empty Instruction set

To add an empty Instruction set where you can subsequently move Instructions:

1. Navigate to the **Settings→Instructions→Instruction sets** page.
2. Click the **Add new set** button.
3. In the **Add new instruction set** popup, enter a suitable name for the Instruction set.
4. You can optionally add a custom icon, in JPG or PNG format, that will be used when displaying the instruction:
    a. Click the **Choose File** button.
    b. In the **Open** dialog, locate and select the JPG or PNG file you want to use.
    c. Click **Open** to load the file into Tachyon.
    d. The file location and a preview of the file will be displayed in the popup.
5. Click the **Add** button.

1.7.5.1.4 Moving Instructions to Instruction sets

The following steps are used to move instructions between Instruction sets:

1.7.5.1.4.1 Move one or more selected Instructions:

1. Select the source Instruction set you want to move the Instruction(s) from, or select **All**, from the list of Instruction sets, and locate the Instruction(s) you want to move.
2. Check the checkbox at the start of each Instruction item in the Instructions table for each Instruction you want to move.
3. When the selection has been made click the **Move** button.
4. In the **Move instructions** popup subsequently displayed:
    a. Select the desired destination Instruction set from the **Destination instruction set** dropdown list.
    b. Click **Move** when the set has been selected.

1.7.5.1.5 Deleting Instructions sets and Instructions

Instruction sets are relatively simple to add, populate and delete, making the re-organization of Instruction permissions easy to do.

When deleting you get to choose whether you just want to delete the Instruction set or to also remove the Instructions in the Set from Tachyon:

- If you choose to delete just the Instruction set, any Instructions it contained will be returned to the **Unassigned** Set, effectively making them unavailable until they are assigned to another Instruction set.

- If you choose to delete both the Instruction set and all the Instructions it contains, those Instructions will be unavailable to Tachyon until they are loaded back into the system and assigned to another Instruction set.

Before deleting you need to be aware:

- Instructions in the Instruction set you want to delete may currently be running. Deleting an Instruction set will invalidate any role-based permissions from that point onwards, though any instructions that are in flight will not change.
- Any Custom Roles that were previously configured for the deleted Instruction set will still remain but will be disconnected from the deleted Instruction set.

1.7.5.1.5.1 Deleting an Instruction set

The following steps can be used to delete an Instruction set:

1. Navigate to the **Settings→Instructions→Instruction sets** page.
2. Locate the Instruction set you want to delete in the Instruction sets list.
3. Hover the mouse over the Instruction set name, a tooltip with three vertical dots will appear. Click on this to display a menu.
4. Select **Delete**.
5. In the **Delete instruction set** popup subsequently displayed you have the choice as to whether you want to just delete the Instruction set or delete the Instruction definitions it contains too. To delete both you check the **Delete both instruction set and instructions inside set** checkbox.
6. Once you've made your choice click the **Yes, delete instruction set** button to proceed with the deletion.
7. If you chose to just delete the Instruction set, as shown in our example, the Instructions previously held in the Instruction set go back to the **Unassigned** Instruction set.
8. If you chose to delete the Instruction set and instructions all the instructions contained in the set are removed from Tachyon.

1.7.5.1.5.2 Deleting one or more selected Instructions from Tachyon

The following steps can be used to delete one or more selected Instructions:

1. Navigate to the **Settings→Instructions→Instruction sets** page.
2. In the Instructions table, select the Instruction set containing the Instruction(s) you want to delete, or select **All**.
3. Select the checkbox at the left-hand end of the Instruction's row in the Instructions table for each one you want to delete.
4. Click on **Delete** button in the button panel on the right.
5. In the **Confirm delete** dialog subsequently displayed click **Delete** to continue and remove the selected Instruction(s) from Tachyon or **Cancel** to cancel the operation.

1.7.5.1.6 Updating Instructions

To update an Instruction you load the newer version into Tachyon, and it will be updated in place, keeping any currently set Instruction set intact.

Statistics for the upload operation can be viewed by clicking on the drop zone.

1.7.5.1.6.1 Upgrading and updating Instructions

Tachyon Instructions are designed as far as possible to be backwards compatible, but as a general rule we recommend that you update your Tachyon Product Packs to the latest version so that you can gain the benefit of newer features.

When upgrading you should be able to safely keep your existing Instructions. We recommend that newer versions of Instructions are verified in a test environment to ensure that they still behave as expected before updating in your production environment.

> **Note**
>
> An instruction is not upgraded if it is the same version, or is currently *in use*. You will be notified if any instructions are not upgraded because they are in use. You can upload the product pack again later, after the instruction has completed, or cancelled.

Your license should retain any code signing certificates you may have registered. This means your custom instructions should continue to be licensed as normal following an upgrade of Tachyon. You may want to check the /document/preview/736743#UUID-33c212b3-863e-21bc-bc5d-52e41a0492b3 in the TachyonSDK pages to check for any changes to the SCALE language.

1.8 Introducing Inventory

How to use the Inventory application to view and export inventory, and manage associations.

Inventory provides normalized inventory, software usage analytics, and (enterprise tier only) ServiceNow CMDB Augmentation:

- **Normalized inventory** - consolidate and normalize software inventory into a consistent Vendor, Product, and Version schema to get a clear view on what's out there. Understand hardware usage, such as which employees use the most devices.
- **Software usage analytics** - group all software into Used, Rarely Used, and Unused so you can make better licensing decisions and reduce software bloat.
- **ServiceNow CMDB augmentation** (enterprise only) - augment ServiceNow CMDB with real-time, hyper-accurate inventory to solve the stale data problem.

1.8.1 Inventory features

The Inventory app captures data from different sources, then consolidates, normalizes, and stores it in repositories. The Inventory app is also used to view and export inventory, and manage associations.

Inventory uses connectors to capture software, hardware, and other data from sources such as Tachyon, Configuration Manager, Big Fix, and vCenter where it is consolidated, de-duplicated, and normalized. Normalization uses software and hardware entries in The 1E Catalog.

An empty repository called **Default Inventory** is provided out of the box. You can optionally create additional inventory repositories to partition data by source, time period, or other purposes. To populate a repository, you must use one or more inventory connectors, and either manually sync the data or schedule a sync. For more detail, please refer to Repositories page and Schedules page in Settings.

Inventory repositories are used by the following applications:

- Introducing Patch Success - reports on and ensures successful patching of your enterprise
- Introducing Application Migration - automates the migration of applications during a Configuration Manager OS deployment
- Introducing AppClarity - manages entitlements, compliance and reclaiming unused software.
- Any application - if you need it to use Management Groups.

You will need to decide which of the following connectors you will use to populate Inventory repositories.

Connectors are used to connect to other 1E and third party systems, retrieve their data and populate repositories. The following inventory connectors are provided to populate the Repositories page:

- BigFix connector — Connects to a BigFix Inventory database server.
- BigFixInv connector — Connects to a BigFix Inventory database.
- File Upload connectorr — Uploads inventory data from a folder containing tab (TSV) and comma (CSV) separated value file(s).
- Intune connector — Connects to an Intune application and collects inventory and usage data.
- Microsoft Office 365 connector — Connects to an Office 365 application in Intune and pulls in inventory and usage data.
- OpenLM connector — Connects to an OpenLM database server.
- Oracle LMS connector — Connects to Oracle LMS and queries it for inventory information.
- ServiceNow connector — Connects to a ServiceNow instance to import basic inventory data.
- System Center Configuration Manager connector — Connects to a Configuration Manager database and pulls in inventory and usage data.
- Tachyon connector — Connects the Inventory and SLA components to support the Management group and Inventory Powered Inventory features. The Inventory Powered Inventory feature uses instructions to fetch inventory data from clients, and is a prerequisite for Patch Success.
- vCenter connector — Connects to a vCenter server and pulls in inventory data.
- Windows Server Update Services connector — Connects to a WSUS database and pulls in patch data.

Use the links above to find more information about each type of connector. Please refer to Introducing Inventory for more information about viewing and exporting inventory repositories.

Additional connectors may exist for add-on Consumer applications that have been installed. For example, Connectors page has the following connectors to populate its entitlement repository:

- AppClarity v5.2 connector — Exports entitlements from an AppClarity 5.2 database into a TSV file, which can then be reviewed and imported into.
- Entitlement .tsv connector — Uploads entitlements from a folder containing one or more tab or comma separated value file(s).

Note

AppClarity and some other Consumer applications add additional connectors to populate their repositories.

1.8.1.1 AI Powered Auto-curation

Using the AI Powered Auto-curation feature, you'll be able to increase the total amount of normalized software in your Inventory repositories. This is done using AI that integrates with the inventory consolidation process. By using AI, your organization will benefit from significant numbers of normalized software and a reduced manual effort needed to normalize software.

You can enable AI Powered Auto-curation either when you install Tachyon or post installation. Refer to AI Powered Auto-curation to find out how you can do this.

1.8.1.2 AI Powered Auto-curation

Using the AI Powered Auto-curation feature, you'll be able to increase the total amount of normalized software in your Inventory repositories. This is done using AI that integrates with the inventory consolidation process. By using AI, your organization will benefit from significant numbers of normalized software and a reduced manual effort needed to normalize software.

You can enable AI Powered Auto-curation either when you install Tachyon or post installation. Refer to AI Powered Auto-curation to find out how you can do this.

1.8.2 Hardware

Hardware Inventory shows data captured from sources such as Configuration Manager, Big Fix, and vCenter if you have them configured.

The dashboard is refreshed (recalculated) when the page is opened or the page is refreshed in the browser.

1.8.2.1 Hardware Inventory

The Hardware Inventory page shows a list of all hardware gathered using the Configuration Manager software inventory.

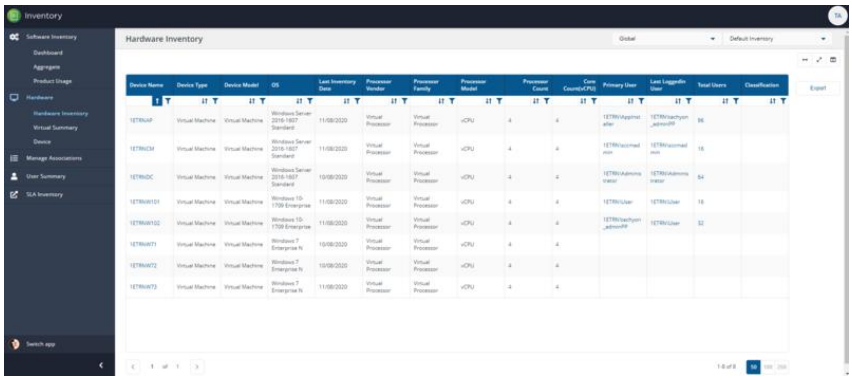
In the top right of the page in line with the screen title are two dropdown lists, **Global** and **Default Inventory**. If you select the **Global** dropdown list and look at the available options, you'll see any Management groups you have configured listed there.

If you have multiple Management Groups, choose each option and see how the display changes to show the software installed on each Management group, you may need to scroll to see all the groups. To find out more about Management Groups refer to the Management Groups page.

If you have configured more than one Inventory they will be available to choose from the **Default Inventory** dropdown list.

You can customize which fields are displayed on the page by using the **Choose Columns** control.

> **Note**
>
> You can choose which columns are displayed in some detail tables to increase readability. On pages where you can pick the displayed columns you'll see a new control like the one below:
>
>
>
> To find out more about this feature refer to Choosing the columns displayed in reports.

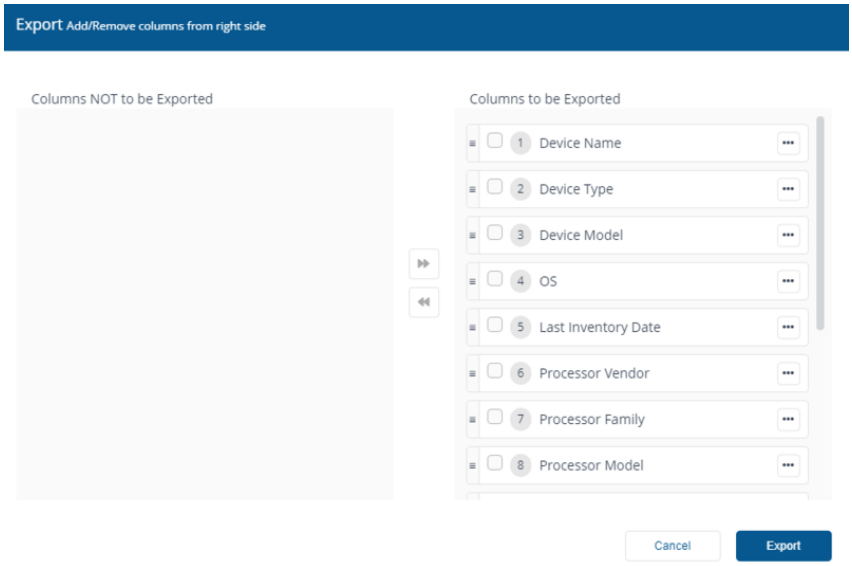


1.8.2.1.1 Exporting Hardware Inventory

You can use the **Export** button to the right of the table to export currently displayed data in a downloadable report.

When you click on the **Export** button you'll see the **Export** popup. You can choose which columns to export in the same way you can choose columns to display in the main report panel.

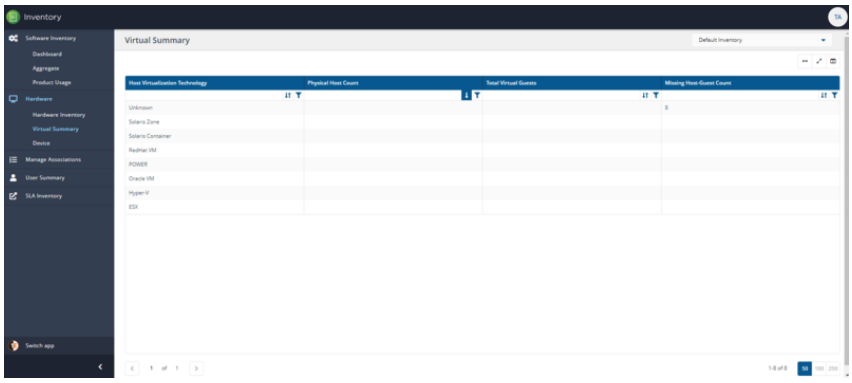
The report is exported in a .TSV format, for example, **HardwareInventory_20200813111828.tsv**. The file is exported and downloaded to the default location for the browser you are using.



1.8.2.2 Virtual Summary

This page displays information on the **Host Virtualization Technology**, **Physical Host Count**, **Total Virtual Guests** and **Missing Host-Guest Count** in your environment, in the example we only have eight devices shown.

In the top right of the page in line with the screen title, there is a dropdown list, **Default Inventory**. If you have configured more than one Inventory they will be available to choose from here.



1.8.2.3 Device

The **Device** page will be blank by default.

When you enter a device name in the **Search device** field at the top of the screen, it will resolve, so you can select it. The information returned shows **Basic Info** for the selected device and **User Details** such as **User Name** and **Last Login**.

At the bottom of the page, there are two tabs showing the software titles installed on the device:

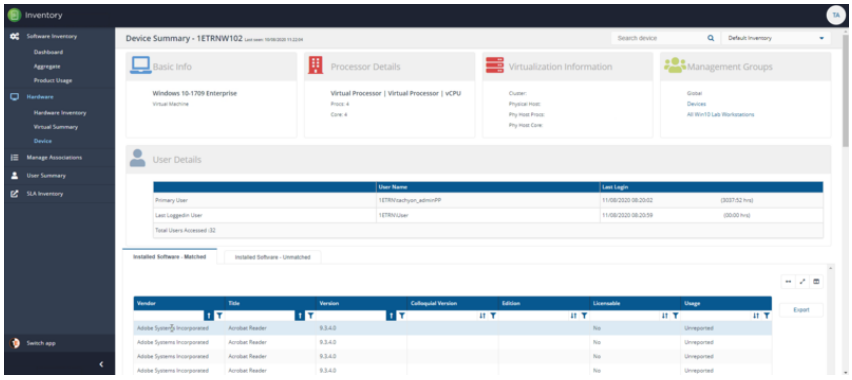
- Installed Software - Matched tab- titles matched with titles in Inventory
- Installed Software - Unmatched tab titles unmatched with titles in Inventory.

In the top right of the page in line with the screen title there is a dropdown list, **Default Inventory**. If you have configured more than one Inventory they will be available to choose from here.

Note

The **Export** button is only enabled for users with either a Full or Group Administrator role. For more details about roles refer to the Roles page.

The Roles page lets you view the system roles and currently defined custom roles. From the Roles page, you can also go into each role to set its membership and any associated management groups.



1.8.2.3.1 Installed Software - Matched tab

The Installed Software - Matched tab shows titles matched with titles in Inventory using the following default fields:

- Vendor
- Title
- Colloquial Version
- Edition
- Licensible
- Usage.

You can customize which fields are displayed on the page by using the **Choose Columns** control.

Note

You can choose which columns are displayed in some detail tables to increase readability. On pages where you can pick the displayed columns you'll see a new control like the one below:

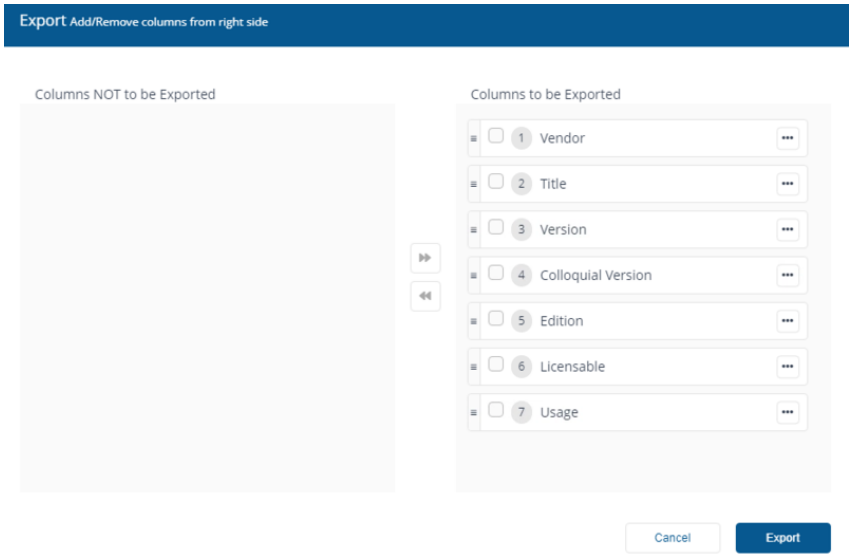
To find out more about this feature refer to Choosing the columns displayed in reports.

1.8.2.3.1.1 Exporting the Installed Software - Matched and Installed Software table

You can use the **Export** button to the right of the table to export currently displayed data in a downloadable report.

When you click on the **Export** button you'll see the **Export** popup. You can choose which columns to export in the same way you can choose columns to display in the main report panel.

The report is exported in a .TSV format, for example, **MatchedSoftware_20200813111828.tsv**. The file is exported and downloaded to the default location for the browser you are using.



1.8.2.3.2 Installed Software - Unmatched tab

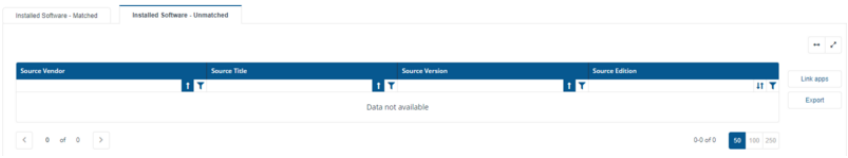
The Installed Software - Unmatched tab shows titles unmatched with titles in Inventory using the following default fields:

- Source Vendor
- Source Title
- Source Version
- Source Edition.

You can customize which fields are displayed on the page by using the **Choose Columns** control.

> **Note**
>
> You can choose which columns are displayed in some detail tables to increase readability. On pages where you can pick the displayed columns you'll see a new control like the one below:

To find out more about this feature refer to Choosing the columns displayed in reports.

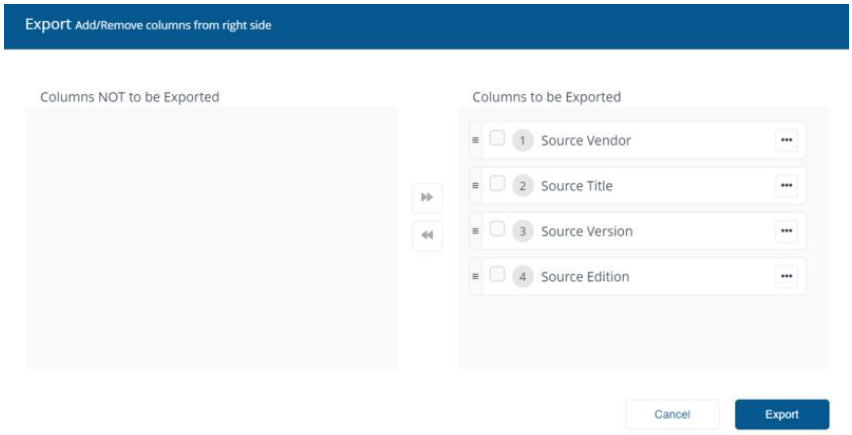


1.8.2.3.2.1 Exporting the Installed Software - Unmatched and Installed Software table

You can use the **Export** button to the right of the table to export currently displayed data in a downloadable report.

When you click on the **Export** button you'll see the **Export** popup. You can choose which columns to export in the same way you can choose columns to display in the main report panel.

The report is exported in a .TSV format, for example, **UnmatchedSoftware_20201022124749.tsv**. The file is exported and downloaded to the default location for the browser you are using.



1.8.3 Software Inventory

Software Inventory shows data captured from sources such as Configuration Manager, Big Fix and vCenter if you have them configured.

The dashboard is refreshed (recalculated) when the page is opened or the page is refreshed in the browser.

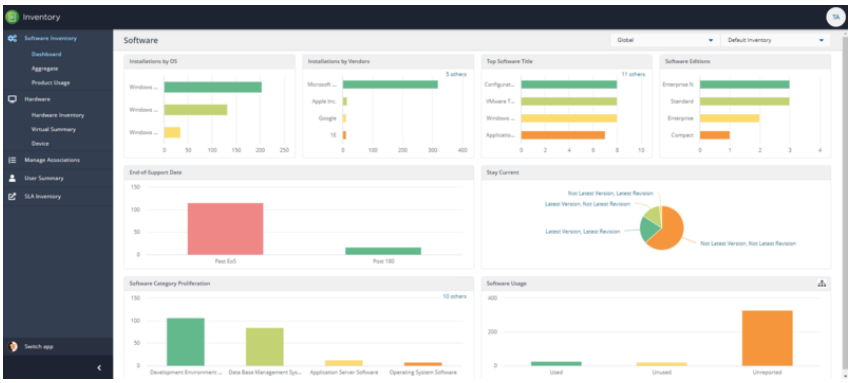
1.8.3.1 Dashboard

The dashboard page displays eight panels, reflecting the current Inventory.

The Software Inventory dashboard presents a number of panels:

- Installations by OS
- Installations by Vendors
- Top Software Title
- Software Editions

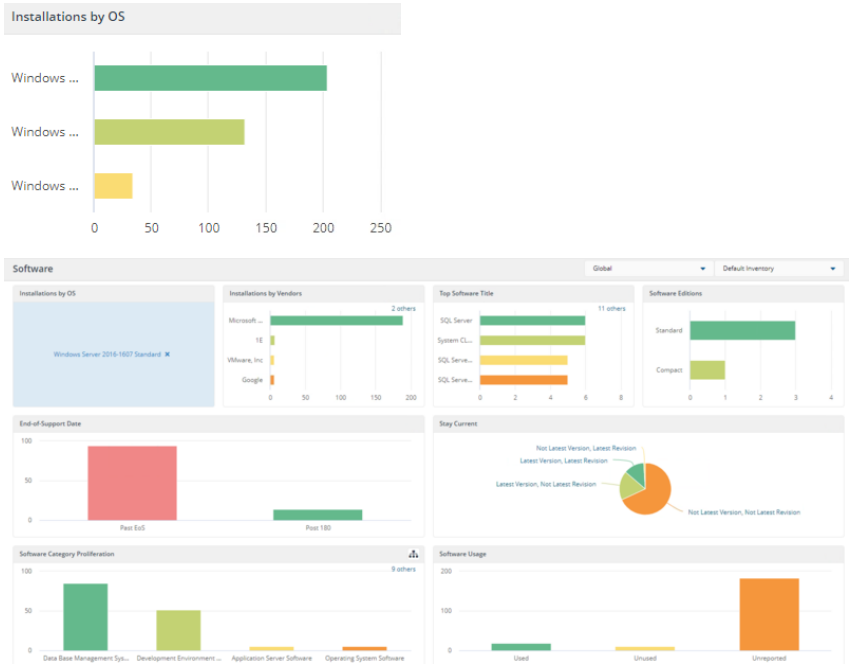
- End-of-Support Date
- Stay Current
- Software Category Proliferation
- Software Usage.



1.8.3.1.1 Installations by OS

This panel presents installations grouped by the operating system.

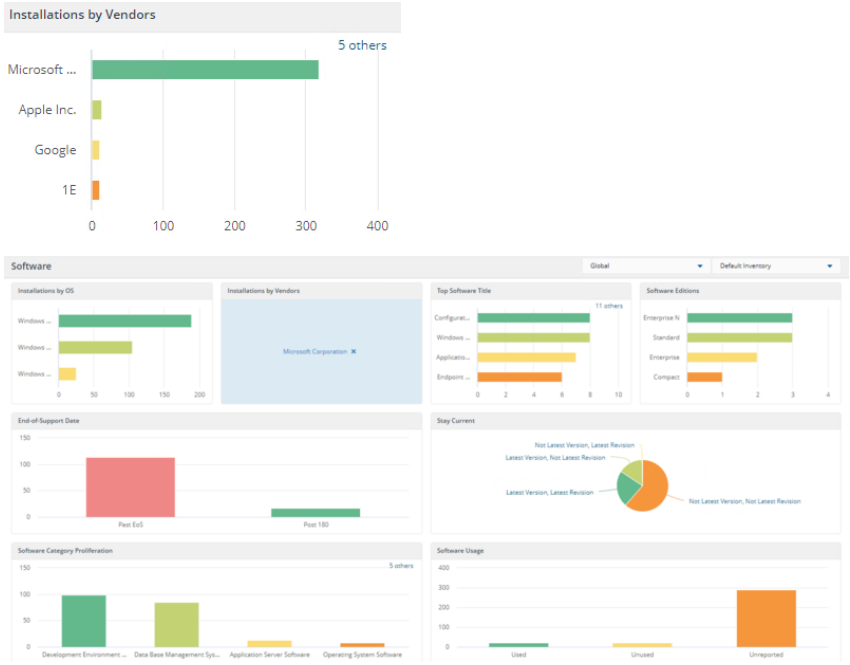
The user has the ability to drill down into each installation for each group by clicking on each color bar. This updates the other fields on the dashboard with data related to your choice. Our example shows details for **Windows Server 2016-1607 Standard**.



1.8.3.1.2 Installations by Vendors

This panel presents installations grouped by vendors.

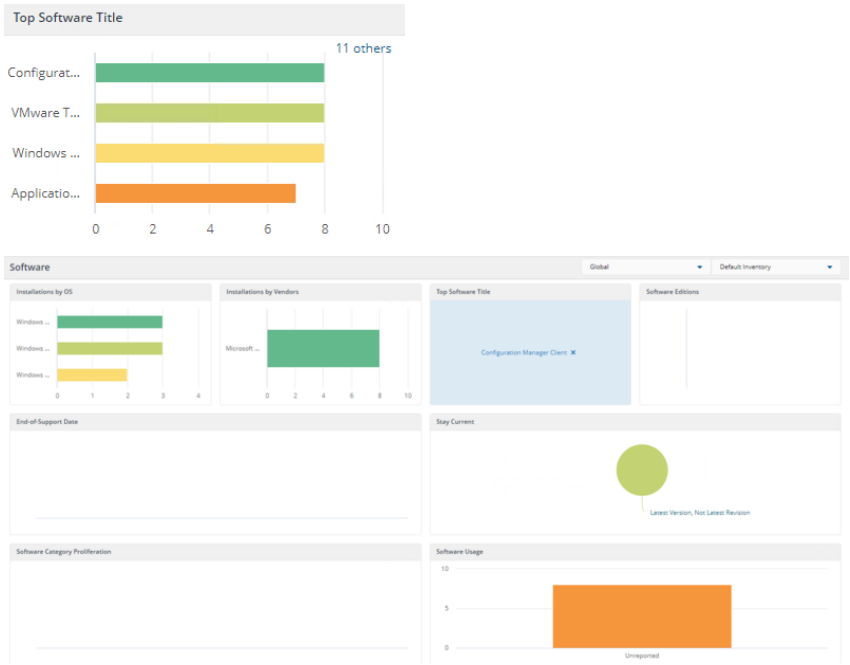
The user has the ability to drill down into each installation for each group by clicking on each color bar. This updates the other fields on the dashboard with data related to your choice. Our example shows details for **Microsoft Corporation**.



1.8.3.1.3 Top Software Title

This panel presents installations grouped by **Top Software Title**.

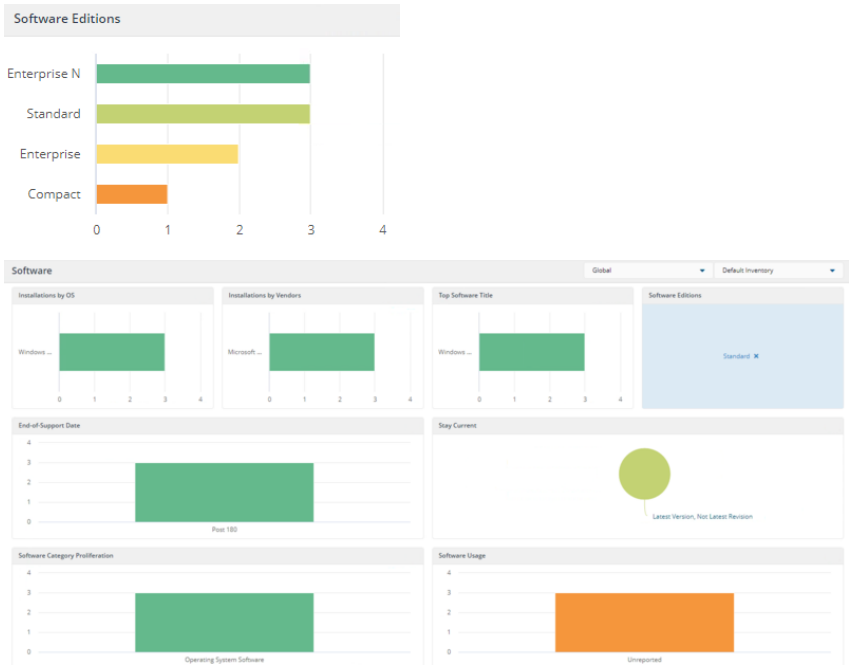
The user has the ability to drill down into each installation for each group by clicking on each color bar. This updates the other fields on the dashboard with data related to your choice. Our example shows details for **Configuration Manager Client**.



1.8.3.1.4 Software Editions

This panel presents installations grouped by **Software Edition**.

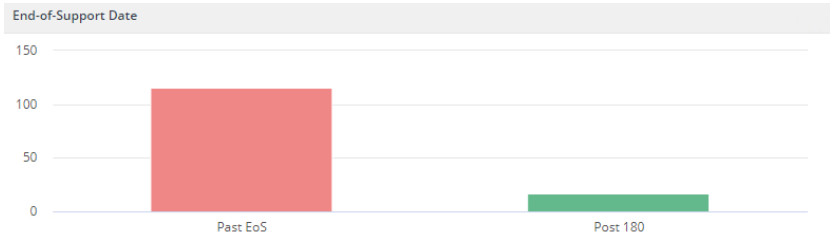
The user has the ability to drill down into each installation for each group by clicking on each color bar. This updates the other fields on the dashboard with data related to your choice. Our example shows details for **Standard** editions.

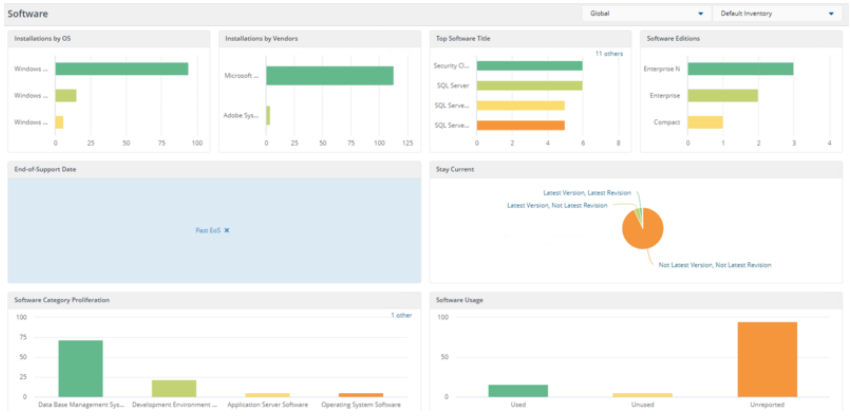


1.8.3.1.5 End-of-Support Date

This panel presents installations grouped by **End-of-Support Date**.

The user has the ability to drill down into each installation for each group by clicking on each color bar. This updates the other fields on the dashboard with data related to your choice. Our example shows details for **Past EoS**.

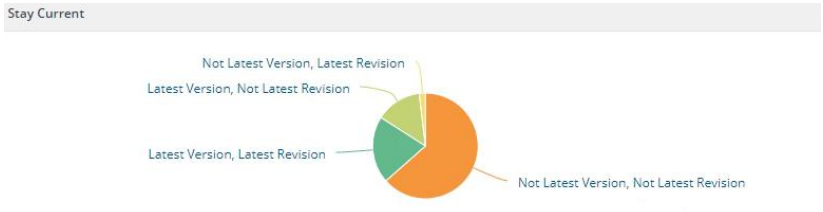


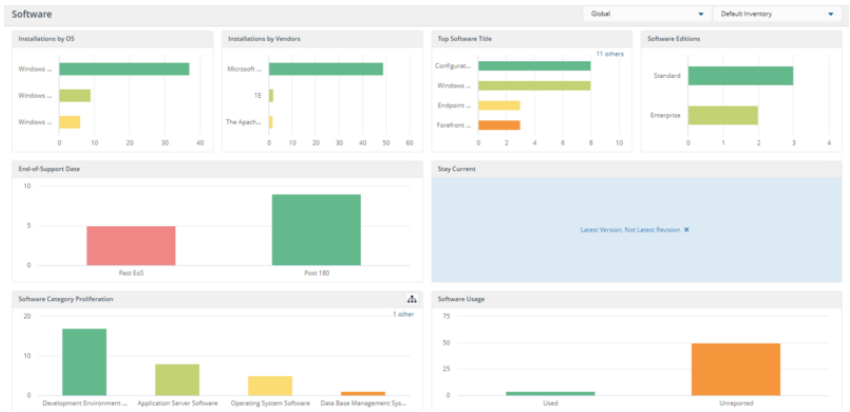


1.8.3.1.6 Stay Current

This panel presents installations grouped by **Stay Current**.

The user has the ability to drill down into each installation for each group by clicking on each color segment. This updates the other fields on the dashboard with data related to your choice. Our example shows details for **Latest Version, Not Latest Revision**.

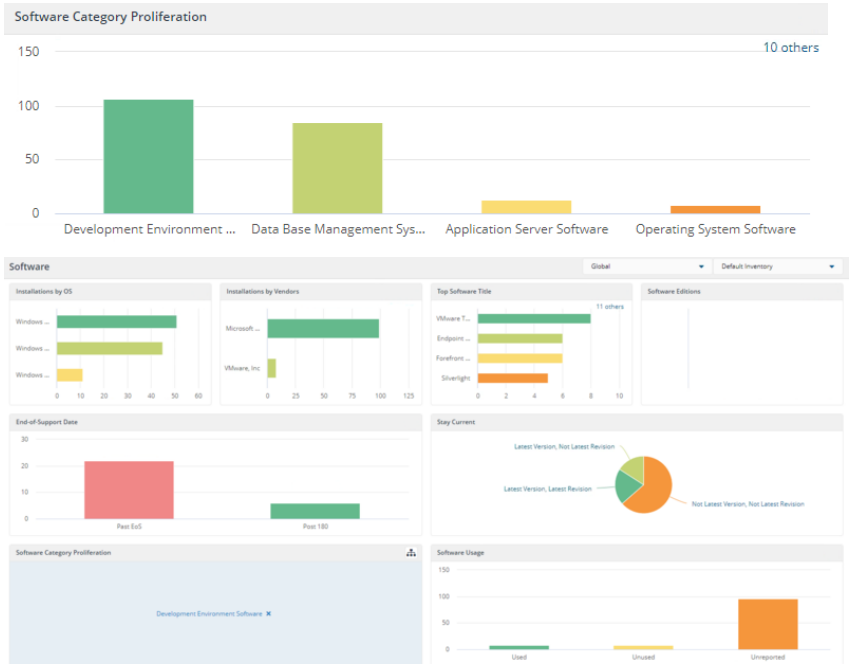




1.8.3.1.7 Software Category Proliferation

This panel presents installations grouped by **Software Category Proliferation**.

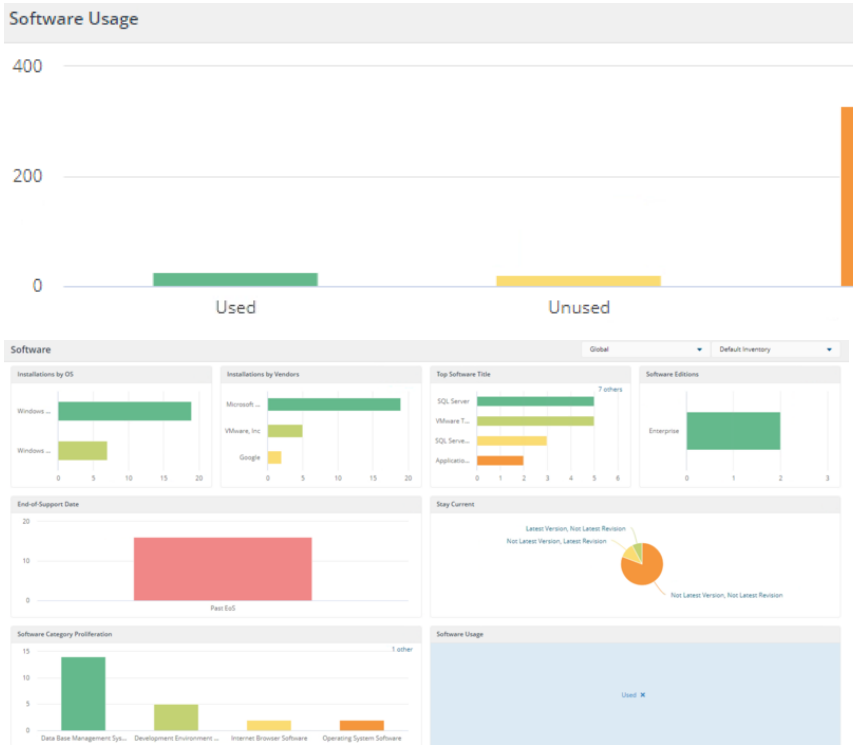
The user has the ability to drill down into each installation for each group by clicking on each color bar. This updates the other fields on the dashboard with data related to your choice. Our example shows details for **Development Environment Software**.



1.8.3.1.8 Software Usage

This panel presents installations grouped by **Software Usage**.

The user has the ability to drill down into each installation for each group by clicking on each color bar. This updates the other fields on the dashboard with data related to your choice. Our example shows details for **Used**.



1.8.3.2 Aggregate

The Aggregated Software Inventory page shows a list of all software gathered using Configuration Manager software inventory.

In the top right of the page in line with the screen title are two dropdown lists, **Global** and **Default Inventory**. If you select the **Global** dropdown list and look at the available options, you'll see listed any additional Management groups you have configured.

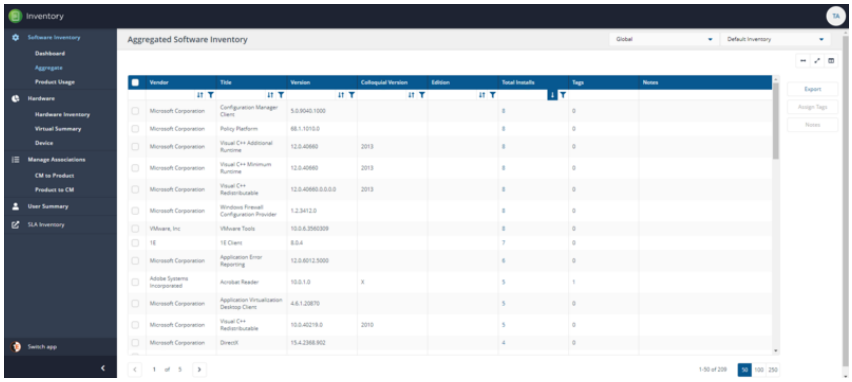
If you have multiple Management Groups, choose each option and see how the display changes to show the software installed on each Management group, you may need to scroll to see all the groups. To find out more about Management Groups refer to the Management Groups page. If you have configured more than one Inventory, they will be available to choose from the **Default Inventory** dropdown list.

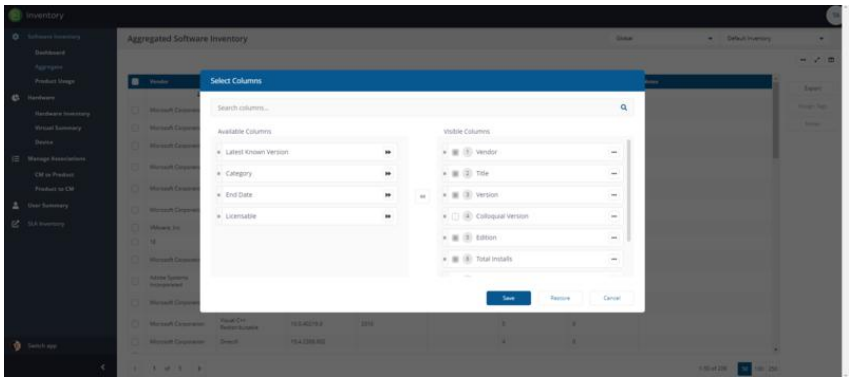
> **Note**
>
> You can choose which columns are displayed in some detail tables to increase readability. On pages where you can pick the displayed columns you'll see a new control like the one below:
>
>
>
> To find out more about this feature refer to Choosing the columns displayed in reports.

The following table shows the available **Aggregated Software Inventory** columns, not all columns are displayed by default. You can add other columns or remove them using the column chooser control.

Column	Description	Displayed by default
Vendor	The software vendor.	Yes
Title	The software title.	Yes
Version	The version of the software installed.	Yes
Colloquial Version	If known or exists, the Colloquial version is installed.	Yes
Edition	The edition installed.	Yes
Total Installs	The number of times the software has been installed on the estate.	Yes
Latest Known Version	The latest version was discovered using AI matching.	No

Column	Description	Displayed by default
Category	Category information is set in Configuration Manager.	No
End Date	If provided, the end date for the License.	No
Licensable	Yes or No if the software is Licensed.	No



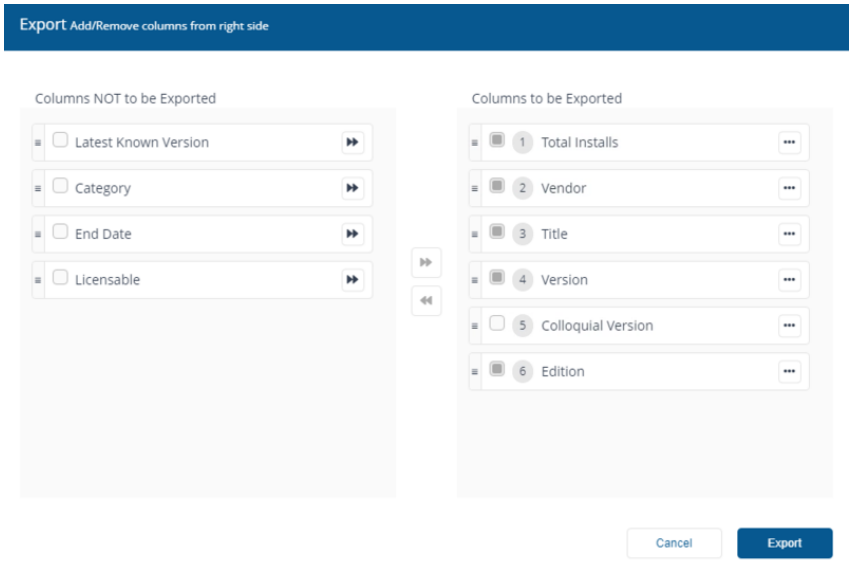


1.8.3.2.1 Export

You can use the **Export** button to export currently displayed data in a downloadable report.

When you click on the **Export** button you'll see the **Export** popup. You can choose which columns to export in the same way you can choose columns to display in the main report panel.

The report is exported in a .TSV format, for example, **AggregatedSoftwareInventory_20200813095415.tsv**. The file is exported and downloaded to the default location for the browser you are using.



1.8.3.2.2 Assign Tags

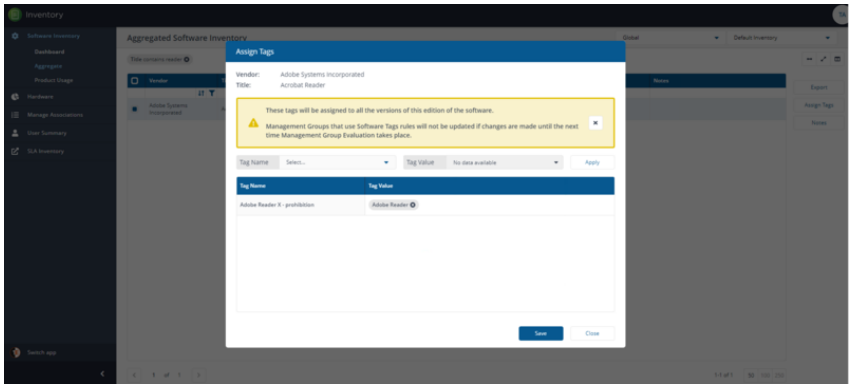
Using Software Tags allows you to create custom labels and associate them with the software titles you have deployed in your estate. An administrator with either the **Full Administrator** or **Group Administrator** role can set Software Tags in their environment, they can also create Management Groups based on the tag name and value. For details about configuring Users, Roles, and Management Groups refer to the Permissions Menu pages.

In short, you can work with Software tags by:

1. Creating your Software Tag.
2. Associating the new tag with a software title.
3. Creating a Management Group based on the Software Tag name and Tag value rules (This step can be run anytime before an evaluation).
4. Evaluating the new Management Group by running a Basic Inventory Consolidation.

If an administrator adds or modifies Software Tags or associations, they will have to run the Management Group evaluation report again to see the updated devices reflected in the Inventory.

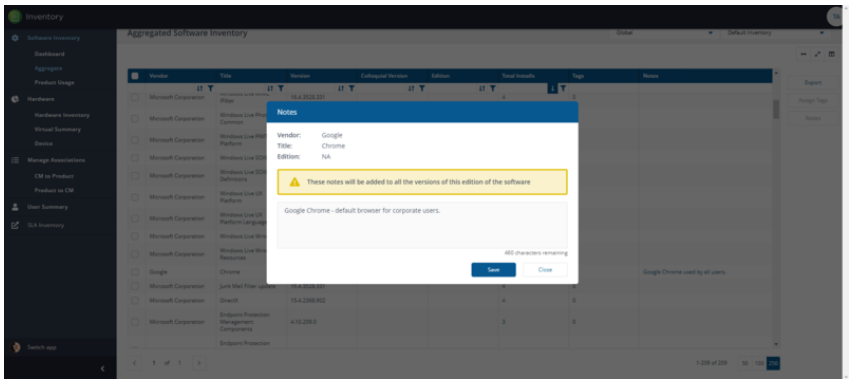
To find out more about using Software Tags, refer to the Software Tags page.



1.8.3.2.3 Notes

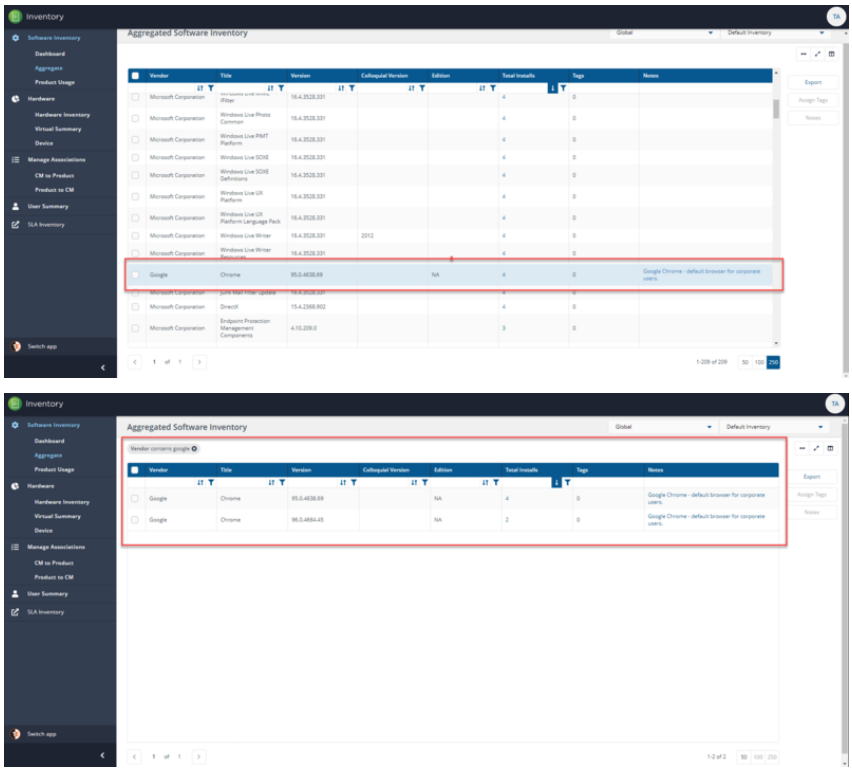
An important feature of software management is to provide additional information for each software title.

From Inventory 8.0 you can add notes which allow you to add additional information for each software title. Software notes are a simple text field that can be added to any software title as required.



You can add a note to each title, and it will be added to every version of that software edition. In our example, we applied a note to **Google Chrome v95.0.4638.69**.

But as the note applies to all versions of Google Chrome when we filter **Aggregated Software Inventory** by **Vendor contains google**, we can see that our note was also applied to **Google Chrome v95.0.4664.45**.



1.8.3.3 Product Usage

The **Product Usage** page shows the distribution of software installs, the top five categories by install and top saving opportunities across your software estate.

In the top right of the page in line with the screen title are two dropdown lists, **Global** and **Default Inventory**. If you select the **Global** dropdown list and look at the available options, you'll see any Management groups you have configured listed there.

If you have multiple Management Groups, choose each option and see how the display changes to show the software installed on each Management group, you may need to scroll to see all the groups. To find out more about Management Groups refer to the Management Groups page. If you have configured more than one Inventory they will be available to choose from the **Default Inventory** dropdown list.

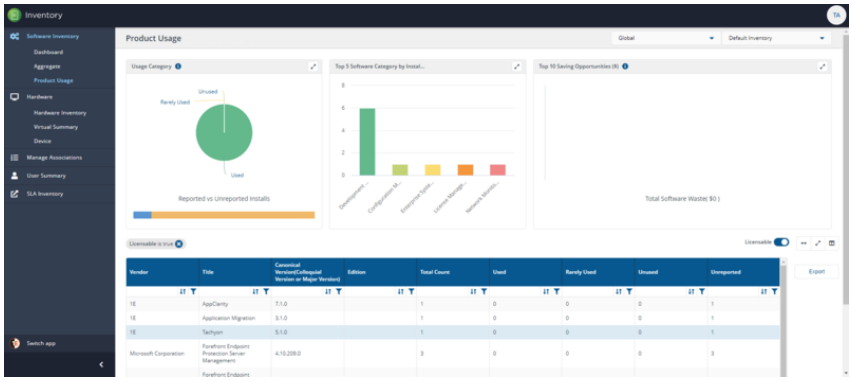
By clicking each colored bar and segment in the three top panels you can narrow the view to only those related products. The table below the top panels is then dynamically updated with these results which are exportable to a downloadable .TSV format. For both the displayed table and the exported file you can choose which columns are shown and exported.

> **Note**
>
> You can choose which columns are displayed in some detail tables to increase readability. On pages where you can pick the displayed columns you'll see a new control like the one below:
>
>
>
> To find out more about this feature refer to Choosing the columns displayed in reports.

Available **Product Inventory** columns:

Column	Description
Vendor	The software vendor.
Title	The software title.
Canonical Version (Colloquial Version or Major Version)	If known or exists the Colloquial version is installed.
Edition	The edition installed.
Total Count	Total count per software title.
Used	Total count of used instances of a title.
Rarely Used	Installs are categorized as rarely used.
Unused	Installs are categorized as unused.

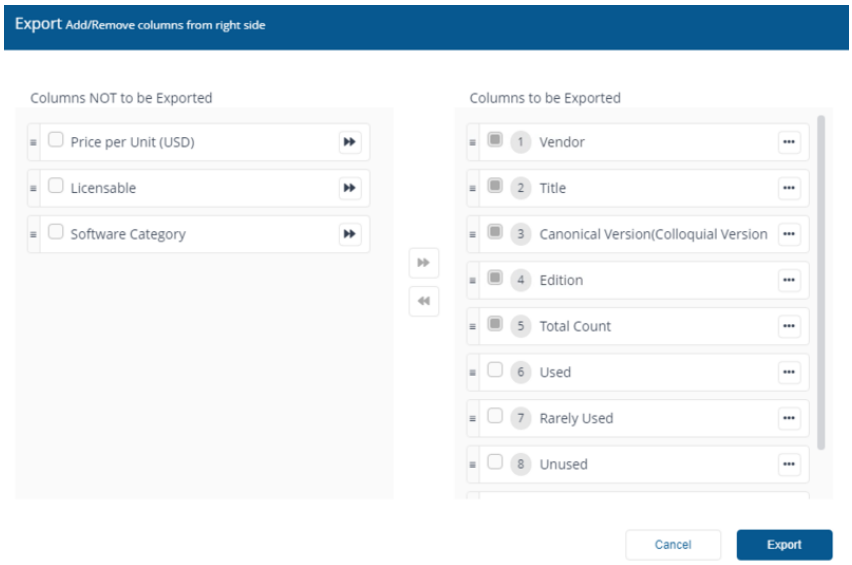
Column	Description
Unreported	Total count of titles where usage information is unavailable.
Price per Unit (USD)	The price per title is shown in the default currency.
Licensable	Yes or No if the software is Licensed.
Software Category	Category information is set in Configuration Manager.



You can use the **Export** button to export currently displayed data in a downloadable report.

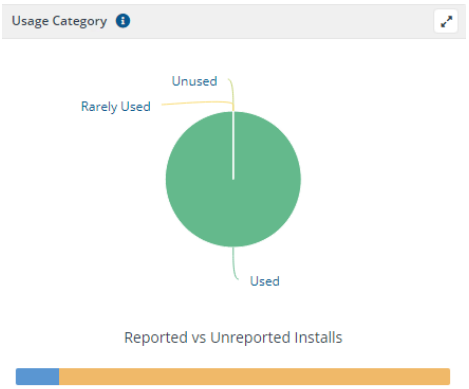
When you click on the **Export** button you'll see the **Export** popup. You can choose which columns to export in the same way you can choose columns to display in the main report panel.

The report is exported in a .TSV format, for example, **InventoryProductUsage_20200813102621.tsv** and is downloaded to the browser's download folder.



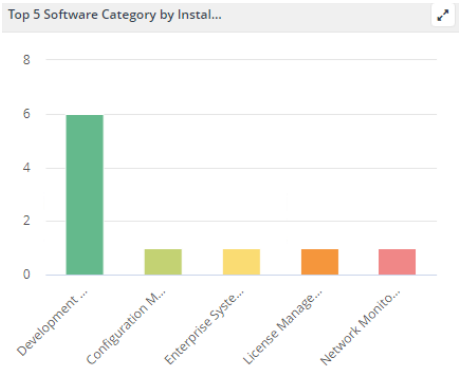
1.8.3.3.1 Usage Category

The pie chart shows the distribution of installs **Used**, **Rarely used**, and **Unused** as a percentage of total installs that report usage (i.e. **Total Reported Installs**). The bar at the bottom shows the distribution of installs as **Reported** and **Unreported** as a percentage of **Total Installs**.



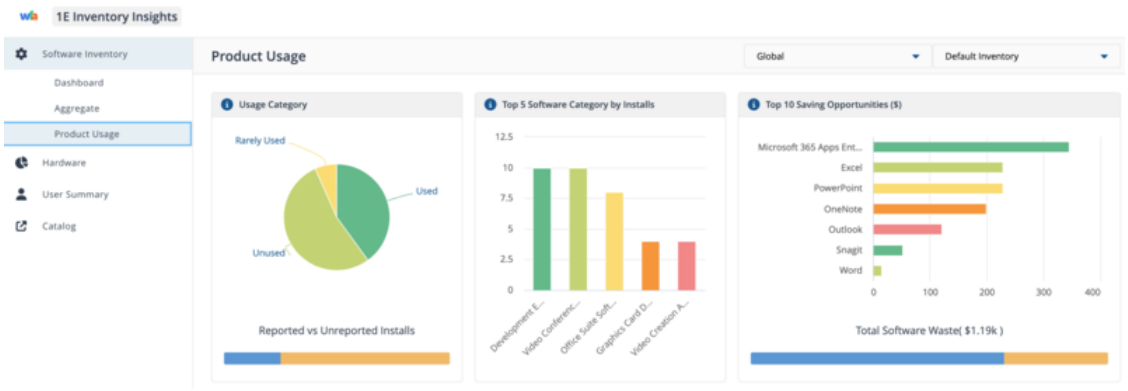
1.8.3.3.2 Top 5 Software Category by installation

The bar chart shows the top five categories by installs. The chart ignores operating systems and internet browser categories for calculating the top five categories.



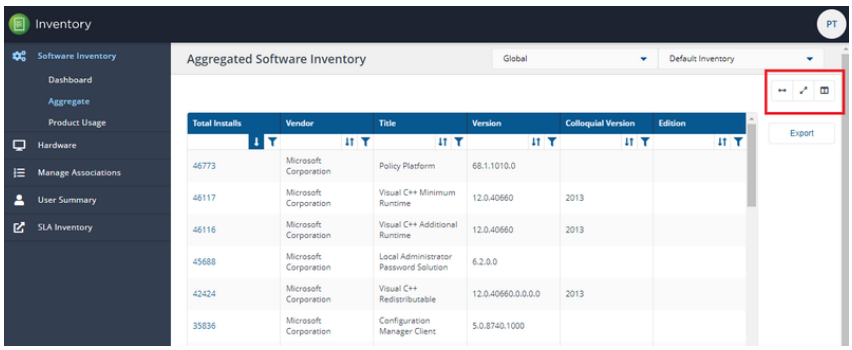
1.8.3.3.3 Top 10 Saving Opportunities ($)

The bar chart shows the top ten products offering maximum saving opportunities in USD. The calculation is based on multiplying a product's unit price and the sum of **Unused** and **Rarely Used** installs. The bar at the bottom shows the total opportunity in USD, segregated from **Unused** and **Rarely Used** installs.



1.8.3.4 Choosing the columns displayed in reports

To increase readability, you can choose the columns displayed in detail tables. On the pages where you can pick the displayed columns you'll see the control highlighted in the opposite example.



When you click on the **Choose columns** control it opens a popup displaying every column on the current screen, the controls are:

Control	Explanation
Available Columns	Columns which are hidden by default from being displayed on screen. You can still include any of them to display on screen.
Visible Columns	Displays the list of columns displayed on screen. Mandatory Columns cannot be excluded, the selection controls for these items are disabled. They can still be moved up or down. **Tip** Some pages have mandatory columns and a set of default hidden columns.
Arrow buttons	To move up or move down, exclude or include any column, clicking on the ellipsis displays these additional controls:

Control	Explanation
Drag and drop	You can drag and drop columns to change how they are displayed.
Exclude columns	Exclude column button allows you to select columns to exclude from the current display.

For example, in**Inventory**→**Aggregated Software Inventory** we use the **Choose columns** control to pick which columns are displayed.

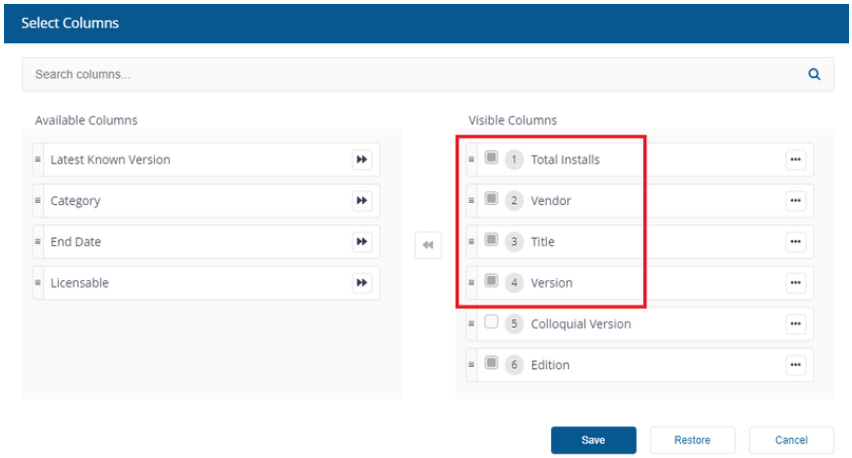
On this page the default columns are:

- Total Installs
- Vendor
- Title
- Version
- Colloquial Version
- Edition.

Some pages also have mandatory columns which cannot be excluded from the display. The excluded columns are greyed out and cannot be removed.

The Aggregated Software Inventory page has the following mandatory columns which you cannot remove:

- Total Installs
- Vendor
- Title
- Version
- Edition.



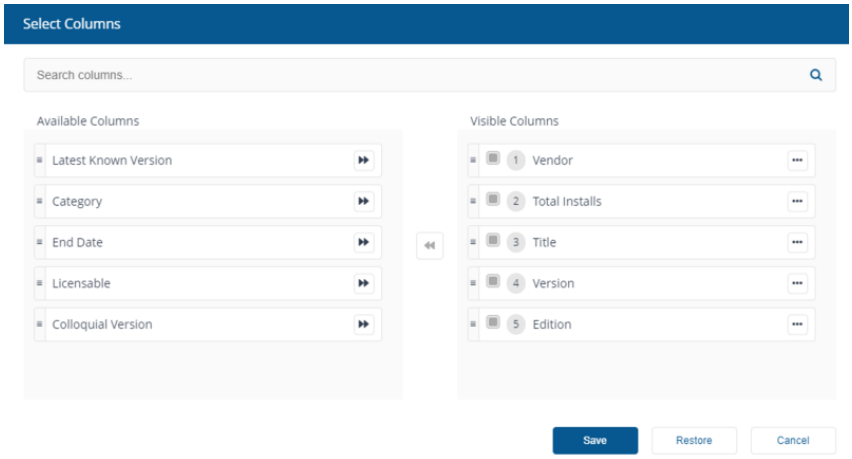
From this screen we chose to exclude **Colloquial Version** and move **Vendor** to the top of the list.

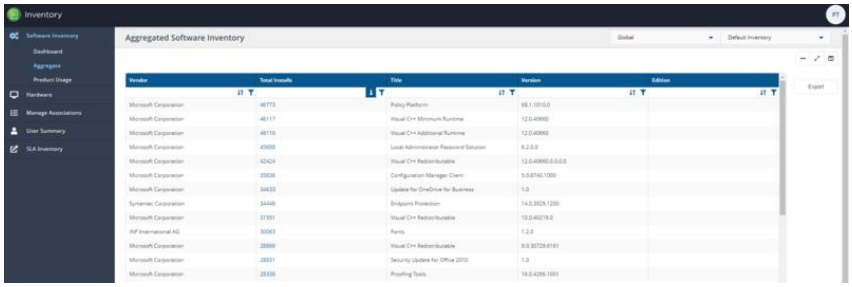
To apply this view to the current report, we click **Save**.

You can also choose **Restore** to reset the column chooser or **Cancel** to cancel your changes and exit the **Choose columns** control.

Note

When you refresh reports on a page where you have amended the displayed columns, the report view will reset back to its default view once the refresh completes and the page reloads.





1.8.4 Manage associations

Applications and Packages in Configuration Manager are identified by a name and optionally publisher and version arbitrarily determined by the Configuration Manager administrator that created them. The Inventory platform uses a standard format of Vendor, Title, Version, and Edition to identify applications.

The **Manage Associations** section of Inventory enables an administrator to effectively normalize the Applications and Packages imported from Configuration Manager by associating them with a Vendor, Title, Version, and Edition defined in the 1E Catalog. These associations are then used to define migration rules in Introducing Application Migration and reclaim rules in Introducing AppClarity.

To manage associations, the Inventory repository used by your application must be populated by a System Center Configuration Manager connector that collects details of Applications and Packages defined in Configuration Manager.

1.8.4.1 The Manage Associations section

The Manage Associations section allows you to associate Applications and Packages in CM with a Vendor, Title, Version and Edition from the 1E catalog. It provides two views of the data.

- The **CM to Product** view lists all Applications and Packages that were imported from CM during the last Inventory sync. You typically use this view when initially setting up Application Migration, as it allows you to work through each Application and Package available for deployment and associate them with a suitable Vendor, Title, Version and Edition.

  You would also use this view after new Applications or Packages have been added in CM. Once you've created the associations you can then create migration rules that refer to the products without having to refer back to the CM Application or Package that installs them.

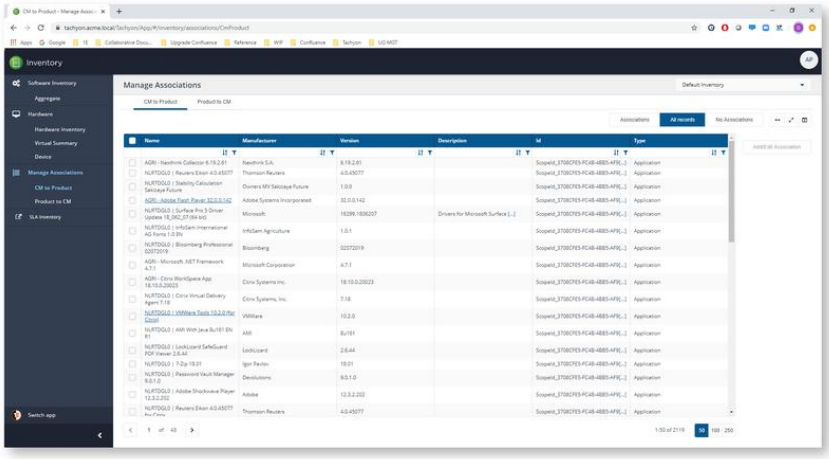
- The **Product to CM** view lists all products (by Vendor, Title, Version and Edition) installed in your environment, indicating the products that have been associated with an Application or Package in CM and can therefore be installed through Application Migration or removed using AppClarity reclaim.

  This view is ideal for identifying the products installed in your environment that are not currently set up for automated installation or removal using Application Migration and AppClarity.

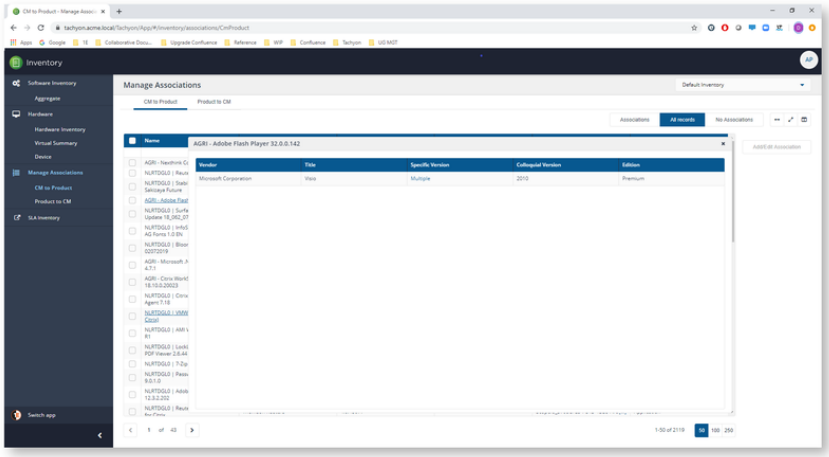
1.8.4.1.1 Associating a Configuration Manager application or package with a product (Vendor, Title, Version, and Edition)

After syncing a connector with Configuration Manager, the **Inventory→Manage Associations->CM to Product** tab on the Manage Associations page lists the applications and packages found in Configuration Manager.

> **Note**
>
> You can choose which columns are displayed in some detail tables to increase readability. On pages where you can pick the displayed columns you'll see a new control like the one below:
>
>
>
> To find out more about this feature refer to Choosing the columns displayed in reports.

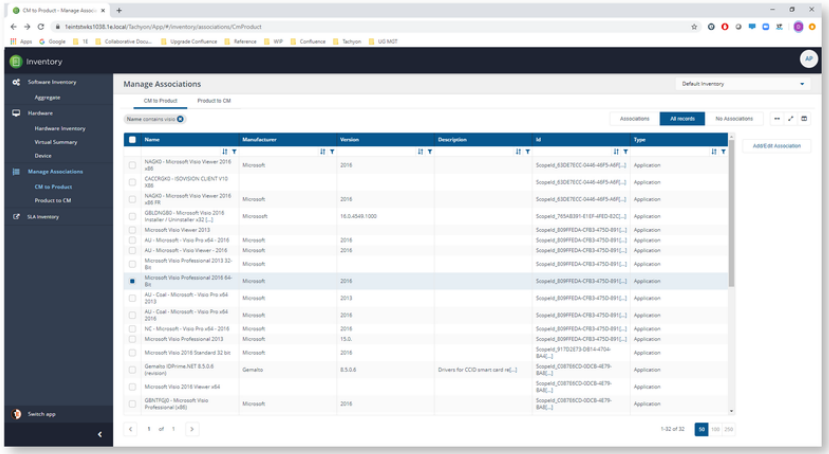


For any Configuration Manager applications/packages, where there are any product associations present, the application/package name in the **Name** column is a link that displays a pop-up that shows the existing association.

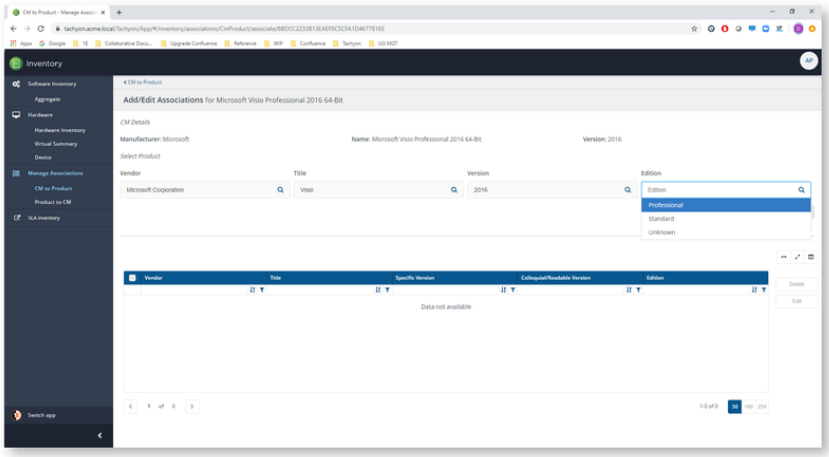


After selecting a single application/package from the table the **Add/Edit Associations** button is enabled. If the application/package already has an association you get to edit the association, if any other application/package is selected you get to create a new association for it.

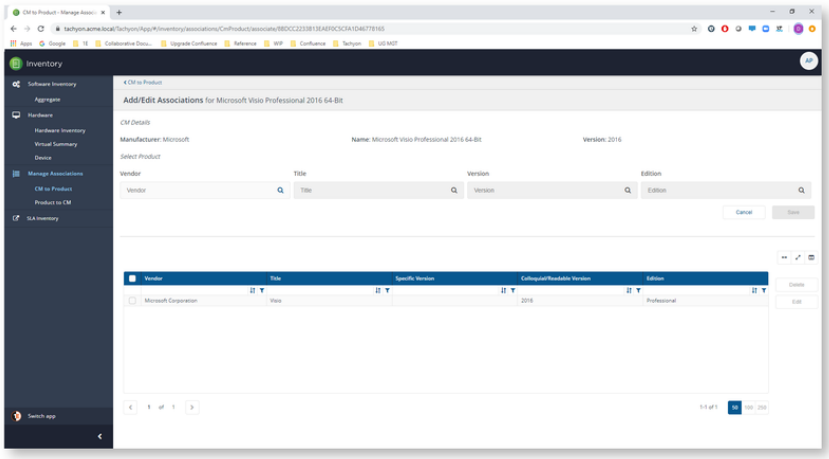
The picture shows an unassociated application/package for Microsoft Visio.



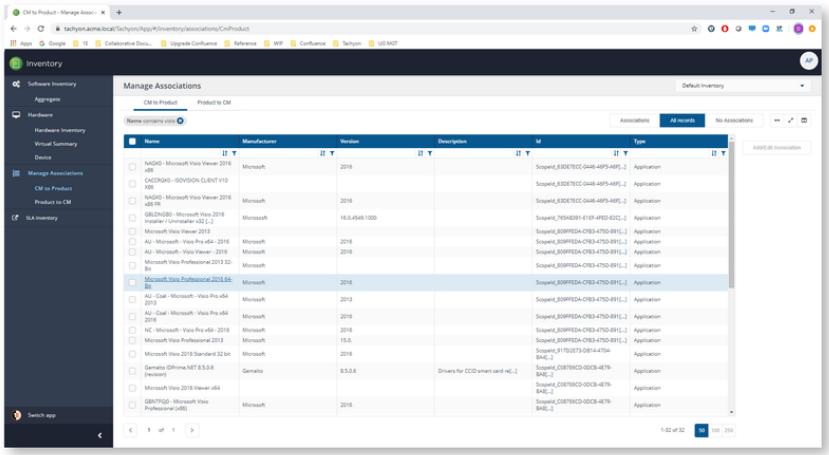
To set a new association you must specify the VTVE in the top **Vendor**, **Title**, **Version** and **Edition** drop downs to search for a product.



After clicking the **Save** button, just below the VTVE fields, the association is saved.



Now when you navigate back to the **CM to Product** screen, the Visio application/package name is a link indicating that it has an association.



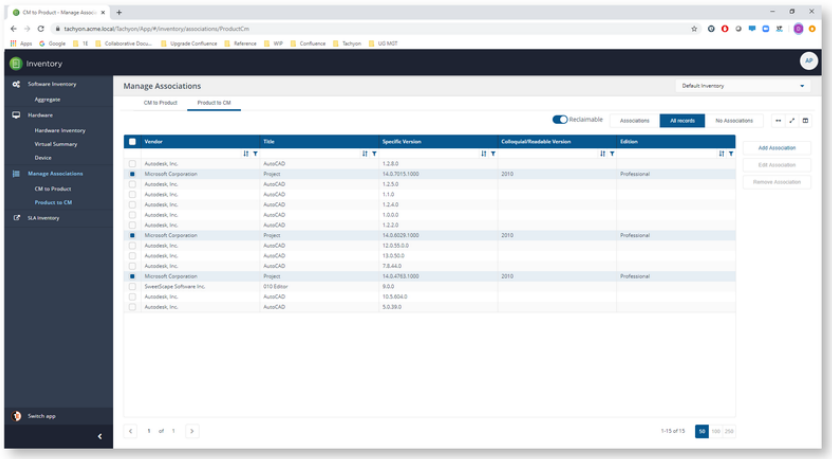
1.8.4.1.2 Associating one or more products (Vendor, Title, Version and Edition) with a Configuration Manager application or package

Navigate to the **Inventory->Manage Associations→Product to CM** page.

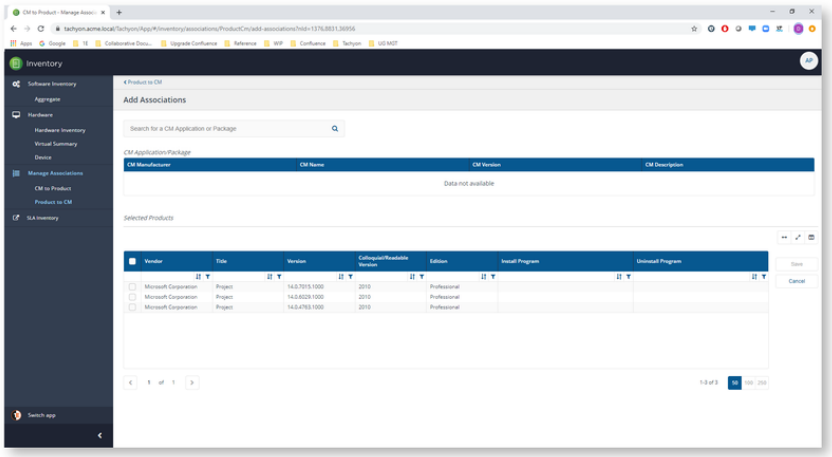
The products which are installed in the selected inventory are listed in the table.

For any product, where there are any associations present, the version number in the **Specific Version** column is a link that displays a pop-up that shows the existing association.

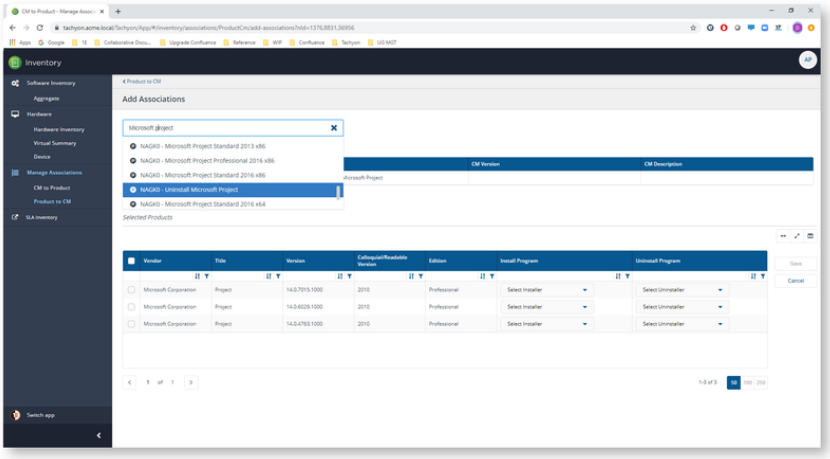
You can set associations for more than one version of a product at a time. The picture shows three versions of the Microsoft Project selected.



Clicking the **Add Association** button displays the **Add Associations** page with the selected products added, as shown in the picture.

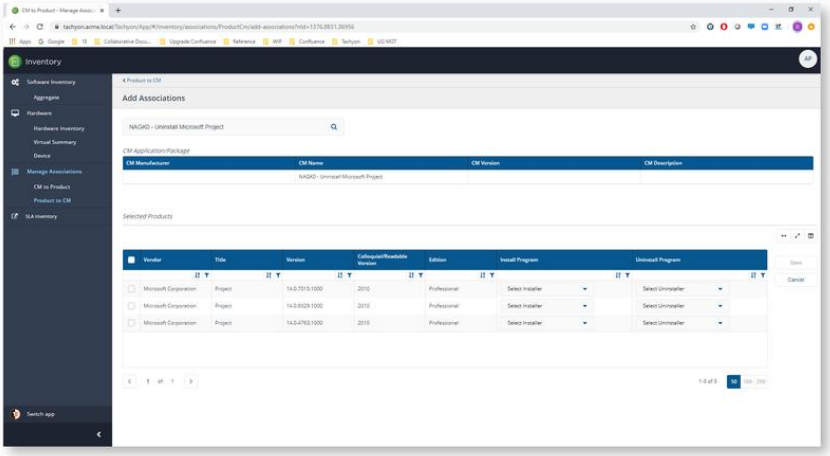


You can search Configuration Manager for a specific application or legacy package by typing into the search field at the top of the page. The picture shows a search for Microsoft Project and the selection of a specific legacy package option called **NAGKO - Uninstall Microsoft Project**.



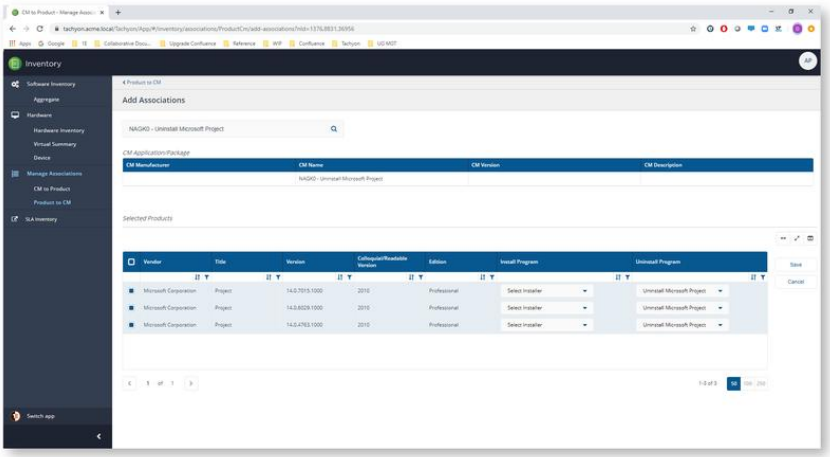
If you select a legacy package the listed selected products change appearance slightly to allow you to select any associated install and uninstall programs, as shown in the picture.

If you select an application there is no option to select the Install/Uninstall Program as that is not necessary for applications.



In our example, we will apply the selected **CM Application/Package** to all the selected products and then set their **Uninstall Program** items to **Uninstall Microsoft Project**, as shown in the picture.

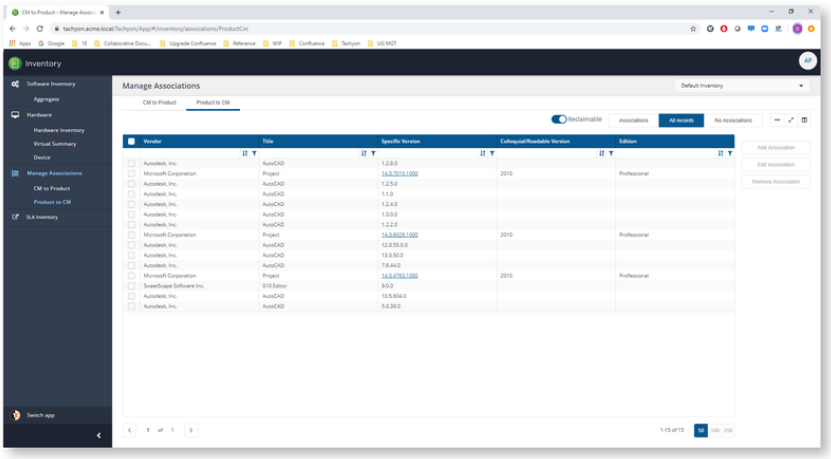
Click the **Save** button to save the associations.



Now when you navigate back to the **Product to CM** page you'll see that your selected products now have associations added. You can see this in the picture where the three Microsoft Project versions now have links.

1.8.4.1.2.1 The Reclaimable toggle

You will also notice that there is a toggle button just above the table on the **Product to CM** tab. When this is turned on the table will be filtered to only display the products that have a reclaim policy associated with them in AppClarity. This can be useful after having defined reclaim policies for installed products in AppClarity to then easily associate them with Configuration Manager applications or programs.



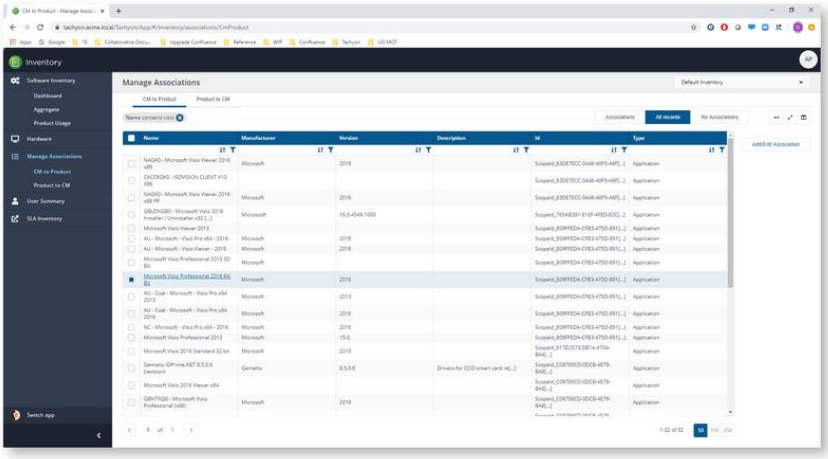
1.8.4.2 Editing associations

The steps for editing associations are different depending on which page the association was created.

1.8.4.2.1 Editing CM to Product associations

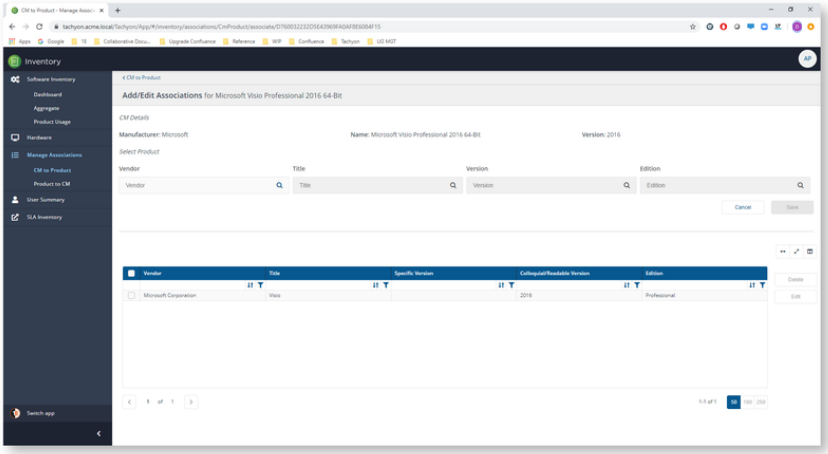
You can edit an existing CM to Product association by selecting it from the **CM to Product** associations list and then clicking on the **Add/Edit Association** button. The picture shows the previously created Microsoft Visio association selected.

> **Note**
>
> You can only select one association to edit at a time. If you make multiple selections the **Add/Edit Association** button will be disabled.



On the **Add/Edit Associations** page subsequently displayed you can save new associations in the top part of the page and edit or delete existing ones on the lower part. The picture shows the previously added Microsoft Visio association being edited.

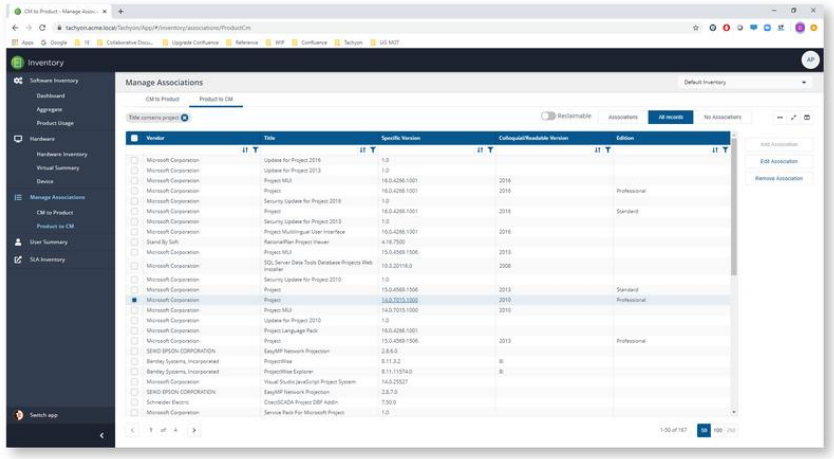
Modifications are stored whenever you click on **Save** or **Delete**. Once you've finished making the changes you need you can navigate back to the main **CM to Product** page by clicking on the **< CM to Product** link at the top of the page or using the navigation tree on the left.



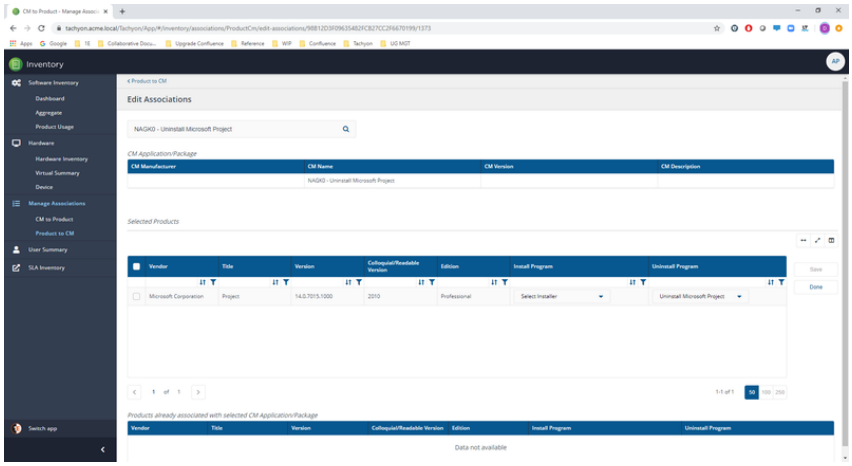
1.8.4.2.2 Editing Product to CM associations

You can edit an existing CM to Product association by selecting it from the **Product to CM** associations list and then clicking on the **Edit Association** button. The picture shows one of the previously created Microsoft Project associations selected.

> **Note**
>
> You can only select one association to edit at a time. If you make multiple selections the **Edit Association** button will be disabled.

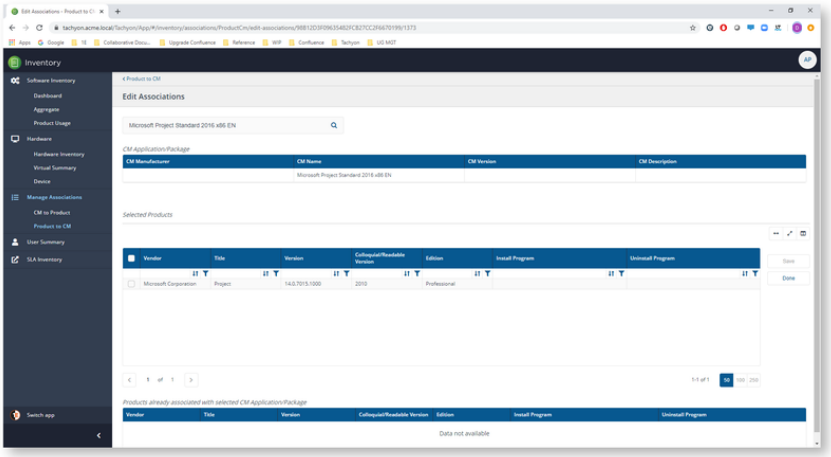


On the **Edit Associations** page subsequently displayed you can select a new Configuration Manager application or legacy package in the top part of the page and edit the specific product association on the lower part, including setting the **Install Program** and **Uninstall Program** for legacy packages. The picture shows the previously added Microsoft Project association being edited.



To select another Configuration Manager application or legacy package you search for it using the search field at the top of the page, in the same way as you would if you were creating a completely new product for CM association. In the picture we've changed the original **NAGK0 - Uninstall Microsoft Project** CM legacy package to the **Microsoft Project Standard 2016 x86 EN** application.

Once you've made this change you'll need to select the product in the **Selected Products** list and then click on **Save** to commit any changes made to the listed product.



Click **Done** to close the **Edit Associations** page without saving, a notification popup will be displayed. You can also navigate back to the main **Product to CM** page by clicking on the **< Product to CM** link at the top of the page or using the navigation tree on the left.

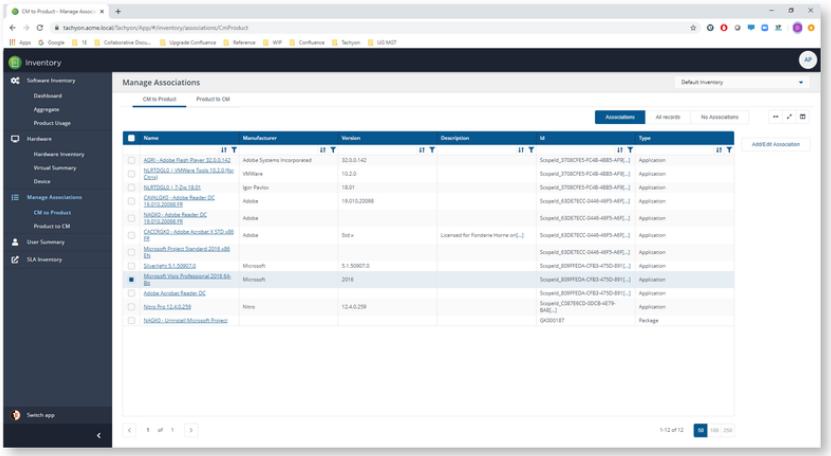
1.8.4.3 Deleting associations

The steps for deleting associations are different depending on which page the association was created.

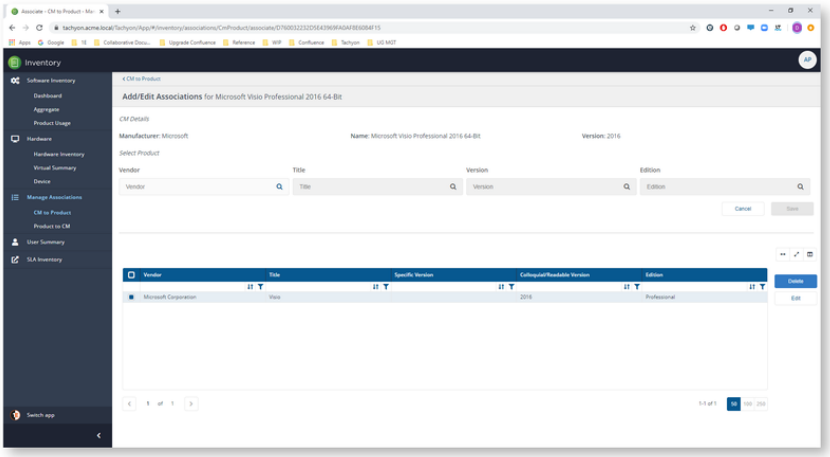
1.8.4.3.1 Deleting CM to Product associations

You delete a **CM to Product** association by deleting all the product associations it holds. This is done via the **Add/Edit Associations** page. First, select the association you want to delete from the **CM to Product** associations list and then click on the **Add/Edit Association** button. The picture shows the previously created Microsoft Visio association selected.

> **Note**
>
> You can only select one association to edit at a time. If you make multiple selections the **Add/Edit Association** button will be disabled.

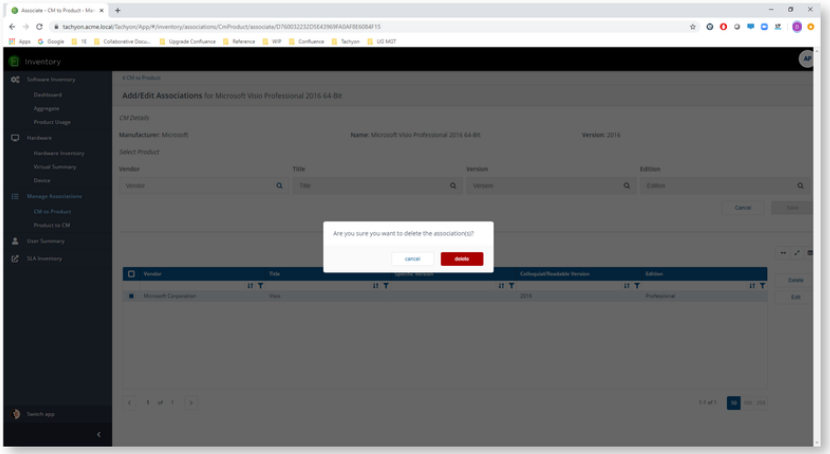


When the **Add/Edit Associations** page is displayed select all the associations by clicking on the selection field at the left-hand end of the products table. Then click on the **Delete** button, as shown in the picture.



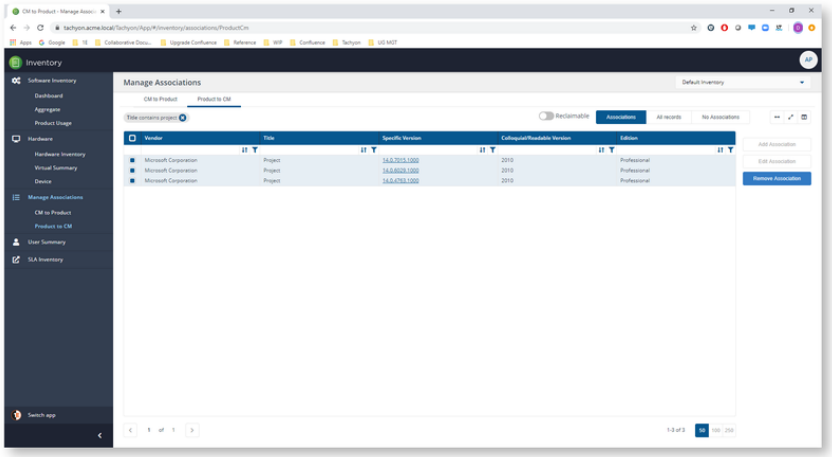
A popup will be displayed asking whether you want to delete the association(s). Click on **delete** to remove all the products from the association.

Subsequently, when you navigate back to the **CM to Product** page you will see that the association has been deleted as a result of all the products having been deleted from the association.

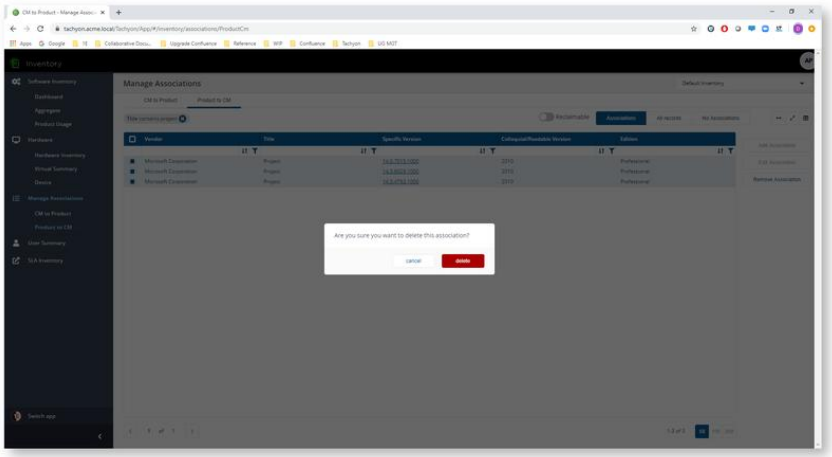


1.8.4.3.2 Removing Product to CM associations

You can remove one or more **Product to CM** associations in a single operation on the **Product to CM** page. To do this you select all the associations you want to remove and then click on the **Remove Association** button. The picture shows the Microsoft Project associations selected that we created earlier, with the **Remove Association** button highlighted.



Clicking on the button displays a notification popup asking if you want to continue with the process of removing the selected associations, as shown in the picture. Click **delete** to continue and remove all the selected associations. At this point, the associations will be removed and no longer appear in the console.



1.8.5 User Summary

User Summary shows data captured from sources such as Configuration Manager, Big Fix, and vCenter if you have them configured.

The dashboard is refreshed (recalculated) when the page is opened or the page is refreshed in the browser.

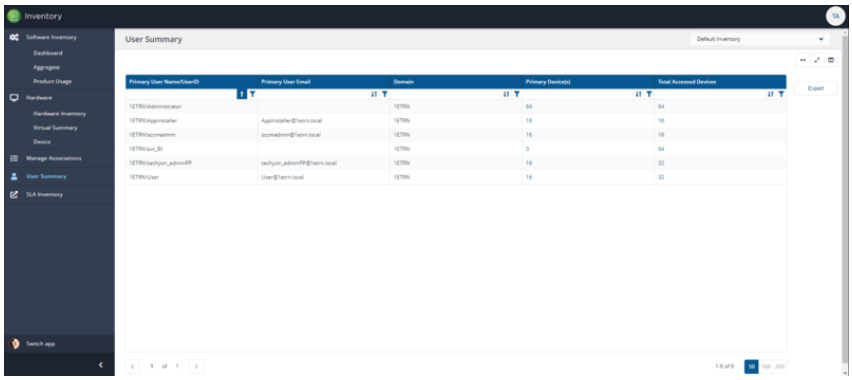
The User Summary page shows a list of active users gathered using the Configuration Manager software inventory.

In the top right of the page in line with the screen title, there is a dropdown showing **Default Inventory**. If you have configured more than one Inventory they will be available to choose from here.

You can also customize which fields are displayed on the page by using the **Choose Columns** control.

> **Note**
>
> You can choose which columns are displayed in some detail tables to increase readability. On pages where you can pick the displayed columns you'll see a new control like the one below:

To find out more about this feature refer to Choosing the columns displayed in reports.

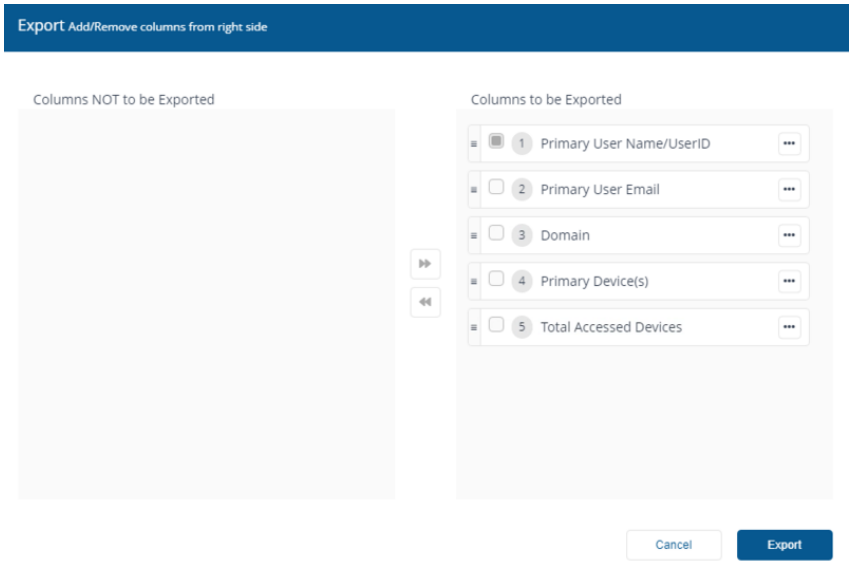


1.8.5.1 Export

You can use the **Export** button to export currently displayed data in a downloadable report.

When you click on the **Export** button, you'll see the **Export** popup. You can choose which columns to export in the same way you can choose columns to display in the main report panel.

The report is exported in a .TSV format, for example, **InventoryProductUsage_20200813120506.tsv**. The file is exported and downloaded to the default location for the browser you are using.



1.8.6 The 1E Catalog

An introduction to 1E Catalog and how to access and use the feature.

1E Catalog provides the following capabilities within the Inventory and other applications:

- Have a consistent view of your estate
- Uniquely identify software products deployed in your estate

- Identify device types (laptop, desktop, virtual machine), operating system, device family, device manufacturer, and maximum number of processors
- Normalize processor information like processor model, processor family, vendor name, and number of cores of processors running on your devices
- Define and apply bundling rules to identify suites and their components
- Define and apply entitlement rights, such as version upgrade/downgrade, edition downgrade, and software assurance rights which are used during license demand and compliance calculations
- Apply autofill entitlement information using software SKU.

1E Catalog and SLA are components of the Inventory application. Other applications such as AppClarity access it directly and many Catalog related operations are carried out within these companion applications and features. Therefore you will rarely need to directly access the Catalog UI, but it can be used for the following:

- Managing software products
- Adding a new version
- Managing match rules - so the Catalog can link and normalize inventory products.

1.8.6.1 Connecting to the CatalogWeb UI

Note

The Catalog UI can be reached directly using the following URL:

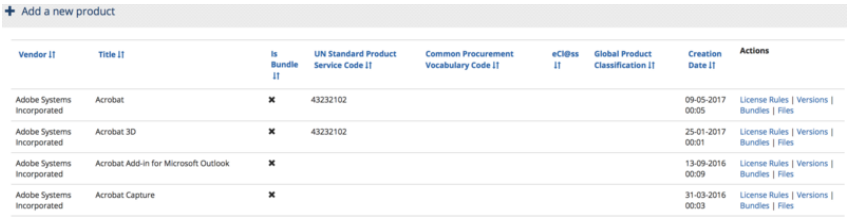
```
https://<tachyon DNS Name FQDN>/CatalogWeb
```

where <tachyon DNS Name FQDN> is the one set up during the preparation phase, as described under the heading DNS Names.

1.8.6.2 Software Products page

When you access the Catalog UI, the first page displays a list of software products in the Catalog.

The top right of the screen shows navigation elements for each section of the UI:

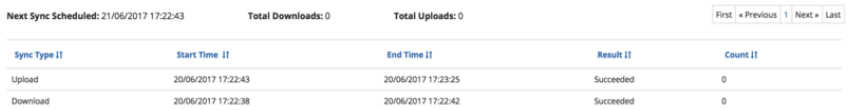


1.8.6.2.1 Admin

Allows you to manage who runs resynchronization events to refresh Catalog data. Only users with admin privileges see this tab.

1.8.6.2.2 Updates

Provides the status for catalog updates - only if you subscribe to the service.



Next Sync Scheduled: 21/06/2017 17:22:43 **Total Downloads:** 0 **Total Uploads:** 0

First « Previous 1 Next » Last

Sync Type	Start Time	End Time	Result	Count
Upload	20/06/2017 17:22:43	20/06/2017 17:23:25	Succeeded	0
Download	20/06/2017 17:22:38	20/06/2017 17:22:42	Succeeded	0

1.8.6.2.3 Products

The software products screen, which is also the Catalog landing page where you can perform tasks like:

- Managing software products
- Adding a new version
- Managing bundles
- Adding a fileset
- Managing license rules.

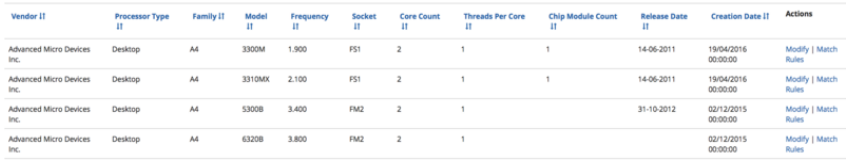
1.8.6.2.4 Devices

List of Catalog devices - click **Managing match rules** to update details of a device or Match Rules to edit an existing rule or associate a new rule with it.

Vendor	Device Type	Family	Model	Max Socket Count	Release Date	Creation Date	Actions
1E652	Motherboard		A30	1		21/04/2016 00:00:00	Modify | Match Rules
AAEON	Motherboard		FSB-B75H	1		21/04/2016 00:00:00	Modify | Match Rules
Acer Inc.	Notebook	Aspire	E1-532	2	01-10-2013	13/04/2016 00:00:00	Modify | Match Rules
Acer Inc.	Desktop	Veriton	M410	1		18/08/2015 00:00:00	Modify | Match Rules
Acer Inc.	Desktop	AspireRevo	R3610	1		18/08/2015 00:00:00	Modify | Match Rules

1.8.6.2.5 Processors

List of Catalog processors - click **Modify** to update the details of a processor or Managing match rules to edit an existing rule or associate a new rule with it



Vendor	Processor Type	Family	Model	Frequency	Socket	Core Count	Threads Per Core	Chip Module Count	Release Date	Creation Date	Actions
Advanced Micro Devices Inc.	Desktop	A4	3300M	1.900	FS1	2	1	1	14-06-2011	19/04/2016 00:00:00	Modify | Match Rules
Advanced Micro Devices Inc.	Desktop	A4	3310MX	2.100	FS1	2	1	1	14-06-2011	19/04/2016 00:00:00	Modify | Match Rules
Advanced Micro Devices Inc.	Desktop	A4	5300B	3.400	FM2	2	1		31-10-2012	02/12/2015 00:00:00	Modify | Match Rules
Advanced Micro Devices Inc.	Desktop	A4	6320B	3.800	FM2	2	1			02/12/2015 00:00:00	Modify | Match Rules

1.8.6.2.6 Vendors

List of software publishers in the Catalog

Vendor	Short Name	Creation Date	Actions
Adobe Systems Incorporated	Adobe	02/12/2015 00:00:00	Aliases
Adolfo Marinucci		31/03/2016 00:00:00	Aliases
Adolix		31/03/2016 00:00:00	Aliases

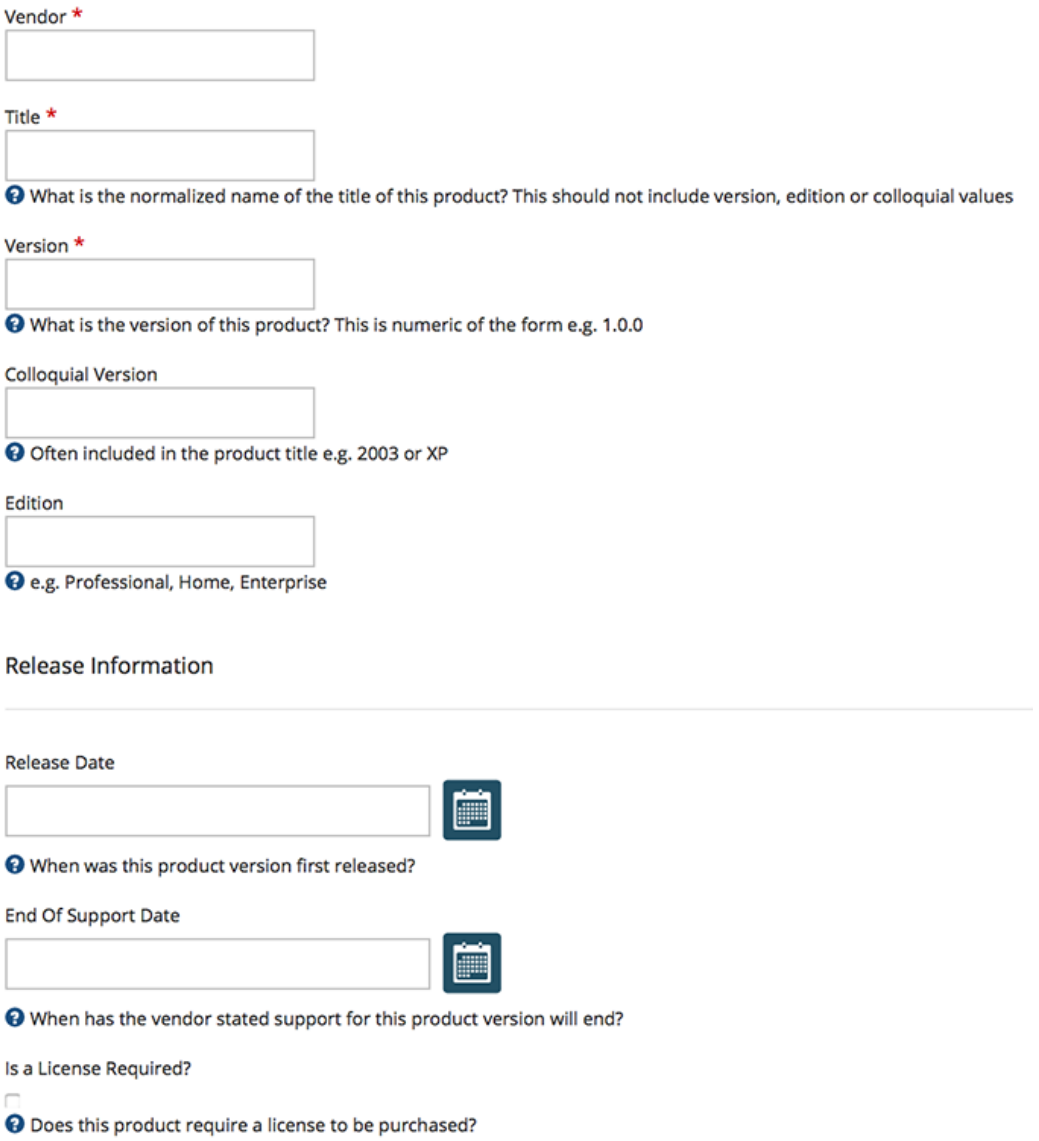
1.8.6.2.7 Glossary

List of terms used in the Catalog UI

1.8.6.3 Managing software products

To add a new software product:

1. Click the **Add a new product** link.
2. On the Product Information page, complete the following mandatory fields:



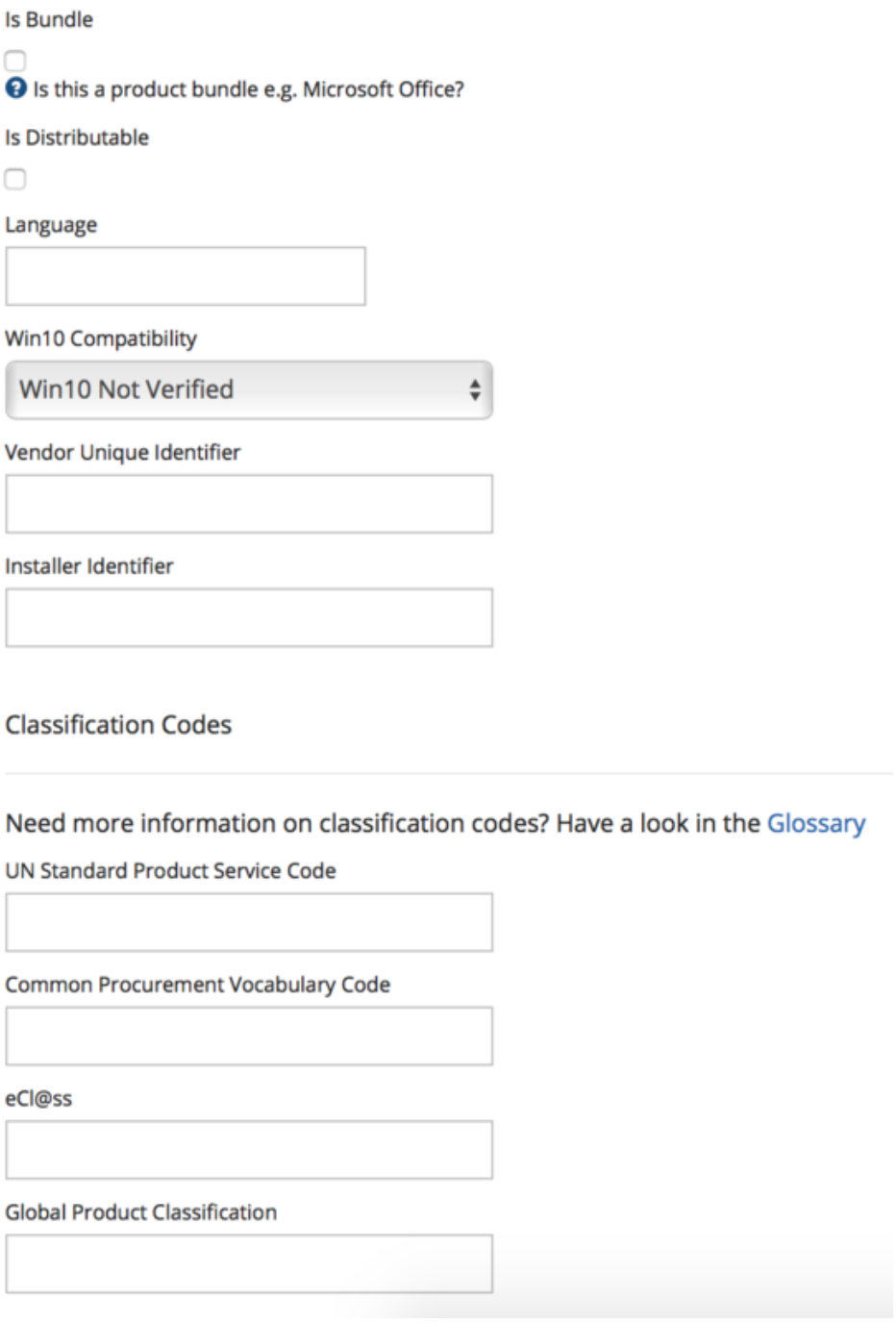
   - Vendor
   - Title
   - Version

   And optionally:

   - Colloquial Version

- Edition
- Release Date
- End of Support Date
- Is a License Required?

3. Click **Save**.
4. To provide more information about the new product, click the **Additional details** tab and complete these fields or tick the checkboxes as necessary:



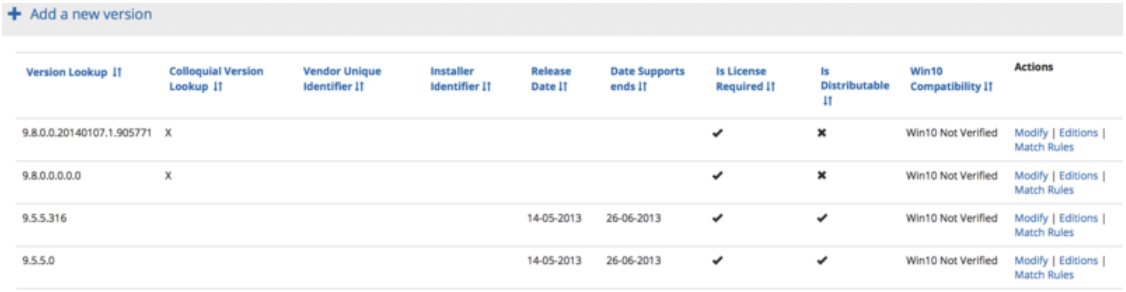
- Is Bundle
- Is Distributable - is this software title distributed separately?
- Language
- Windows 10 Compatibility
- Vendor Unique Number
- Installer Identifier

- UN Standard Product Service Code
- Common Procurement Vocabulary Code
- eCl@ss
- Global Product Classification.

5. Click **Save**.

1.8.6.4 Managing versions

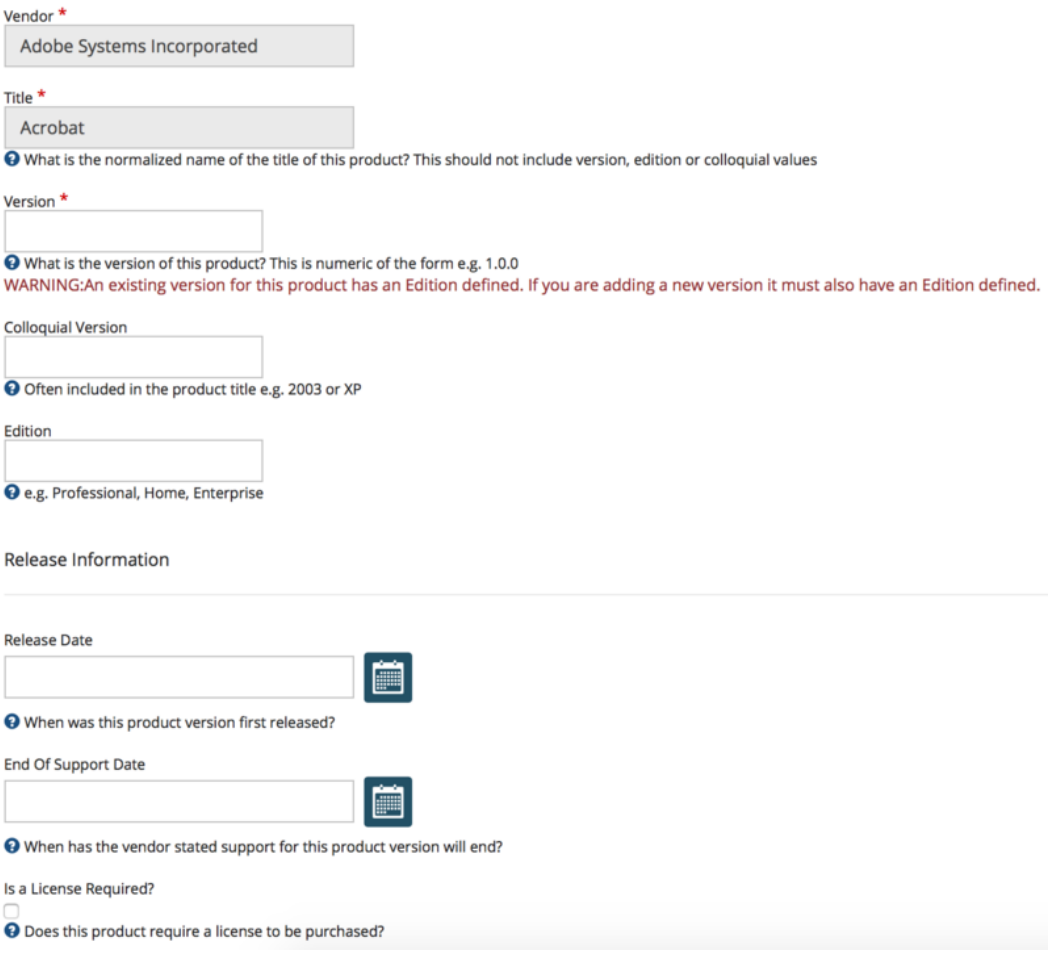
To view a software product's versions, click the **Version** link to the right of the product screen to show a list of versions for that product, refer to Using filters.



1.8.6.4.1 Adding a new version

To add a new version:

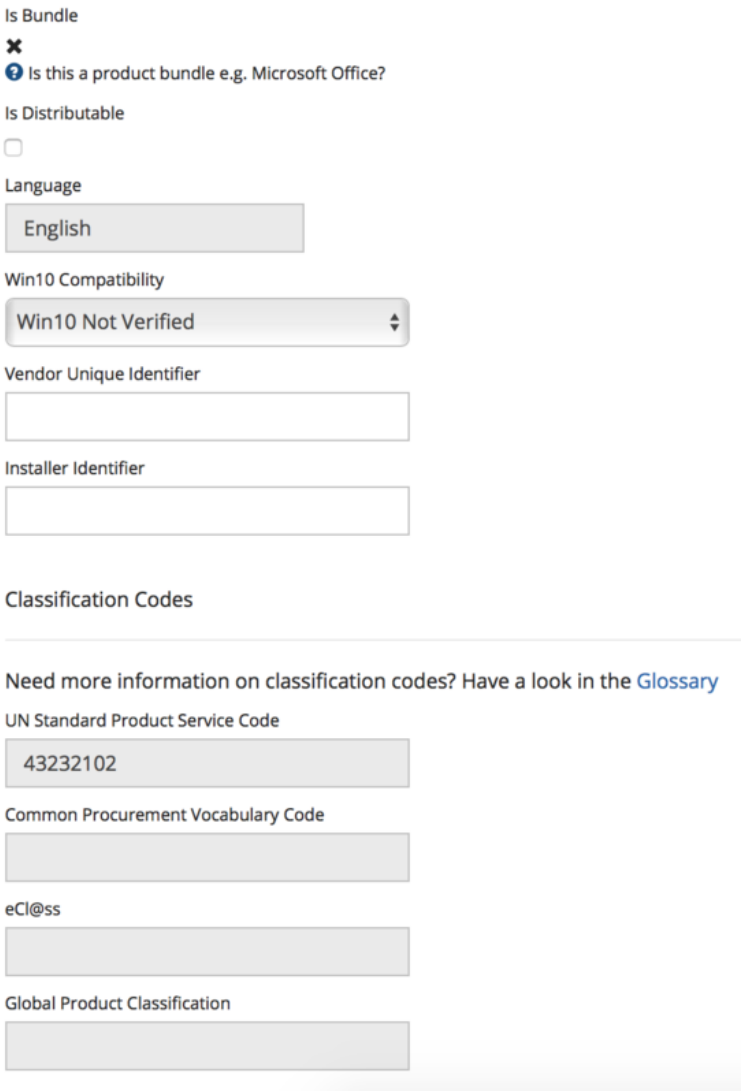
1. Click the **Add a new version** link at the top of the screen - Adobe Acrobat in this example.
2. On the **Product details** tab for Adobe Acrobat, complete the **Version** field.



And optionally:

- Colloquial Version
- Edition
- Release Date
- End of Support date
- Is a License Required?

3. Click **Save**.
4. To provide additional information associated with this particular version, click the **Additional details** tab and complete the fields or tick the checkboxes as necessary:



- Is Distributable?
- Vendor Unique Identifier
- Installer identifier.

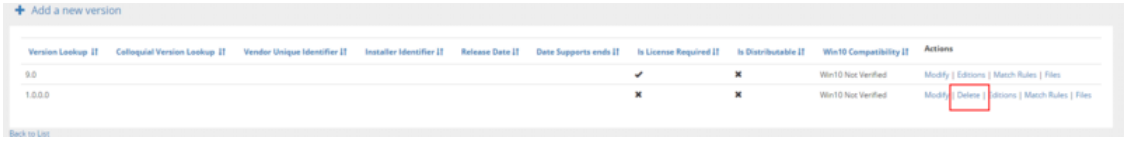
5. Click **Save**.

1.8.6.5 Deleting an existing product version or edition

You can only delete products, versions, or editions you created. New product items added by the 1E curation team are marked as 1E Verified and cannot be deleted.

To delete an existing product version or edition:

1. On the **Version** screen find the item in the list.

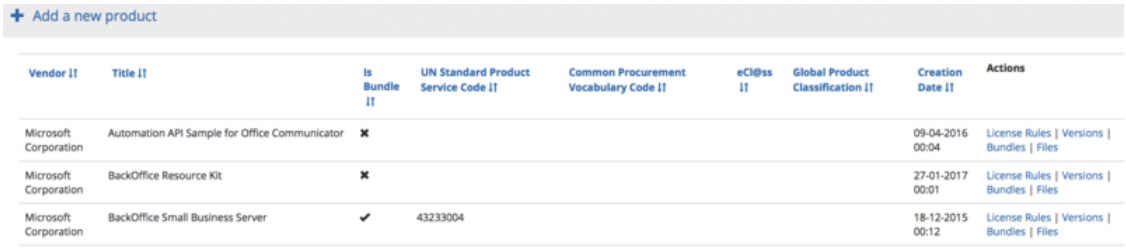


2. Under the **Actions** column, click **Delete**.

1.8.6.6 Managing bundles

Bundles are a collection of products and the 1E Catalog already contains all the bundles you should need. In the event you need to create a bundle:

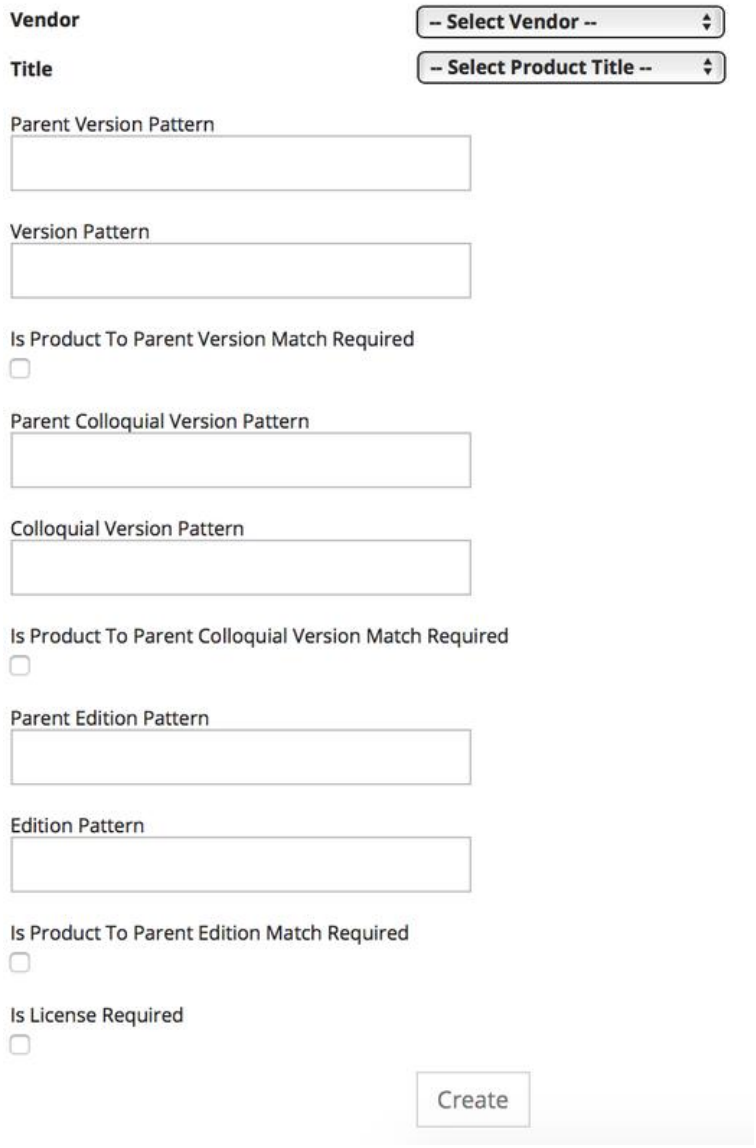
1. On the **Products** screen, find the item from the list, for example, Microsoft BackOffice Small Business Server.



2. Under the **Actions** column, click **Bundles**.

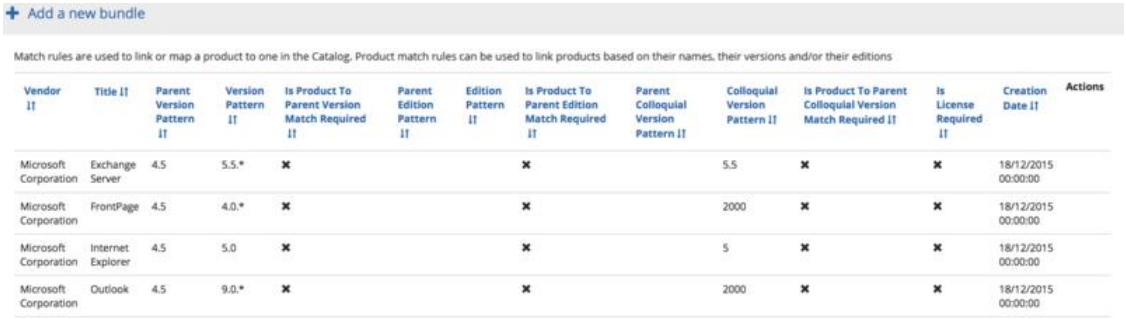
3. Click **Add a new bundle**.

4. On the **Bundles** screen:



- In **Vendor**, click the list and choose a vendor for this bundle. The title list displays after you pick a vendor - the image displays both the Vendor and Title pick lists
- In Title, click the list and choose a product title for this bundle
- Complete the remaining fields as necessary.

5. Click **Create**.



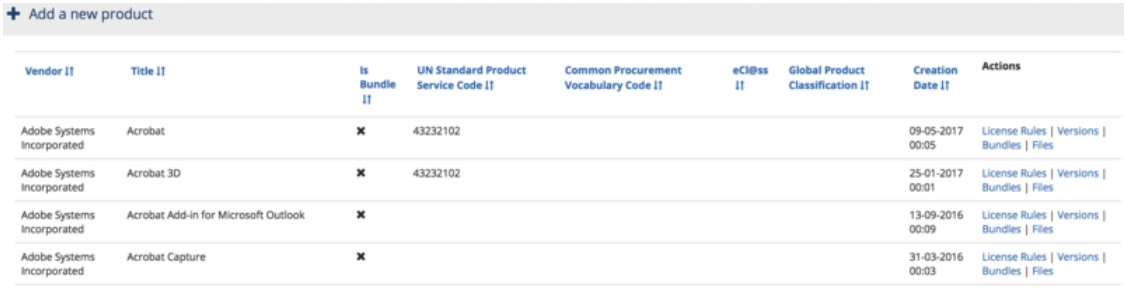
1.8.6.7 Managing filesets

Filesets define which files are used by a particular product. AppClarity consumer uses filesets to determine its usage, it does this by looking at the last run dates for that filename.

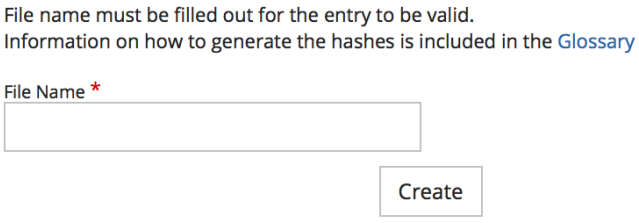
1.8.6.7.1 Adding a fileset

To add a fileset:

1. On the **Product** screen, find the item you want to add files to.
2. Under **Actions** click on Files.



3. On the **Product Files** screen, click **Add a new Product File**.
4. On the **Product File** screen, enter the filename:



Note

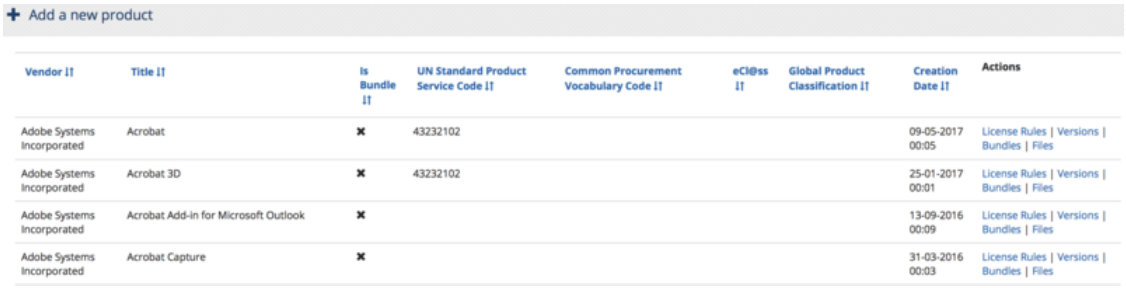
From 1E Catalog 2.0 and later products can be associated with more than one executable, before this version products were restricted to a single executable.

5. Click **Create**.

1.8.6.7.2 Modifying an existing fileset

To modify an existing fileset:

1. On the **Product** screen, find the item you want to modify.



2. Under the **Actions** column, click **Files**.
3. From the list of files, locate the one you want and click **Edit**.

4. In the **Product File** screen, update its filename
5. Click **Save**.

1.8.6.7.3 Deleting an existing fileset

To delete an existing fileset:

1. Repeat steps 1 and 2 above.
2. From the list of files, locate the one you want and click **Delete**.
3. You will be prompted to confirm your actions.

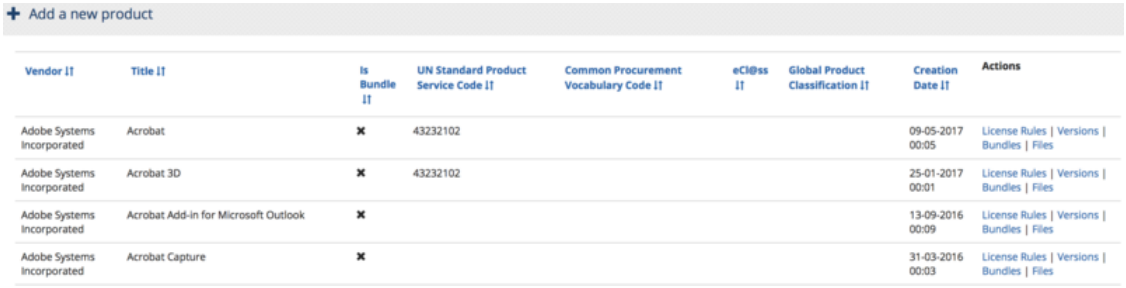
4. Click **Delete** to remove the file or **Back to List** to cancel the action.

1.8.6.8 Managing license rules

Licensing rules define how a product or a specific version of a product is licensed, for example, what metric they use or the average price of the license. You can set up different license rules for specific versions by using version patterns, for example, 10.*.* has license metric = Device; 11.* is licensed by User.

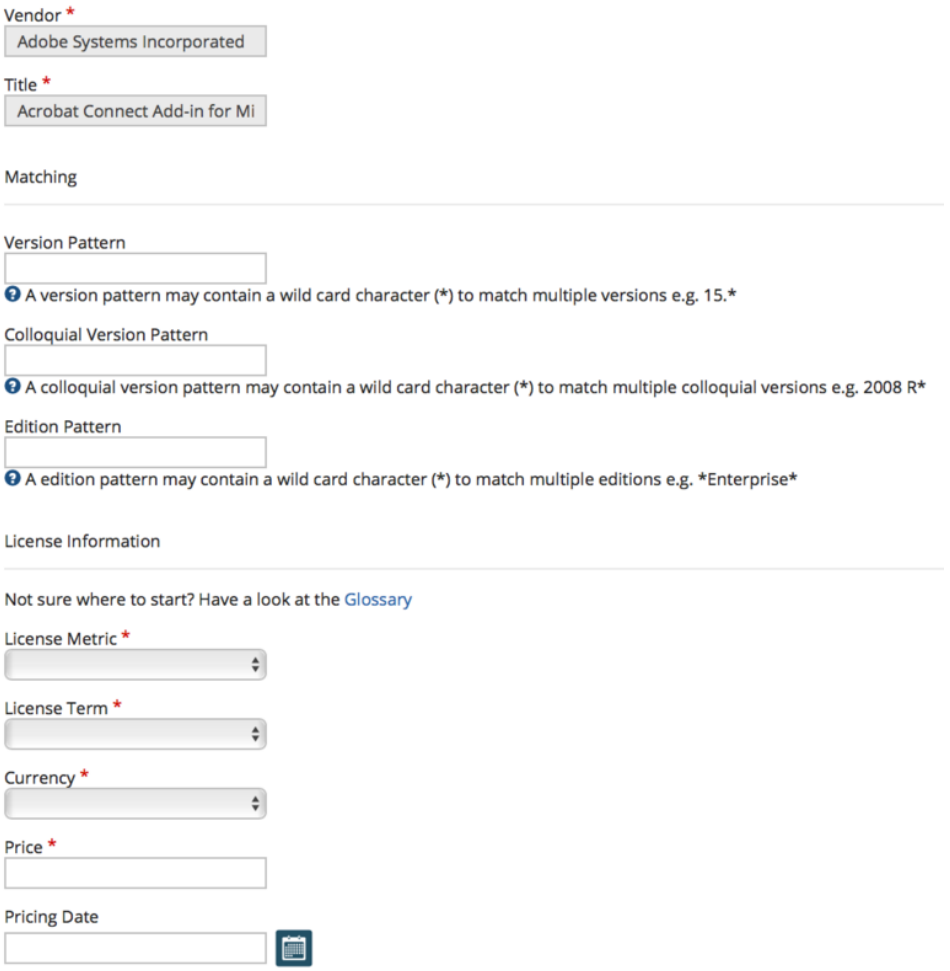
To add a licensing rule:

1. On the **Product** screen, locate the item you want to associate a licensing rule with.
2. Under the **Actions** column for that product, click **License Rules**.



3. Click **Add a new license rule**.

4. In the **Product Information** screen:



a. In the **Matching** section, populate the pattern fields if you are using patterns - you can use the wildcard (*) in the pattern.

b. In the **License information** section for these mandatory fields:

- **License Metric** - click the list and choose one
- **License Term** - click the list and choose from device, non-perpetual, perpetual or subscription
- **Currency** - click the list and choose one
- **Price** - enter the unit price for it

Optionally:

- **Pricing Date**.

5. Click **Save**.

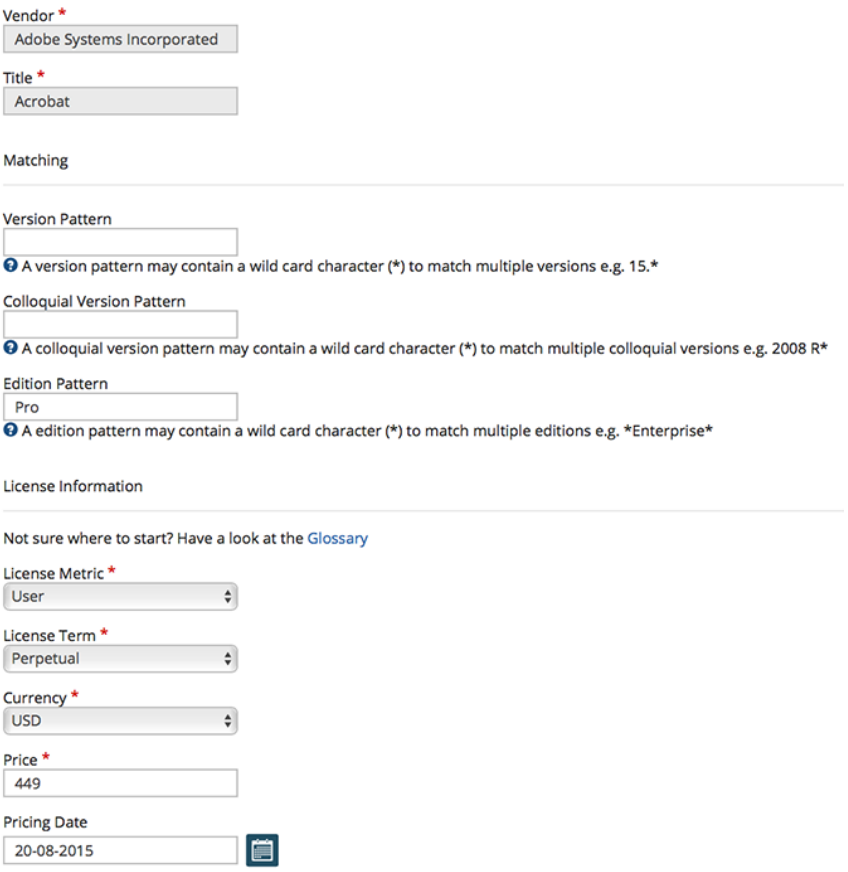
1.8.6.8.1 Updating an existing license rule

You can modify or delete an existing Licensing Rule associated with a product, for example the licensing rules for Adobe Acrobat.

Version Pattern	Colloquial Version Pattern	Edition Pattern	License Metric	License Term	Currency	Price	Pricing Date	Actions
		Pro Extended	User	Perpetual	USD	$ 699	20-08-2015	Modify | Delete
		Standard	User	Perpetual	USD	$ 299	20-08-2015	Modify | Delete
		Pro	User	Perpetual	USD	$ 449	20-08-2015	Modify | Delete

To modify an existing license rule:

1. Locate the item from the list and under the **Actions** column, click **Modify**.
2. In the **Product Information** screen, update the fields as necessary.



3. Click **Save**.

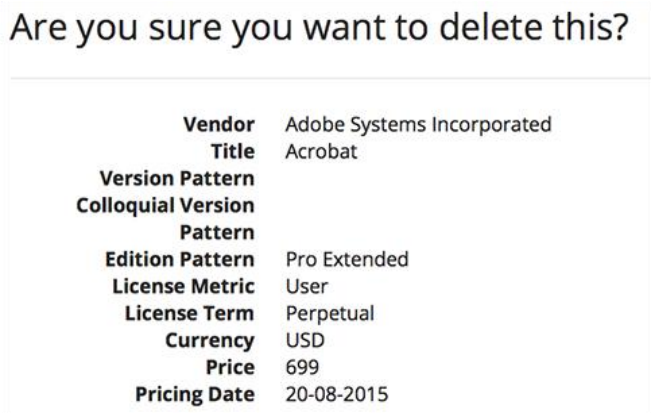
1.8.6.8.2 Deleting an existing license rule

To delete an existing license rule:

1. Locate the item from the list and under the **Actions** column, click **Delete**.

Version Pattern	Colloquial Version Pattern	Edition Pattern	License Metric	License Term	Currency	Price	Pricing Date	Actions
		Pro Extended	User	Perpetual	USD	$ 699	20-08-2015	Modify | Delete
		Standard	User	Perpetual	USD	$ 299	20-08-2015	Modify | Delete
		Pro	User	Perpetual	USD	$ 449	20-08-2015	Modify | Delete

2. You will be prompted to confirm your actions.

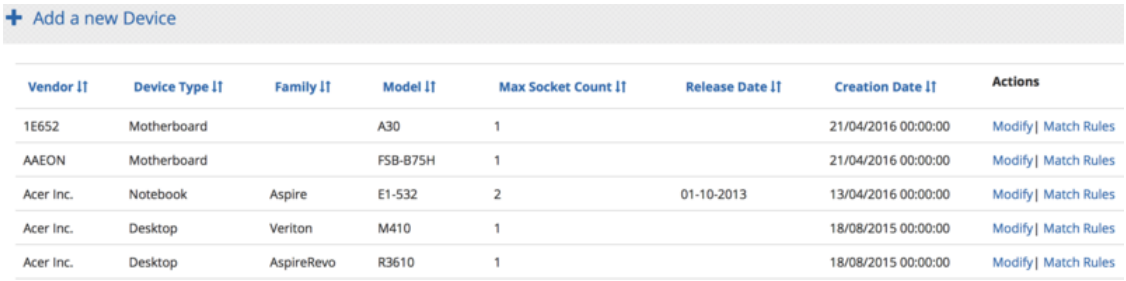


3. Click **Delete** to remove the rule for that product or click **Back to List** to cancel the action.

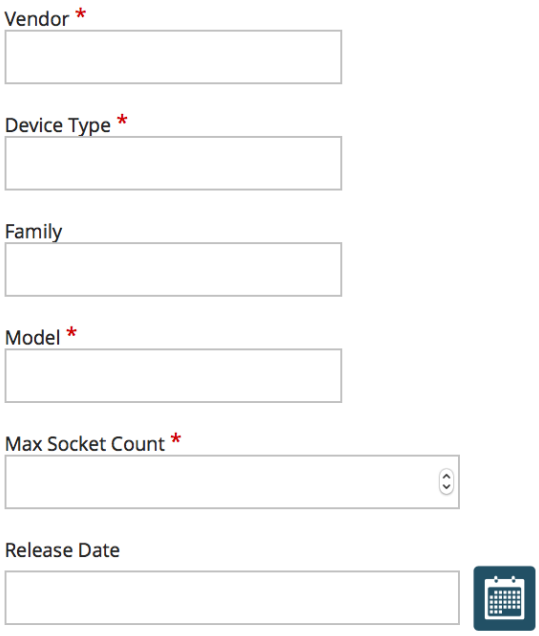
1.8.6.9 Managing devices

To add a new device:

1. Click the **Devices** link - top right of the screen.
2. On the **Devices** screen, click **Add new Device**.



3. On the **Add a new Device** screen - fields marked with a red asterisk are mandatory:



- **Vendor** - enter the name of the vendor
- **Device Type** - enter the type of device, for example, motherboard, laptop, notebook, desktop, server, or blade server
- **Family** - enter the family of the device such as EliteBook, HP Omni, Pavilion, Pro, TouchSmart
- **Model** - enter the model number of the device
- **Max Socket Count** - enter the socket count for the device
- **Release Date** - click the calendar icon and choose a date.

4. Click **Save**.

1.8.6.10 Managing processors

Note

From 1E Catalog 1.2.100 and later Processor identification and normalization has greater accuracy and coverage.

To achieve this we removed the current dependency on Processor frequency during normalization. We did this because processors can run at a variety of speeds, so using the processor frequency for normalization does not help to identify processor type. For example, you could have up to 10 different speeds for a single processor because an OS typically reports the speed of a processor as it's currently running.

Now, one of the following criteria has to match during normalization:

- SourceFamily and SourceModel
- SourceName.

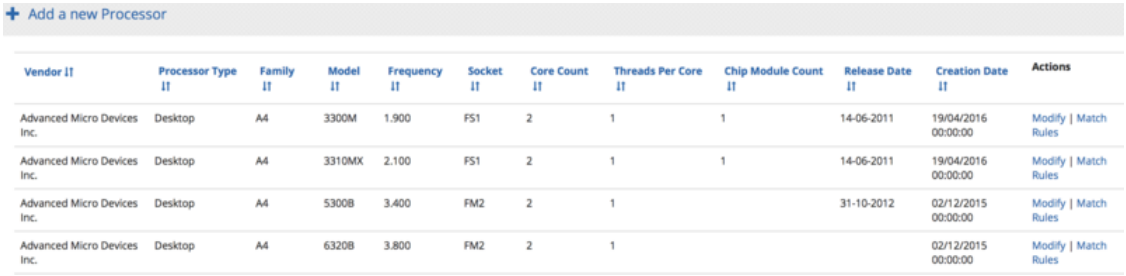
This change makes finding matches more successful because there's no need to evaluate every source field.

In the following example, the two source entries will be matched to the same processor because the SourceName values are the same:

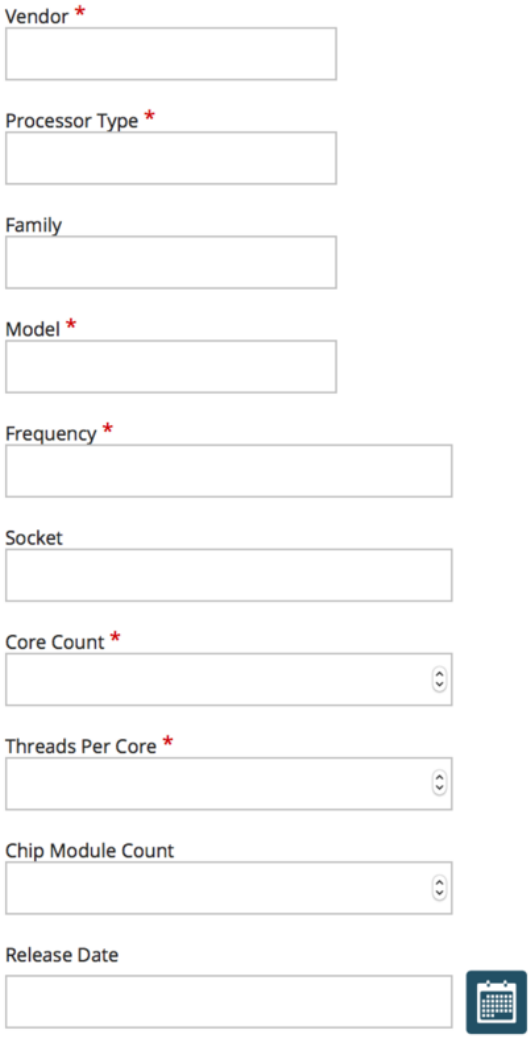
SourceVendor	SourceFamily	SourceName	SourceModel	SourceFrequency	SourceSocket
GenuineIntel	Intel Xeon	Intel(R) Xeon(R) CPU E5-2637 v4 @ 3.50GHz	NULL	3500	NULL
GenuineIntel	NULL	Intel(R) Xeon(R) CPU E5-2637 v4 @ 3.50GHz	NULL	NULL	NULL

To manage processors:

1. Click the **Processors** link - top right of the screen.
2. On the **Processor** screen, click **Add new processor**.



3. On the **Add a new Processor** screen - fields marked with a red asterisk are mandatory:



- **Vendor** - enter the name of the vendor
- **Processor Type** - enter the type of processor such as desktop, server

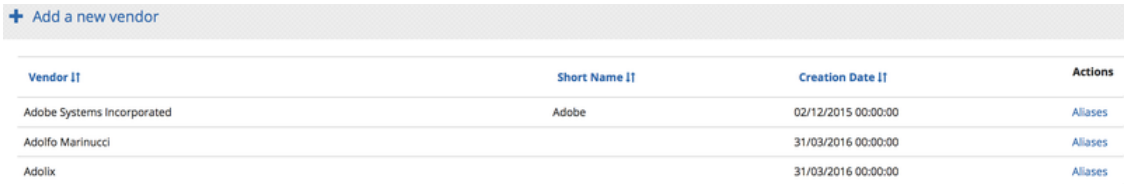
- **Family** - enter the family for the processor such as A4, Athlon XP, Atom, Corei5, Corei7, Pentium, Xeon
- **Model** - enter the model of the processor such as 260M, T2500, Z670
- **Frequency** - enter the processor frequency in GHz such as 0.600, 2.500
- **Socket** - enter the model of the socket supported by the processor such as FM1, FCBGA676
- **Core Count** - enter the number of cores for the processor such as 1, 2, 4, 8
- **Threads Per Core** - enter the threads for the processor core such as 1, 2
- **Chip Module Count** - enter the count for it such as 1
- **Release Date** - click the date icon and choose a date.

4. Click **Save**.

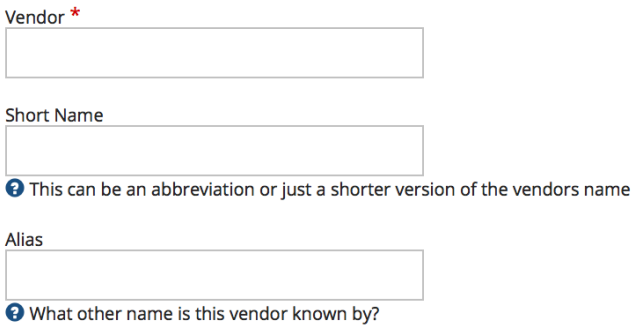
1.8.6.11 Managing vendors

To add a new vendor:

1. Click the **Vendors** link - top right of the screen.
2. On **Vendors** screen, click **Add new vendor**



3. On the **Add a new vendor screen**:



- **Vendor** - enter the name of the vendor - a mandatory field.
- **Short Name** - enter a short name for the vendor.
- **Alias** - enter an alias if there is one.

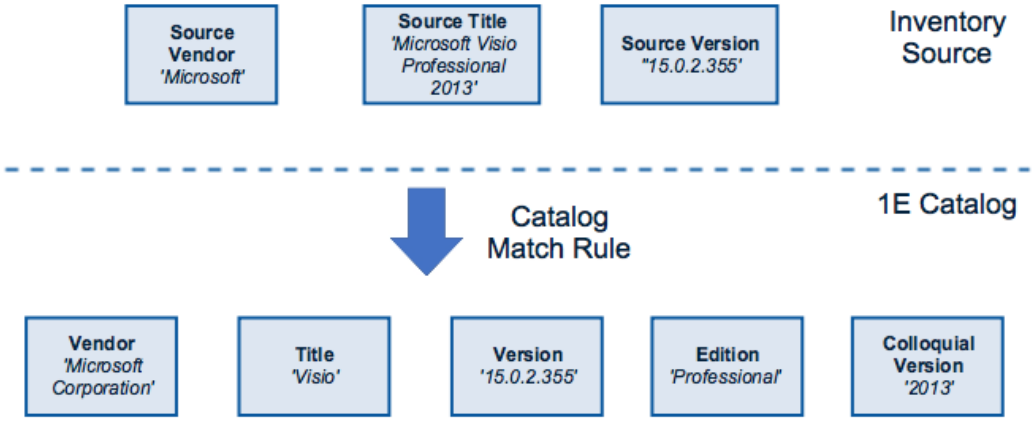
4. Click **Save**.

1.8.6.12 Managing match rules

Match rules are the method used to link source inventory to catalog entries. Match rules can be assigned to a specific:

- Version of a product - typically used if the product is not an edition-based product
- Edition of a version of a product - typically used if the product is an edition-based product.

For example, the inventory source holds the following information about a software title:



- Source Vendor = Microsoft
- Source Title = Microsoft Visio Professional 2013
- Source Version = 15.0.2.355

However, the corresponding entry in the Catalog has a different vendor and title resulting in a mismatch. To resolve this, the Catalog contains rules which directly match these types of entries. In this example, the product is edition-based (Visio) so the Catalog match rule is an edition match rule – linking the source to a specific edition of a specific version (15.0.2.355) of this title.

- Vendor Microsoft resolves to Microsoft Corporation
- The Microsoft Visio Professional 2013 title resolves to:
  - Title = Visio
  - Edition = Professional
  - Colloquial Edition = 2013
- Version 15.0.2.355 maps directly to 15.0.2.355

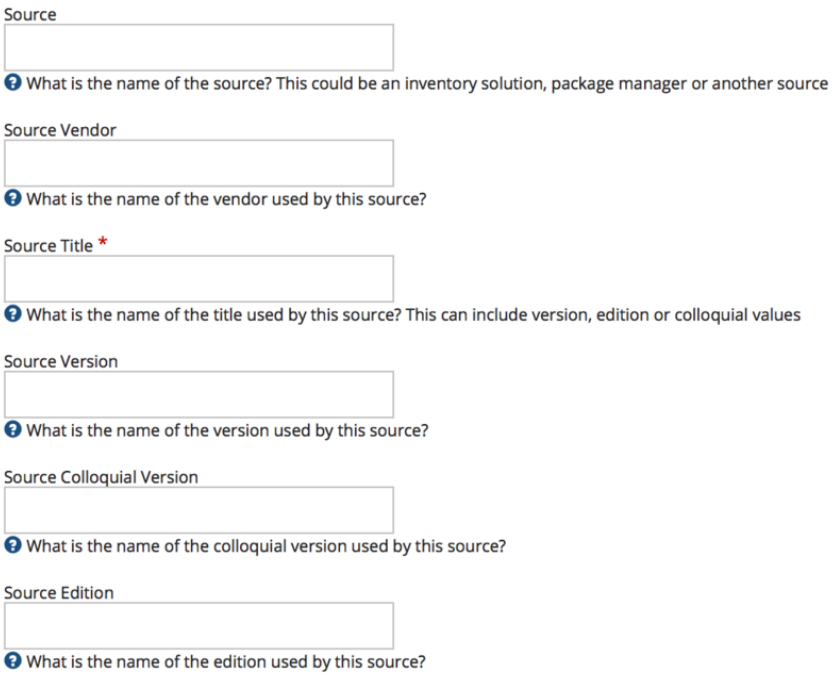
This is how the Catalog normalizes the source inventory. The same match rule principles apply equally to devices and processors in the Catalog.

1.8.6.12.1 Adding a match rule to a version of a product

To associate a match rule to a version of a product:

1. On the **Product** screen, click **Filtering** and enter your search criteria.
2. Click the **Versions** link to the right of the product.
3. Filter by version number to narrow the list and select the product version you want.
4. Under the **Actions** column, click the **Match Rules** link for that specific version.
5. Click the **Add a new match** rule link.

6. Enter the source inventory data that will be used to link to this product and version combination:



   - **Source** - the source for this inventory, for example SCCM
   - **Source Vendor** - the text that's in the Vendor field in the source data
   - **Source Title** (mandatory) - the text that's in the Title field in the source data
   - **Source Version** - the text that's in the Version field in the source data
   - **Source Colloquial Version** - the text that's in the colloquial version field in the source data
   - **Source Edition** - the text that's in the edition field in the source data.

7. Click **Save**

When a source inventory contains all the information that's recorded in the match rule fields, it's linked to the product version containing that match rule.

To add a match rule to an edition of a version, follow steps 1 through 3, and then:

1. Under the **Actions** column, click **Editions**.
2. From the list of editions, choose the one you want and click the **Match Rules** link to the right of it.
3. Repeat steps 5 to 7 above.

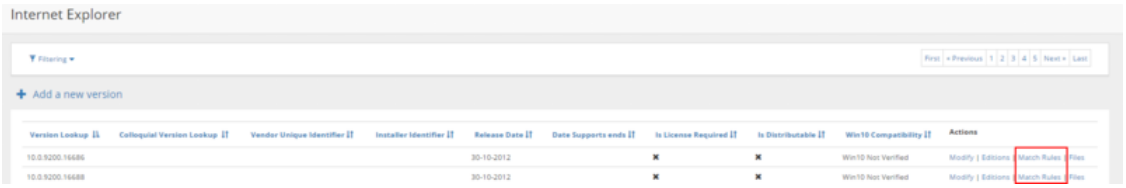
You can add match rules to **Devices** and **Processor** by simply following the procedures above in the respective **Devices** and **Processor** sections.

1.8.6.12.2 Removing an existing match rule

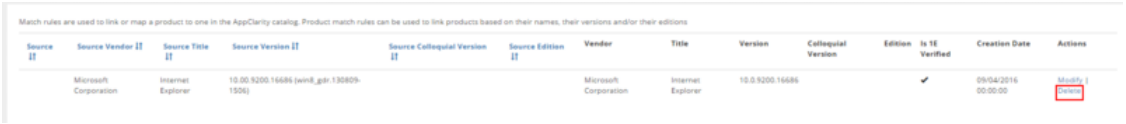
You can disassociate the link between a source inventory and a catalog item by deleting its match rule.

Follow the steps above to navigate to the product or version the current match rule is associated with, or the product, version, or edition.

Click on the **Match Rules** link on the right-hand side of the specific version, or edition.



Then click **delete** on the match rule to be removed:



This unlinks the source inventory from this catalog entry.

1.8.6.13 Using filters

The **Filtering** feature narrows the results of your search list. To do this:

1. Click Filtering.

2. Enter your search criteria.

3. Click **Filter**.

1.8.6.14 How we manage versions

The same number of version parts are required for each **major.minor** version of a product, the logic is:

1. If the first entry for a product is 9.0, we accept it.

2. If a new entry in the Catalog has 9.0.1, the original 9.0 entry will be automatically updated to 9.0.0 thereby forcing a three-part version number for consistency (9.0.0 and 9.0.1).

3. If there are two entries in the Catalog with the same **major.minor** version and title (like 9.0 and 9.0.0) they will be merged to form one record (after merging just 9.0.0 will be left).

4. Any existing match rules are added to the new consolidated record.

For example:

- Adobe After Effects 9.0 has a match rule:

Source			Target				
Vendor	Title	Version	Vendor	Title	Version	Coll Version	Edition
Adobe Systems Incorporated	Adobe After Effects CS4	9	Adobe Systems Incorporated	After Effects	9.0	CS4	

- Adobe After Effects 9.0.0 has a match rule:

Source			Target				
Vendor	Title	Version	Vendor	Title	Version	Coll Version	Edition
Adobe Systems Incorporated	Adobe After Effects CS4	9.0	Adobe Systems Incorporated	After Effects	9.0.0	CS4	

- The source parts of these two match rules are merged to produce two new match rules associated with the new 9.0.0.0 version:

Source			Target				
Vendor	Title	Version	Vendor	Title	Version	Coll Version	Edition
Adobe Systems Incorporated	Adobe After Effects CS4	9	Adobe Systems Incorporated	After Effects	9.0.0.0	CS4	
Adobe Systems Incorporated	Adobe After Effects CS4	9.0	Adobe Systems Incorporated	After Effects	9.0.0.0	CS4	

1.8.7 AI Powered Auto-curation

Describes the AI Powered Auto-curation feature that improves software inventory results. Using the AI Powered Auto-curation feature, you'll be able to increase the total amount of normalized software in your Inventory repositories. This is done using AI that integrates with the inventory consolidation process. By using AI, your organization will benefit from significant numbers of normalized software and a reduced manual effort needed to normalize software.

> **Note**
>
> The Inventory app captures data from different sources, then consolidates, normalizes, and stores it in Inventory repositories. It is also used to view, export, and manage associations.

Inventory uses connectors to capture software, hardware, and other data from sources such as Tachyon, Configuration Manager, Big Fix, and vCenter where it is consolidated, de-duplicated, and normalized. Normalization uses software and hardware entries in The 1E Catalog.

An empty repository called **Default Inventory** is provided out-of-the-box. You can optionally create additional inventory repositories to partition data by source, time period, or another purpose. To populate a repository, you must use one or more inventory connectors, and either manually sync the data or schedule a sync. For more detail, please refer to Repositories page and Schedules page in Settings.

In old versions normalization of software product names was handled by 1E Catalog. This used rules that map source Programs and Features data into an accurate standardized form of Vendor, Title, Version, and Edition (VTVE) fields. These normalized records could then be referred to with the same signature. Although the rules in the 1E Catalog cover the most common software, there is always new software that needs to be manually mapped.

AI Powered Auto-curation normalizes software product names that are not in the 1E Catalog. It first extracts the VTVE from varied raw Programs and Features data by removing excess data and extracting the relevant strings. The AI then standardizes the VTVE fields to a single, accurate form of representation. It also produces a numeric value called the confidence score, this score:

- Represents how confident the AI is in its prediction.
- Is set to a high threshold through testing and validation across a large data set.
- Can be calibrated according to the variety of software data at a customer site to optimize the normalization rate.
- Is controlled by 1E through collaboration with customers.

You can enable AI Powered Auto-curation either during or after the installation of Tachyon.

Note

AI Powered Auto-curation is used by all Inventory connectors. Please refer to the Connectors page for more information about how Connectors are used to connect to other 1E and third party systems.

AI Powered Auto-curation uses model files that govern its behavior and, when the feature is enabled, the versions of the files are compared with the versions in the 1E Cloud, and downloaded whenever a new version is made available.

1.8.7.1 Preparation

Before you enable AI Powered Auto-curation, ensure you've met the additional disk and memory requirements on the Tachyon web server.

Note

The minimum total disk space required for the downloaded AI Package ZIP is approximately 13 GB at installation. This includes:

- Binary and support files for AI and the directory structure is 8 GB
- The ZIP file is approximately 5 GB and stored in the **Download path** - this location is not configurable
- The ZIP file is then temporarily copied to the **Deployment path**, and extracted - the ZIP plus extracted files are approx. 13 GB
- The temporary ZIP is then deleted from the **Deployment path**, leaving approx. 8GB of extracted files - this location is configurable, as described below.

1E Catalog regularly checks it has the latest AI package synced from the 1E Catalog cloud. It downloads the AI Package ZIP (5GB) from the Cloud into the **Download path** folder.

Whenever the **Basic Inventory Consolidation (BIC)** process runs, with the **AI Engine option** enabled, the **1E-AIEngine.exe** uses the AI package files to run the AI process.

When the **1E-AIEngine.exe** is run, it uses a hash comparison of its current AI package, with the Catalog's ZIP.

- If the hash is different, it will make a copy of the new ZIP (5GB) to its **Deployment path**, extract it (8GB), and then delete the ZIP copy.
- If the folder contains the correct AI package, the BIC processes the new inventory data using the package.

Note

1E Catalog is included in the Tachyon Platform zip, and installed by Tachyon Setup.

1.8.7.1.1 Memory requirements

Distinct Software Titles	Extra GB RAM for AI engine
1 to 5000	17
10000	19
20000	21
30000	24
40000	26
50000	29
60000	32

Distinct Software Titles	Extra GB RAM for AI engine
70000	35
80000	39
90000	42
100000	46
110000	50
120000	54
130000	58
140000	62
150000	66
160000	71
170000	76

Values last updated 04 Mar 2022.

The physical memory required for AI Powered Auto-curation is based on the number of distinct software titles in your source data, that AI has to process that do not already have a match in the 1E Catalog. Use the accompanying table as a quick reference for the memory requirements needed by the AI.

> **Note**
>
> For virtual machines, the AI Engine action will not work if you're using a dynamic memory configuration. You'll need to allocate dedicated memory.

If you're only using a System Center Configuration Manager connector for your source data, then use the below **SCCM database query** as a guide for how much extra RAM you need on the Tachyon web server before installing Tachyon.

SCCM database query Expand source

```
/*SCCM database query to get number of distinct software titles from SCCM datab
ase*/
USE [YourSCCMDBName]
GO
SELECT COUNT(*) AS 'Distinct Software Titles'
FROM (
```

```
        SELECT DISTINCT DisplayName0 AS Title FROM [v_ADD_REMOVE_PROGRAMS] WITH
(NOLOCK)
        UNION
        SELECT DISTINCT [Caption0] AS Title FROM [v_GS_OPERATING_SYSTEM] WITH (
NOLOCK)
) AS Titles
```

After installation, we recommend you use the below **SLA-Data database query** to double-check memory requirements. You will need to use the SLA query anyway, if you use a Tachyon connector (for Inventory or Patch Success) either on its own, or with other connectors including SCCM. In this case, use the **SLA-Data database query** after installation and you have collected your source data.

SLA-Data database query Expand source

```
/*SLA query to get number of distinct software titles from SLA-Data database*/
USE [SLA-Data]
CREATE TABLE #Software
       (
              [SoftwareID]                    INT IDENTITY(1,1) PRIMARY KEY,
              [DataSource]                    NVARCHAR(255) COLLATE DATABASE_
DEFAULT,
              [SoftwareIdent]                 NVARCHAR(MAX) COLLATE DATABASE_
DEFAULT,
              [SoftwareIdent_Hash]                   VARBINARY(128),
              [Vendor]                        NVARCHAR(MAX) COLLATE DATABASE_
DEFAULT,
              [Vendor_Hash]                             VARBINARY(128),
              [Title]                         NVARCHAR(MAX) COLLATE DATABASE_
DEFAULT,
              [Title_Hash]                    VARBINARY(128),
              [Version]                       NVARCHAR(MAX) COLLATE DATABASE_
DEFAULT,
              [Version_Hash]                  VARBINARY(128),
              [ColloquialVersion]             NVARCHAR(MAX) COLLATE DATABASE_
DEFAULT,
              [ColloquialVersion_Hash]        VARBINARY(128),
              [Edition]                       NVARCHAR(MAX) COLLATE DATABASE_
DEFAULT,
              [Edition_Hash]                  VARBINARY(128),
              [NormalizedProductID]           INT
       );
SELECT * FROM #Software
EXEC [usp_ReportDataEx_se] 1, N'Software', N'#Software';

SELECT count(*) AS 'Distinct Software Titles'
FROM
(
SELECT DISTINCT [Title] FROM #Software
) a

DROP TABLE #Software
```

1.8.7.2 Enabling AI Powered Auto-curation

You can enable AI Powered Auto-curation either during or after installation of Tachyon.

1.8.7.2.1 Enabling AI Powered Auto-curation during installation of Tachyon

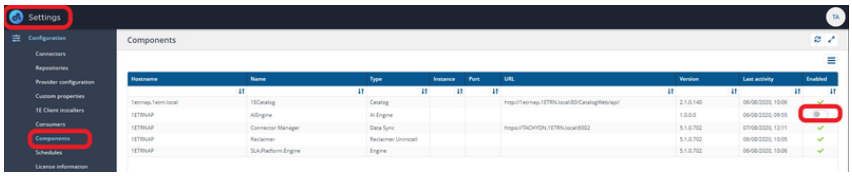
AI is switched off by default in the Tachyon Setup, this is because the feature requires additional memory to run correctly. For more details please refer to the AI Powered Auto-curation requirements.

During Tachyon setup you'll need to check the **Enable AI-based auto-curation** checkbox on the **SLA and Catalog** screen of the Tachyon Setup wizard. For more details please refer to the Tachyon Setup and SLA and 1E Catalog.

1.8.7.2.2 Enabling AI Powered Auto-curation after installation of Tachyon

You can enable AI Powered Auto-curation after you've installed Tachyon, but before enabling check these pages for more details on the disk space and RAM requirements: Tachyon Setup and SLA and 1E Catalog.

Once you have confirmed the pre requisites to enable AI you should access the Settings→Configuration→Components and toggle the Enabled switch on the AI Engine row.



At the point when you enable AI, a popup will be displayed, shown opposite.

1.8.7.2.3 Disabling AI Powered Auto-curation after installation of Tachyon

You can use the same **Enabled** toggle on the AI Engine row in the **Settings → Configuration → Components** page to turn off the AI Powered Auto-curation by sliding it to the left, off position.

1.8.7.2.4 Changing the AI Deployment path

The AI feature consists of an **1E-AIEngine.exe** and AI model files contained in an **AIPackage_<version>.zip**.

The minimum total disk space required for the downloaded AI Package ZIP is approximately 13 GB at installation. This includes:

- Binary and support files for AI and the directory structure is 8 GB
- The ZIP file is approximately 5 GB and stored in the **Download path** - this location is not configurable
- The ZIP file is then temporarily copied to the **Deployment path**, and extracted - the ZIP plus extracted files are approx. 13 GB

- The temporary ZIP is then deleted from the **Deployment path**, leaving approx. 8GB of extracted files - this location is configurable, as described below.

1E Catalog regularly checks it has the latest AI package synced from the 1E Catalog cloud. It downloads the AI Package ZIP (5GB) from the Cloud into the **Download path** folder.

Whenever the **Basic Inventory Consolidation (BIC)** process runs, with the **AI Engine option** enabled, the **1E-AIEngine.exe** uses the AI package files to run the AI process.

When the **1E-AIEngine.exe** is run, it uses a hash comparison of its current AI package, with the Catalog's ZIP.

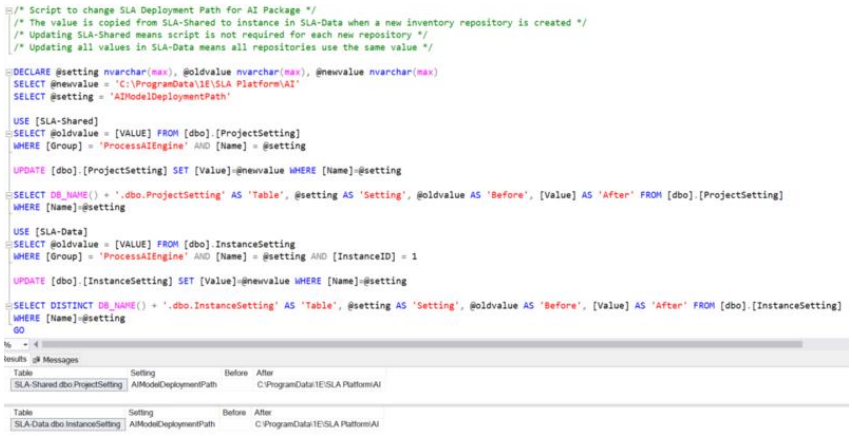
- If the hash is different, it will make a copy of the new ZIP (5GB) to its **Deployment path**, extract it (8GB), and then delete the ZIP copy.
- If the folder contains the correct AI package, the BIC processes the new inventory data using the package.

Name	Default path	Purpose
Download path	C:\ProgramData\1E\Catalog\CatalogSynchronization\Prediction Model	This path is not configurable.
Deployment path	C:\ProgramData\1E\SLA Platform\AI	This path is configurable using the SQL script described below.

SQL script to configure AIModelDeploymentPath setting Expand source

```
/* Script to change SLA Deployment Path for AI Package */
/* The value is copied from SLA-Shared to instance in SLA-Data when a new inven
tory repository is created */
/* Updating SLA-Shared means script is not required for each new repository */
/* Updating all values in SLA-Data means all repositories use the same value */

DECLARE @setting nvarchar(max), @oldvalue nvarchar(max), @newvalue nvarchar(max
)
SELECT @newvalue = 'C:\ProgramData\1E\SLA Platform\AI'
SELECT @setting = 'AIModelDeploymentPath'

USE [SLA-Shared]
SELECT @oldvalue = [VALUE] FROM [dbo].[ProjectSetting]
WHERE [Group] = 'ProcessAIEngine' AND [Name] = @setting

UPDATE [dbo].[ProjectSetting] SET [Value]=@newvalue WHERE [Name]=@setting
```

```
SELECT DB_NAME() + '.dbo.ProjectSetting' AS 'Table', @setting AS 'Setting', @ol
dvalue AS 'Before', [Value] AS 'After' FROM [dbo].[ProjectSetting]
WHERE [Name]=@setting

USE [SLA-Data]
SELECT @oldvalue = [VALUE] FROM [dbo].InstanceSetting
WHERE [Group] = 'ProcessAIEngine' AND [Name] = @setting AND [InstanceID] = 1

UPDATE [dbo].[InstanceSetting] SET [Value]=@newvalue WHERE [Name]=@setting

SELECT DISTINCT DB_NAME() + '.dbo.InstanceSetting' AS 'Table', @setting AS 'Set
ting', @oldvalue AS 'Before', [Value] AS 'After' FROM [dbo].[InstanceSetting]
WHERE [Name]=@setting
GO
```



1.8.7.3 Verifying AI Auto-curation is working

The process for downloading the latest AI Package is described above in Changing the AI Deployment path.

You can review the Catalog sync progress in the following logs located at: **C:\ProgramData\1E\Catalog**

- Catalog.Integration.UI.log
- Catalog.UpdateService.log

A successful sync should be similar to the example **Catalog.UpdateService.log** opposite.

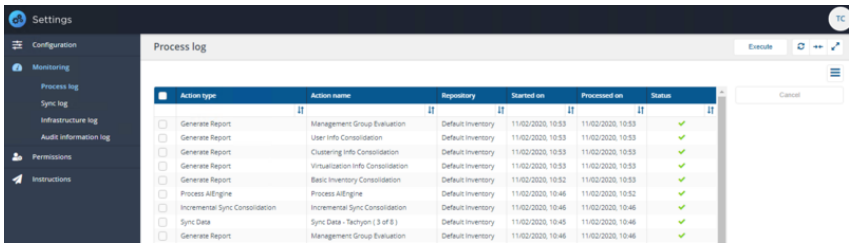
Catalog.UpdateService.log Expand source

```
[Info] T11 2020-01-31 15:45:48.567: Syncing AI Package with cloud
[Info] T11 2020-01-31 15:45:48.756: Downloading AI Package version 1.3.0.700 wi
th cloud of size 4804685823 from url  api/sync/aiengine?Version=1.3.0.700
[Info] T11 2020-01-31 15:45:48.772: Indexes re-creation started after Sync.
[Info] T12 2020-01-31 15:58:25.929: Indexes are created successfully after Sync
.
[Info] T5 2020-01-31 16:30:47.930: Download complete. Comparing file hash..
[Info] T5 2020-01-31 16:31:07.120: Successfully synced AI Package version 1.3.0
.700 with cloud
```

When enabled, a new action called **Process AIEngine** is created. This is automatically run after the **Sync Data** action for a supported connector. The sync time for the **Process AIEngine** action depends on the number of distinct software records being processed, hardware and environment configuration.

AI Powered Auto-curation is used by all Inventory connectors. Please refer to the Connectors page for more information about how Connectors are used to connect to other 1E and third party systems.

You can see the **Process AIEngine** action in **Settings**→Monitoring→Process log .



You can review its progress using the **Engine.log** located at **C:\ProgramData\1E\SLA Platform**

In the log, you should see something similar to the opposite example.

Engine.log Expand source

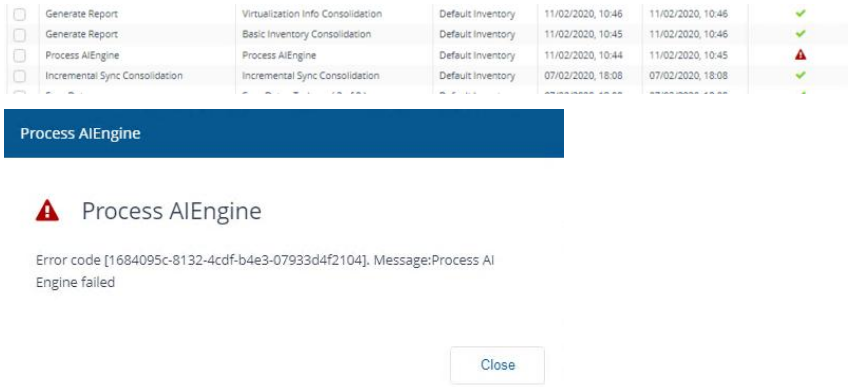
```
2020-03-31 08:46:25.0274 INFO  Action Process AIEngine starting! Jobs: 1/5
2020-03-31 08:46:25.0274 INFO  ID=612d1b08-7eb7-4bf1-9c23-46dea29d9b6d Starting
action: 11065
2020-03-31 08:46:25.0274 DEBUG  [HubConnection] Adding notification '11065' to
queue. Queue count:3.
2020-03-31 08:46:25.0274 INFO  Folder's available in PreProcessAsync: output- T
rue, input- True, tempDir- True, training- True
2020-03-31 08:46:25.0500 INFO  Catalog web address: http://LAB.LAB.local/Catalo
gWeb/
2020-03-31 08:46:25.0704 INFO   Is higher version False, localVersion 1.3.0.700
, serverVersion 1.3.0.700
2020-03-31 08:46:25.0704 INFO  serverFileDetails.Base64filehash 0x853E29401B209
301C9F9C4D381202C931816C871, modelFileDetails.Base64filehash 0x853E29401B209301
C9F9C4D381202C931816C871
2020-03-31 08:46:25.0724 INFO  Condition for download before checking: False
2020-03-31 08:46:25.0724 INFO  Saving Model file hash (0x853E29401B209301C9F9C4
D381202C931816C871) and version (1.3.0.700)
2020-03-31 08:46:25.1124 DEBUG  [HubConnection] Notification sent '11064'
2020-03-31 08:46:25.1484 DEBUG  [HubConnection] Adding notification '0' to queu
e. Queue count:2.
2020-03-31 08:46:25.1484 INFO  Folder's available in ProcessAsync: output- True
, input- True, tempDir- True, training- True
2020-03-31 08:46:25.1504 INFO  Folder's available in Before Invoking AI EXE: ou
tput- True, input- True, tempDir- True, training- True
2020-03-31 08:46:25.1504 DEBUG  [HubConnection] Notification sent '0'
2020-03-31 08:46:25.1504 INFO  process started - 9636process name is 1E-AIEngin
e
2020-03-31 08:46:25.1504 INFO  in wait for exit async
2020-03-31 08:46:25.1504 INFO  In Read Async
```

```
2020-03-31 08:46:25.1724 DEBUG  [HubConnection] Notification sent '11065'
2020-03-31 08:46:25.1967 DEBUG  [HubConnection] Notification sent '0'
2020-03-31 08:51:05.5709 INFO  Folder's available in After Invoking AI EXE: out
put- True, input- True, tempDir- True, training- True
2020-03-31 08:51:05.5709 INFO  AI process completed with exit code: 0
```

If you see a red warning triangle in the Process log, this indicates a problem.

The most common reason for the Process AIEngine to fail is due to insufficient memory when it runs, refer to Memory requirements for details.

In this example, clicking on the red warning triangle displays an error message explaining that the Process AIEngine has failed.

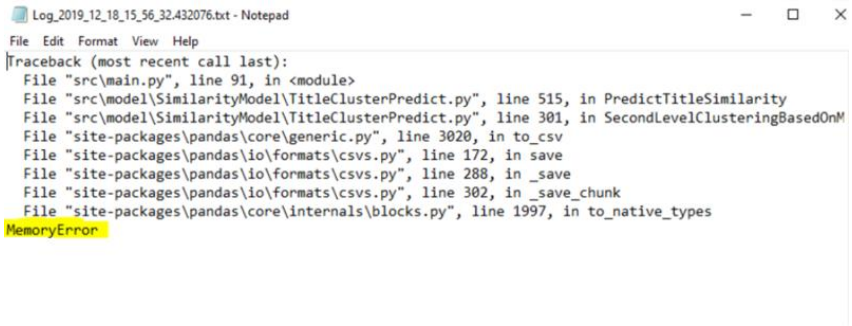


You can review the AI logs at: **C:\ProgramData\1E\SLA Platform\AI\Log_*.txt**

The picture opposite shows an example of a failure logged due to insufficient memory. **Log_*.txt**

> **Note**
>
> If the AI processing step does fail, the overall inventory consolidation will not. In the event of a failure, the AI processing step is skipped, making sure the rest of the process takes place as expected.

Log_*.txt > Expand



1.8.7.4 Differences in SLA Inventory screens when AI Powered Auto-curation is enabled

The SLA Inventory UI screens differ if AI Powered Auto-curation is enabled or disabled.

The process of setting up connectors, creating inventory repositories and running the basic inventory consolidation remains the same.

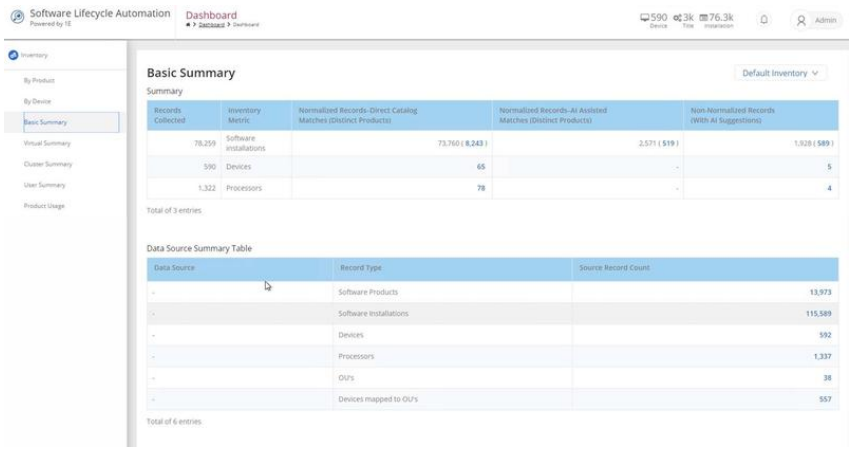
1.8.7.4.1 Basic Summary screen

You can access the Basic Summary screen using the **Inventory** app and by choosing **SLA Inventory** from the left-hand menu. The data in this screen is updated by the Basic Inventory Consolidation process.

The **Summary** table now includes software records curated by AI. The first column in the table shows the total **Records Collected**. The next three columns are:

- **Normalized Records-Direct Catalog Matches (Distinct Products)** - corresponds to software records identified using existing rules in the 1E Catalog. Exploring these will show you the normalized entries with enriched data regarding licensability, end-of-support date etc.
- **Normalized Records-AI Assisted Matches (Distinct Products)** - the software records which AI has automatically matched and normalized. The AI recognizes the vendor, title, version and edition and normalizes them. Over time, the 1E Catalog reviews records identified by AI and enriches them with data regarding licensability, end-of-support date etc. for inclusion in future downloads.
- **Non-Normalized Records (With AI Suggestions)** - software records which AI has low confidence in automatically matching. AI makes predictions for all source data, but predictions with a low confidence score should be manually reviewed by drilling down to the Unidentified Software Records screen.

The numbered links in brackets allow you to drill down to more detailed screens.



1.8.7.4.2 Unidentified Software Records screen

You can access this screen by clicking on the number link in the **Non-Normalized Records (With AI Suggestions)** column of the **Basic Summary** screen. This screen shows AI predictions that have a low confidence score preventing them being automatically matched and normalized. These predictions should still be close to accurate, therefore making the task of manually adding rules to the Catalog much easier.

This screen has the following elements:

1.8.7.4.2.1 Overview

Shows a count of distinct software records to be identified, so you can keep track of progress.

- Software Products left to identify - show all records
- **AI predicted** - records the AI was unable to identify, but was able to provide suggestions
- **AI predicted and partially matched** - where the vendor or title was identified through previous knowledge from the 1E Catalog, these records have a default high confidence score
- **Cannot be identified** - these records have insufficient information to recognize the software or make a prediction.

1.8.7.4.2.2 Application Type

Filters by application type.

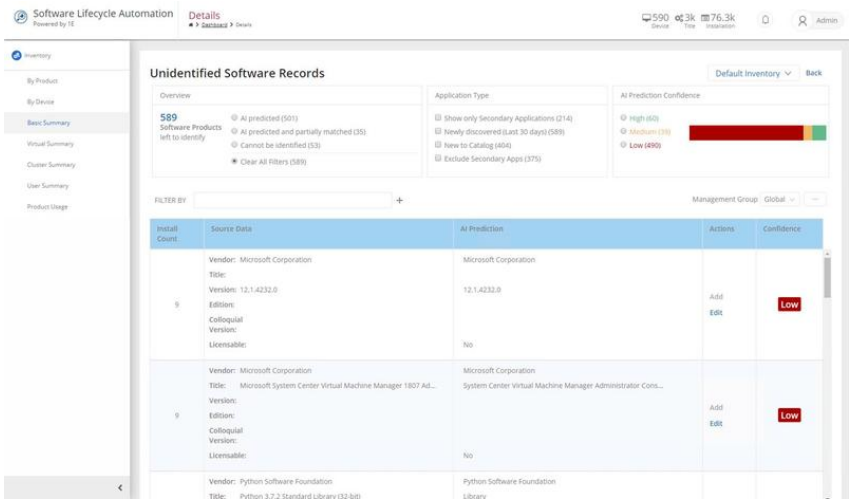
- **Show only Secondary Applications** -filters to only secondary applications (for example, updates, hotfixes or language packs)
- **Newly discovered (Last 30 days)** - filters to applications discovered within the last 30 days
- **New to Catalog** - filters to applications that are either new vendors or titles previously unknown to the 1E Catalog
- **Exclude Secondary Apps** - removes any applications considered secondary, like updates, hot fixes or language packs.

1.8.7.4.2.3 AI Prediction Confidence

Confidence scores for predictions are divided into three equal parts below the threshold. **High**, **Medium** and **Low** confidence relate to the ease at which the AI engine suggestions can be manually reviewed and added as rules.

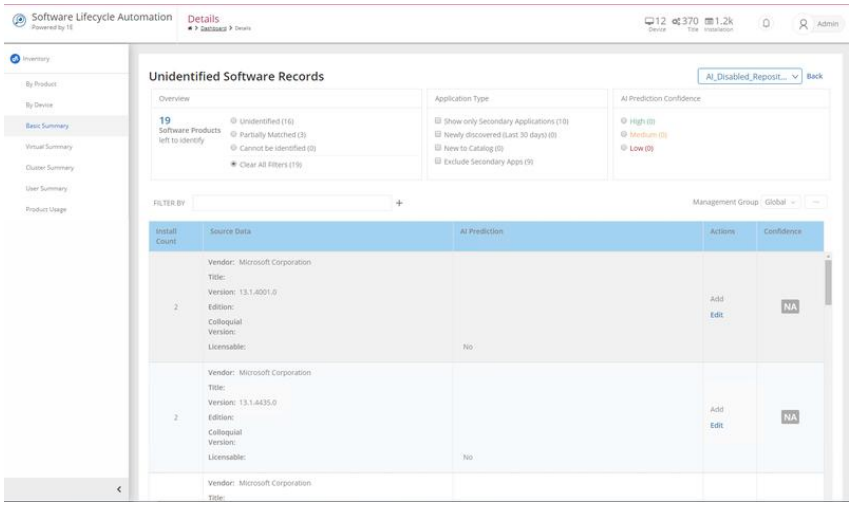
1.8.7.4.2.4 FILTER BY

Use this to add conditional filters for various fields on the **Unidentified Software Records Table**, for example you could filter on "Vendor Contains Micro" to return results based on Microsoft as a software vendor.



Note

If the AI feature is disabled the **Basic Summary** screen will differ to when AI is enabled, note the difference in the **Overview** element.



1.8.7.4.2.5 Unidentified Software Records Table

Each row on this table corresponds to a distinct set of software records. There are four values **Install Count**, **Source Data** , **AI Prediction** , **Confidence** and a number of actions to perform for each distinct record. The values are:

Action	Explanation
Install Count	The total number of records found with the same source data across the estate.
Source Data	ARP data extracted into **Vendor, Title**, **Version**, **Edition**, **Colloquial Version** and **Licensable** fields.

Action	Explanation
AI Prediction	The AI suggestion after attempting to extract **Title**, **Version**, **Vendor**, **Edition**, **Colloquial Version** and **Licensable** fields from source data, Licensability is set to a default of **No** on the suggestions table, this can be edited before adding.
Confidence	Abstracted to high, medium or low based on the exact numeric value for prediction confidence, these confidences values will always be lower than the threshold required to automatically normalize records.

For each record the **Actions** are:

Action	Explanation
Add	When clicked, this will add records directly to 1E Catalog. This option is enabled if AI suggestions for a source Vendor, Title, Version and Edition (VTVE) are generated. In case the product is not Edition based then Vendor, Title and Version (VTV) suggestions are enough. After the record(s) is added to 1E Catalog then whenever you run the next**Basic Inventory Consolidation** then the same record(s) will be available in the **Catalog Matched** items.
Edit	Edit functionality is available for all unidentified records. When clicked, it opens a dialog where you can provide details for the selected software record. You also have the option to add this information to 1E Catalog.
Exclude	Exclude is available for all **Unidentified Software Records,** except for **Partially Matched** and **Secondary Application** types of records. Once excluded, the items are moved to **Secondary Applications**. You can also **Include** it again until the next **Basic Inventory Consolidation** is run, afterwards the **Include** option will be unavailable, and the item will become a part of **Secondary Applications**.

You can explore these records to see what the AI has curated by clicking on the related links in the **Basic Summary Report**.

Note

We have also introduced a new screen for AI suggestions for any software records that remain non-normalized. This is a replacement for the **Best Match Screen** which allowed you to add rules.

1.8.8 Configuring 1E Catalog connection to 1E Cloud

Post-install configuration of 1E Catalog synchronization and AI Powered Auto-curation.

1.8.8.1 1E Catalog synchronization options

1E Catalog regularly synchronizes itself with the catalog curated by 1E in the 1E Cloud. Options are:

- **bi-directional synchronization (default)** - pushes site-defined entries to the 1E Cloud Catalog for verification by the 1E curation team and pulls new content entries or updates from the cloud
- **uni-directional synchronization** - pulls new content or updates from the 1E Cloud Catalog
- **no synchronization** - no attempts to synchronize with 1E Cloud Catalog.

For each batch, the synchronization event writes the number of processed records to the log files.

Please refer below for details of Data sent from the 1E Catalog to the 1E Cloud.

1E Catalog can also be configured during installation to download the files related to the AI Powered Auto-curation feature. Please refer to AI Powered Auto-curation for more details.

1.8.8.2 Modifying 1E Catalog Cloud synchronization behavior post-installation

The following script can be used to modify the **SubscriptionType** setting in the **Settings** table of the **1ECatalog** database. You can set the new value to be one of the following:

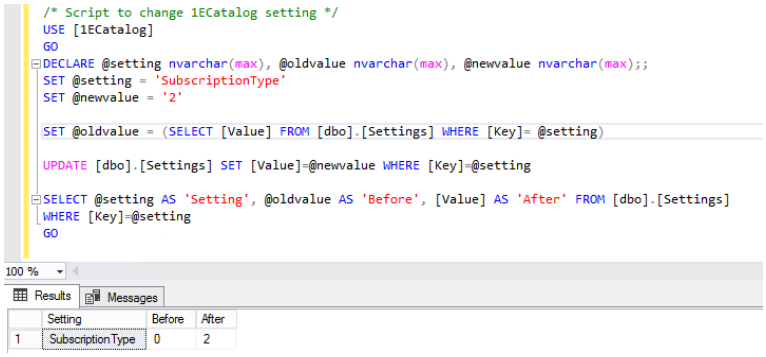
Value	Description
0	no synchronization
1	uni-directional synchronization
2	bi-directional synchronization (default)

After changing the value you will need to restart the **1E Catalog Update Service** for your changes to take effect.

SQL script to configure SubscriptionType setting

```
/* Script to change 1ECatalog setting */
USE [1ECatalog]
GO
DECLARE @setting nvarchar(max), @oldvalue nvarchar(max), @newvalue nvarchar(max
);;
SET @setting = 'SubscriptionType'
SET @newvalue = '2'

SET @oldvalue = (SELECT [Value] FROM [dbo].[Settings] WHERE [Key]= @setting)

UPDATE [dbo].[Settings] SET [Value]=@newvalue WHERE [Key]=@setting

SELECT @setting AS 'Setting', @oldvalue AS 'Before', [Value] AS 'After' FROM [d
bo].[Settings]
```

```
WHERE [Key]=@setting
GO
```



1.8.8.3 Modifying 1E Catalog AI Powered Auto-curation file download post-installation

The following script can be used to modify the **EnableAIPackageSync** setting in the **Settings** table of the **1ECatalog** database . You can set the new value to be one of the following:

Value	Description
True	Download will be enabled.
False	Download will be disabled.

After changing the value you will need to restart the **1E Catalog Update Service** for your changes to take effect.

SQL script to configure EnableAIPackageSync setting

```
/* Script to change 1ECatalog setting */
USE [1ECatalog]
GO
DECLARE @setting nvarchar(max), @oldvalue nvarchar(max), @newvalue nvarchar(max
);;
SET @setting = 'EnableAIPackageSync'
SET @newvalue = 'True'

SET @oldvalue = (SELECT [Value] FROM [dbo].[Settings] WHERE [Key]= @setting)

UPDATE [dbo].[Settings] SET [Value]=@newvalue WHERE [Key]=@setting

SELECT @setting AS 'Setting', @oldvalue AS 'Before', [Value] AS 'After' FROM [d
bo].[Settings]
WHERE [Key]=@setting
GO
```

```
/* Script to change 1ECatalog setting */
USE [1ECatalog]
GO
DECLARE @setting nvarchar(max), @oldvalue nvarchar(max), @newvalue nvarchar(max);;
SET @setting = 'EnableAIPackageSync'
SET @newvalue = 'True'

SET @oldvalue = (SELECT [Value] FROM [dbo].[Settings] WHERE [Key]= @setting)

UPDATE [dbo].[Settings] SET [Value]=@newvalue WHERE [Key]=@setting

SELECT @setting AS 'Setting', @oldvalue AS 'Before', [Value] AS 'After' FROM [dbo].[Settings]
WHERE [Key]=@setting
GO
```

100 %

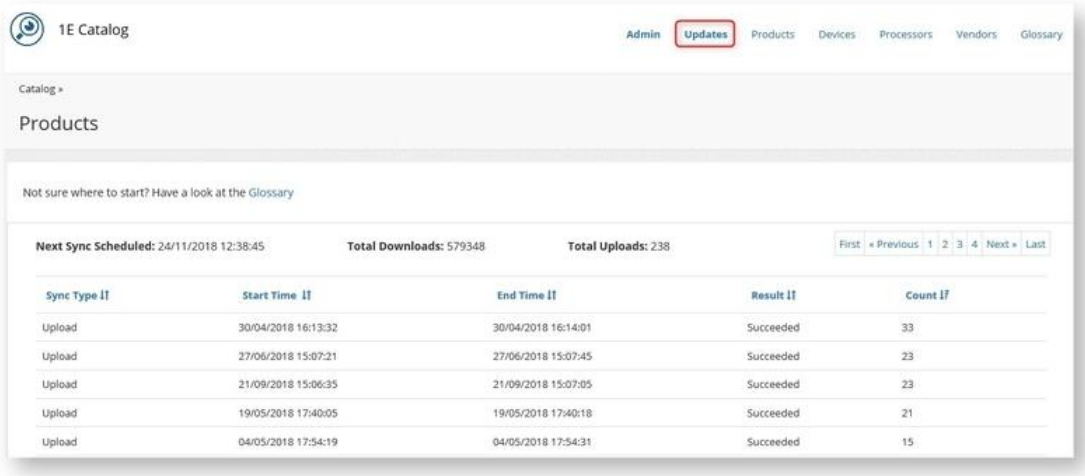
Results | Messages

	Setting	Before	After
1	EnableAIPackageSync	False	True

1.8.8.4 Viewing synchronization events in Catalog UI

View synchronization event history from the **Updates** screen, listing:

- **Sync Type** – whether it was an upload or a download
- **Start Time**
- **End Time**
- **Result** – success or failure - event details are written to log files typically located in *C:\ProgramData\1E\Catalog\Catalog.Updateservice.log*
- **Count** - number of synchronized records.

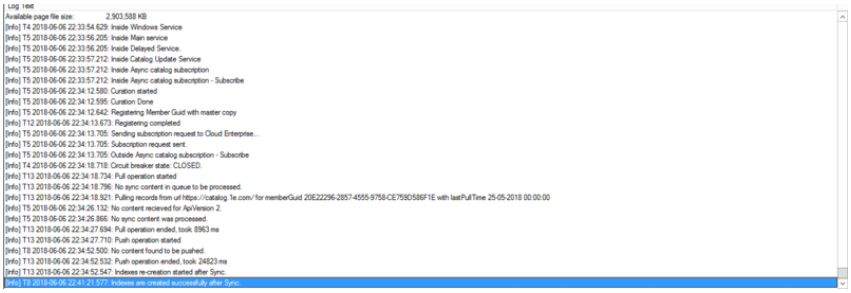


1.8.8.5 Reviewing the log file

The regular synchronization with the 1E Cloud Catalog is logged in **Catalog.UpdateService.log**. In general, the process is as follows:

1. Catalog Registers with the master copy.
2. The Catalog will then pull content.
3. Push content if enabled.

4. The Catalog will then index the content.



1.8.8.6 1E Catalog data files

The 1E Catalog data files, both installed and downloaded from the 1E Cloud during synchronization, are stored in the following locations. These locations are not configurable in this version of 1E Catalog.

Data	Location
Catalog data	%ProgramData%\1E\Catalog
Installer data	%ProgramData%\1E\Catalog\CatalogSynchronization\Data
Synchronization data from the 1E Cloud Catalog	%ProgramData%\1E\Catalog\CatalogSynchronization\Sync
Lucene index	%ProgramData%\1E\Catalog\CatalogSynchronization\LuceneIndex
AI Powered Auto-curation files	%ProgramData%\1E\Catalog\CatalogSynchronization\PredictionModel

1.8.8.7 Data sent from the 1E Catalog to the 1E Cloud

The following show the tables of data sent from the 1E Catalog to the 1E Cloud to help improve the quality of the 1E Catalog data for all customers. The data is mainly related to software products and AI prediction models, no identifiable customer-related information is sent.

- Add/Remove Programs data
- Site-defined processor information
- Device type (not including the device name)
- Software bundling
- Software category

- Start/end dates
- .exe to product mapping data.

PredictionModels

PredictionModelID

Version

VersionMajor

VersionMinor

VersionRevision

VersionBuild

FileName

FileHash

FileSize

SubmissionSource

SubmissionSourceValue

CreationDate

Is1EVerified

IsDeleted

IsDownloaded

PredictionResults

PredictionResultID

PredictionResults

SourceVendor

SourceTitle

SourceVersion

SourceColloquialVersion

SourceEdition

Vendor

Title

Version

ColloquialVersion

Edition

SecondaryVendor

SecondaryTitle

SecondaryVersion

SecondaryColloquialVersion

SecondaryEdition

UpdateGuid

KBNumber

ServicePack

BitLength

Language

PredictionResults

Confidence

ModelVersion

SubmissionSource

SubmissionSourceValue

IsComplete

CreationDate

Is1EVerified

IsDeleted

SimilarityResults

SimilarityResultID

SourceVendor

SourceTitle

SourceVersion

SourceColloquialVersion

SourceEdition

SourceSecondaryVendor

SourceSecondaryTitle

SourceSecondaryVersion

SourceSecondaryColloquialVersion

SimilarityResults

SourceSecondaryEdition

SourceUpdateGuid

SourceServicePack

SourceKBNumber

SourceBitLength

SourceLanguage

Vendor

Title

Version

ColloquialVersion

Edition

Confidence

ModelVersion

IsInCatalog

SubmissionSource

SubmissionSourceValue

CreationDate

Is1EVerified

IsDeleted

ProductMatches

ProductMatchID

Language

SourceProductID

Source

SourceVendor

SourceVendor_MD5

SourceTitle

SourceTitle_MD5

SourceVersion

SourceVersion_MD5

SourceColloquialVersion

SourceColloquialVersion_MD5

SourceServicePack

SourceServicePack_MD5

SourceEdition

SourceEdition_MD5

ProductID

Vendor

Vendor_MD5

Title

ProductMatches

Title_MD5

ProductVersionID

Version

Version_MD5

ColloquialVersion

ColloquialVersion_MD5

ServicePack

ServicePack_MD5

ProductEditionID

Edition

Edition_MD5

SubmissionSourceLookup

SubmissionSourceValue

Is1EVerified

CreationDate

IsDeleted

PatchEnum

PatchIdentifier

ProductVariants

ProductVariantID

VendorID

ProductID

Language

Vendor

Title

ProductVersionID

Version

ColloquialVersion

ServicePack

ProductEditionID

Edition

VendorUniqueIdentifier

InstallerIdentifier

ReleaseDate

EndOfSupportDate

IsLicenseRequired

IsDistributable

IsBundle

IsDeleted

ProductVariants
UNStandardProductServiceCode
CommonProcurementVocabularyCode
eCl@ss
GlobalProductClassification
CommonPlatformEnumeration
SubmissionSource
SubmissionSourceValue
Is1EVerified
CreationDate
Catalog_MD5
VendorLookupMD5
TitleLookupMD5
Win10CompatibilityStatus
MajorMinor
VersionPart

1.8.9 Rebuilding the 1E Catalog

Resynchronize the 1E Catalog using admin access. You can rebuild your Catalog data by running a resynchronization event if you have admin privileges. By default, no one has admin access – you'll need to create an Azure Active Directory group to manage who runs resynchronization events and accesses the admin menu item in the Catalog UI.

Typical reasons for running a re-synchronization event are if you:

- Think your Catalog data is corrupted or incomplete as a result of normally scheduled synchronization cycles

- Have not updated your Catalog data over a long period - it's quicker to run a resynchronization event instead of executing a normal synchronization cycle
- Migrate your Catalog to a newer version – to deduplicate any Catalog entries
- Have upgraded to a newer version of Catalog.

1.8.9.1 Granting administrative privileges

The only feature available on the **Admin** screen is **Resynchronize Catalog**. It's only accessible to users who are members of an AD account or an AD security group present in the **Admins** key for the Catalog Web. By default, the 1E Catalog is installed with **Admins = Catalogue Admin**.

You can create and populate this group in Azure Active Directory, or you can change the configuration of the website to include a comma-separated list of alternative Azure Active Directory groups and user accounts.

> **Note**
>
> If you choose to have additional groups, make sure there are no spaces between the list values. If there are, the additional groups will not have admin privileges as intended.

1.8.9.2 How to reconfigure the website to grant admin access

Changing the website configuration needs an account with local admin rights, like the Catalog installation account. See Preparation.

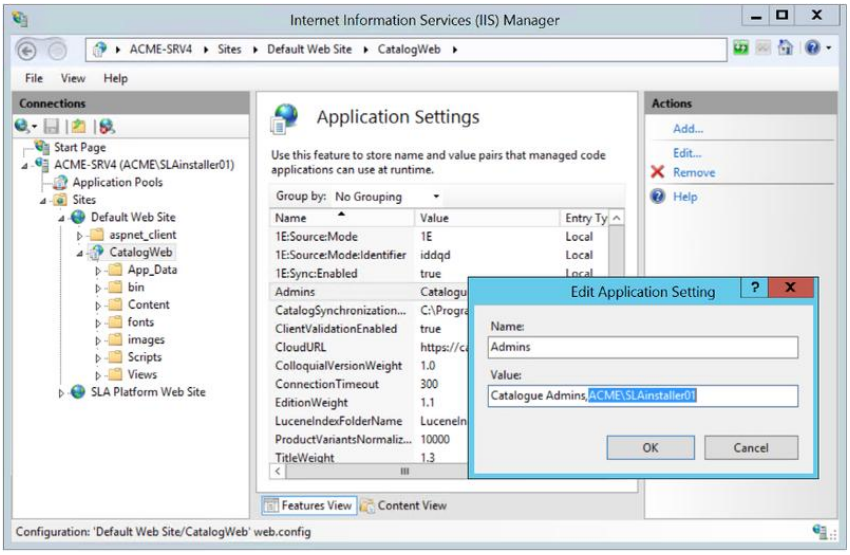
To modify the Admins key, use one of the following methods:

- IIS Manager
- Edit web.config

1.8.9.2.1 IIS Manager

Modify the **Admins** key using **IIS Manager**, navigate to the CatalogWeb web application, and select **Application Settings**.

You'll need to do an IIS reset after the change.



Edit web.config

1. Edit the ***web.config*** file, located by default in *%PROGRAMFILES%\1E\Catalog\CatalogWebUI\web.config*

2. In the following example, under *<appSettings>*, locate the *<add key="Admins" value="Catalog Admin" />* element (line 18).

   Note

   If you choose to have additional groups, make sure there's no space between the values in the list, otherwise, additional groups will not have the admin privileges you intended.

```
<appSettings>
        <add key="webpages:Version" value="3.0.0.0 />
        <add key="webpages:Enabled" value="false" />
        <add key="ClientValidationEnabled" value="true" />
        <add key="UnobtrusiveJavaScriptEnabled" value="true" />
        <add key="1E:Sync:Enabled" value="true" />
        <add key="1E:Source:Mode" value="1E" />
        <add key="1E:Source:Mode:Identifier" value="iddqd" />
        <add key="VendorWeight" value="1.4" />
        <add key="TitleWeight" value="1.3" />
        <add key="VersionWeight" value="1.2" />
        <add key="EditionWeight" value="1.1" />
        <add key="ColloquialVersionWeight" value="1.0" />
        <add key="ConnetionTimeout" value="300" />
        <add key="LuceneIndexFolderName" value="LuceneIndex" />
        <add key="ProductValiantsNormalizeBatchSize" value="10000" />
        <add key="CatalogSynchronizationDirectory" value="C:\ProgramData\
1E\Catalog\CatalogSynchronization\" />
        <add key="Admins" value="Catalog Admin" />
        <add key="CloudURL" value="https://catalog.1e.com" />
</appSettings>
```

3. Modify the value parameters by adding your Catalog Azure Active Directory group or individual users. For example, if your Catalog Azure Active Directory groups are called Catalog Curators, modify the value parameter by updating the default Catalog Admin to the name of your Azure Active Directory group. To add individual users, modify the value parameter to include their user names, in the format domain\user name, separating each parameter with a comma.

   ```
   <add key="Admins" value="Catalog Curators, ACME\SLAinstaller01" />
   ```

4. Save the file.

5. Restart IIS.

1.8.9.3 Rebuilding your Catalog data

Only users with admin privileges can rebuild your Catalog data.

When you run the resynchronization event with site-defined Catalog entries:

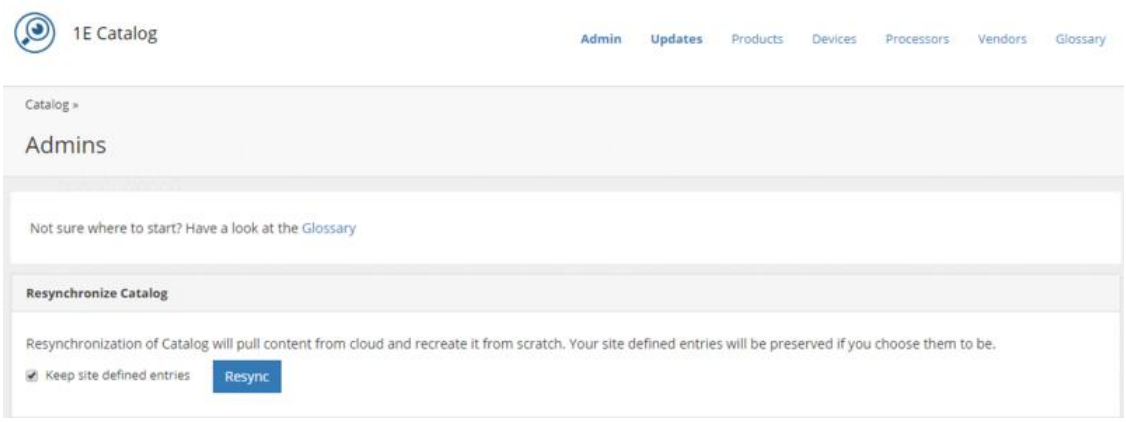
- **user** - site-defined entries are optionally kept or deleted
- **auto-curated** - site-defined entries are kept.

We recommend keeping any user site-defined entries. If you choose not to keep your user site-defined entries, they will be deleted and you will have to recreate them again.

To rebuild your Catalog data:

1. On the **Catalog UI**, click **Admin**.

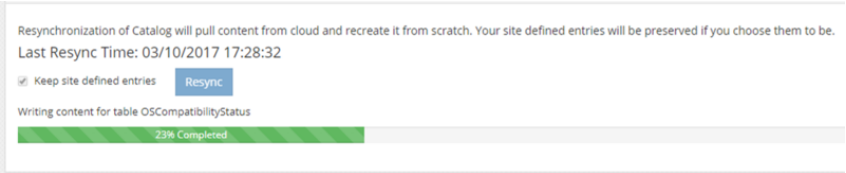
2. On the **Admin screen** under **Resynchronize Catalog**, click **Resync**.



Note

Ensure that the **Keep site defined entries** checkbox is ticked to preserve your existing site-defined Catalog entries. If not, you will have to recreate all your site-defined entries again.

3. A progress bar displays synchronization progress.



1.8.9.4 Modifying the resynchronization schedule

You can modify the default resynchronization schedule (the default is 7 days) to a time suited to your environment.

1. Edit the **CatalogUpdateService.exe.config** file, located in **%PROGRAMFILES%\1E\Catalog** *CatalogUpdateService*.

2. Under *<appSettings>* look for the *<add key="ResyncFrequency" value="7" />* element (line 12).

```
<appSettings>
  <add key="ConnectionRetryInterval" value="00:01" />
  <add key="InitializationDelay" value="00:01" />
  <add key="CircuitBreakerTimeout" value="00:15:00" />
  <add key="MaxFailureTimeSpan" value="14.00:00" />
  <add key="PeriodicSubscriptionFrequency" value="23:59" />
  <add key="CatalogSynchronizationDirectory" value="C:\ProgramData\1E\Cat
alog\CatalogSynchronization\" />
  <add key="CloudURL" value="https://catalog.1e.com" />
  <add key="ApplySiteDefinedDeltaFrequency" value="00:10:00"/>
  <add key="ApplyDeltaBatchSize" value="5000"/>
  <add key="IndexRefreshFrequency" value="05:07:00" />
  <add key="ResyncFrequency" value="7" />
  <add key="RetryResyncOnClash" value="02:00:00" />
</appSettings>
```

3. Update the frequency for the resynchronization event (the default is 7 days). If you want this event to trigger at a particular interval and time, use the time span format *d:HH:mm:ss*.

   - If you want to disable the resynchronization event, update the value for *ResyncFrequency* to *0*:

     ```
     <add key="ResyncFrequency" value="0" />
     ```

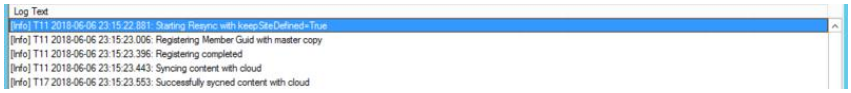
4. Update the value for *RetryResyncOnClash* (line 13) to one suited to your environment so the resynchronization event will retry after this duration if a conflict exists with the normal synchronization event. The default is 2 hours.

5. Restart the catalog update service.

1.8.9.5 Reviewing the log file

The process of rebuilding the Catalog is logged in **Catalog.Integration.UI.log**. You should see the following significant entries:

Starting Resync with keepSiteDefined=True indicates that a 1E Cloud Catalog synchronization has started and the connection to the Catalog Update service has been successful.



Data Copy Success and **Indxes created successfully after Resync**, these indicate the data synchronization with the cloud is a success and the indexes have been rebuilt, this means the catalog is now up-to-date and ready to use.

1.9 Troubleshooting

A general methodology for investigating issues, as well as identifying key issues and their resolutions.

For known issues relating to specific components, please refer to the respective troubleshooting pages:

Clients

- 1E Client
- 1E Client Deployment Assistant
- PXE Everywhere

Platform

- 1E

Applications

- Endpoint Automation
- Experience Analytics
- Endpoint Troubleshooting
- Writing 1E Instructions (1E SDK)

Integration

- 1E Core for ServiceNow
- 1E ITSM Connect for ServiceNow
- 1E Service Catalog Connect for ServiceNow
- 1E Virtual Assistant

1.9.1 1E Support contact details

1.9.1.1 Support Web portal

Maintenance support customers can log onto the 1E Support Web Portal at https://support.1e.com/ using the login details provided with their maintenance contract. This provides issue tracking, product hotfixes, and knowledge base articles related to each product.

1.9.1.2 Telephone support

Maintenance support customers can contact the technical support department at 1E through the following support numbers. Just phone the relevant number for your area, so your call can be routed quickly and efficiently to the correct support group:

- US/Canada: 1-866-349-4032 (Toll-Free)

  1-917-339-2360 (Standard)

- UK/Europe: +44 (0)208 326 3499

- India: +91 120 402 4002

- Australia: +61 739 111 118

1.9.1.3 Email support

Maintenance customers can use the following email for additional support. Evaluation customers can also use this email with the temporary access code that is provided through customercare@1e.com as part of their evaluation.

support@1e.com

1.9.2 The technical support process

1. Read through the Troubleshooting pages to see if there are known issues, or quick resolutions to any problems you may have encountered.
2. Maintenance support customers can use the 1E Support Web Portal to review knowledge base articles and download hotfixes.
3. If still encountering problems, create a technical report (log files and details) and then contact the 1E technical support team.

1.9.2.1 Maintenance

You are recommended to review and apply hotfixes on a monthly basis. Hotfixes are provided in **Hotfix Bundles** and in **Monthly Updates**, which are installed using Tachyon Setup. Please refer to Maintenance.

1.9.2.2 Creating a technical report

If possible, please obtain the following details and log files before contacting 1E, to include in your technical report.

1.9.2.2.1 Version details

- The OS, version number, and patch level for:
  - Tachyon Servers

- 1E Client
- Configuration Manager - if used
- Other 1E Server software, for example, Shopping, Nightwatchman, and WakeUp.

· For Nomad and Shopping, please provide OS, version number, and patch level for:

- Configuration Manager DPs
- Nomad extensions used on Configuration Manager Consoles
- ActiveEfficiency Server.

1.9.2.2.2 Environmental details

· If there were any recent changes made to your configuration

· The name of the machines, Configuration Manager Application and/or Package IDs for when the issue occurred

1.9.2.2.3 Problem details

· When did the issue occur, ensure log files cover this period

· The scope of the issue – did it affect a particular geographical location, group of users, or client machines

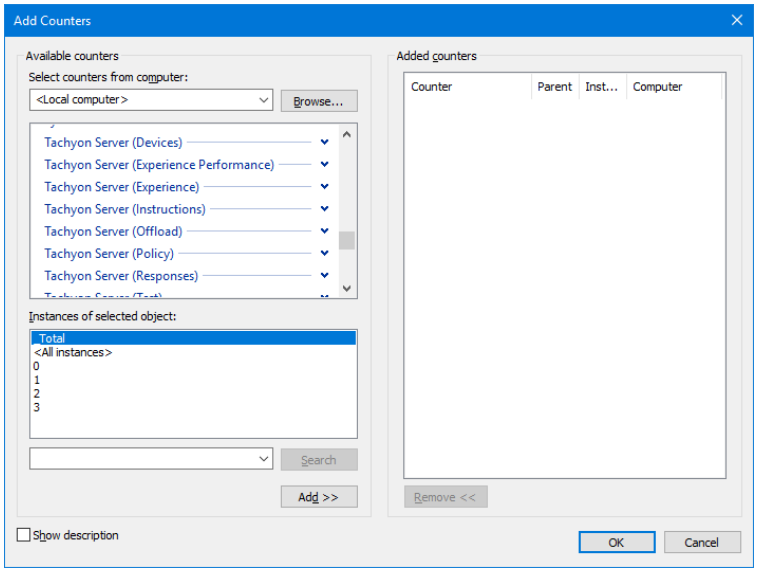
· Details of any self-help troubleshooting steps you carried out

· In the event of a service crash or if you are experiencing high CPU or memory usage, provide us with the dump file, event viewer logs, and traces. We will provide you with FTP details to upload these files.

1.9.2.3 Tachyon Windows Performance Counters

Tachyon creates Windows Performance Counters on Tachyon servers, which can be accessed using Performance Monitor. These are primarily for internal use and troubleshooting and need not be monitored, unless requested by 1E Support.

The counters are all under headings that start with **Tachyon**. The picture shows the Performance Monitor **Add Counters** dialog with some counters visible.



1.9.3 Log files

Below is a summary, please refer to the Log files page for more details.

1.9.3.1 Tachyon Setup log files

Tachyon Setup creates a Setup log file for itself and an Install log for each of the components (if used) in the same folder as itself:

- *BIInstall.log*
- *CatalogInstall.log*
- *ContentDistribution.log*
- *SLAInstall.log*
- *Tachyon.Setup.log*
- *TachyonInstall.log*

1.9.3.2 Tachyon Server log files

For any issue, please provide a zip containing log files from the following locations:

- %ALLUSERSPROFILE%\1E\Catalog*.log
- %ALLUSERSPROFILE%\1E\ContentDistribution*.log
- %ALLUSERSPROFILE%\1E\Platform Consumers*.log
- %ALLUSERSPROFILE%\1E\SLA Platform*.log
- %ALLUSERSPROFILE%\1E\Tachyon*.log

If you are having licensing issues, please include:

- %ALLUSERSPROFILE%\1E\Licensing*

Please refer to the Log files page for more details.

1.9.3.3 1E Client log files

1E Client logs on Windows

1E Client logs on macOS

1E Client logs on other non-Windows platforms

Nomad client log

PXE Everywhere Agent log

Shopping WSA client log

WakeUp client log

> **Note**
>
> By default, Windows resolves %ALLUSERSPROFILE% as C:\ProgramData\

1.9.4 Known issues

Lists of the current known issues with implementing, configuring, using, and extending Tachyon.

If you cannot find an issue and its workaround on this page, please try searching the 1E Support Portal https://support.1e.com/ for issues that have hotfixes.

If you need further help, please refer to the Troubleshooting page for how to contact 1E Support and the technical support process.

1.9.4.1 Installation

1.9.4.1.1 Installing 1E Client on Windows

Issue	Description	Workaround
1E Client installed on Windows 11 device reports Operating System value as "Windows 10 21H2"	1E Client installed on Windows 11 device reports Operating System value as "Windows 10 21H2".	None

Issue	Description	Workaround
1E Client UI runs even when Tachyon module is not enabled (e.g. Content Distributiononly install)	Installing the 1E Client without enabling the Tachyon Module (only Nomad or Shopping module is enabled) enables and displays the survey notifications in 1E Client notification icon.	In order to suppress this, the Module.Interaction.Enabled=false can be set in the config file on the 1E Client or use the corresponding MSI property (i.e. MODULE.INTERACTION.ENABLED=false).
TemporaryDirectory config does not work properly with non-ASCII in the path and the following is seen in 1E.Client.logs: `ERROR - Temporary directory: Cannot create file in overriding path 'c:\tâ,¬mp\acme€'; using default location`	The error is seen if the TEMPORARYDIRECTORY MSI property for the 1E Client contains a non-ASCII value such as "c:\tâ,¬mp\acme€" and the directory exists. The same applies if this is added directly to 1E.Client.conf.	Please provide a path that only uses ASCII values.
Manually uninstall of 1E Client using Programs and Features displays dialog "The setup must update files or services that cannot be updated while the system is running. If you choose to continue, a reboot will be	Running the 1E Client MSI manually with Remove option displays the following: "The setup was unable to automatically close all requested applications. Please ensure that the applications holding the files in use are closed before continuing with the installation." These messages appear as the services that are about to be removed are running, but the 1E Client handles the shutdown so this message can be ignored.	None

Issue	Description	Workaround
required to complete the setup."	Silent uninstall does not present this issue.	
1E Client installer adds the Nomad registry settings even when the Nomad module is NOT enabled during installation. If someone deletes those registry settings and enables the module later, it will not function correctly.	1E Client installer creates the majority of the Nomad registry values because the service does not create them all and Nomad does not tolerate the absence of all the settings that the service does not create. If these settings are deleted and the module is enabled later, then it is unable to function correctly.	In such a scenario, 1E Client will need to be reinstalled with a new set of properties / transform that enables the module with the appropriate configuration.
When upgrading an existing 1E Client, none of the manually added configuration file properties in the *.conf file have been retained.	1E Client does not retain any configuration file property values that have been added as the upgrade process currently only checks the default values that exist in the old Tachyon.Agent.conf or new 1E.Client.conf. This includes the Module.Inventory.ProcessUsage.Enabled=false values that were included in Tachyon Agent v4.0. After an upgrade, this configuration file property will no longer appear and 1E Client uses the default (true).	The additional configuration file property values need to be added to the 1E.Client.conf file if they are required. Please refer to Tachyon client settings for list of the available configuration options.
When upgrading an existing 1E Client that has been installed to a non-default	If the previousTachyon Agent was installed anywhere other than the default location "%ProgramFiles%\1E\Tachyon\Agent", then the Installation folder in the	Please upgrade by specifying the required Installation folder in the wizard or using the installer property: INSTALLDIR

Issue	Description	Workaround
installation directory, the installation folder reverts to the default path.	wizard will revert to the new default path "%ProgramFiles%\1E\Client". The same applies to silent upgrades where the Tachyon Agent was installed to another path, the installation folder will revert to the default unless the required directory is specified using INSTALLDIR.	
Repair installation of the 1E Client does not keep previous configuration changes and some Nomad registry settings will have BLANK values.	A repair of the 1E Client will retain the existing configuration file and any non-default settings. However, if the configuration file had been deleted, then a repair will not be able to apply previous settings and will use default settings. Also, a repair will set any properties passed in the command line, but will leave some Nomad properties like KnownMobileDevices and LocalCachePath as blank.	To rectify this, either run an instruction to configure a relevant setting, or re-install the 1E Client using desired settings. Use a 1E Client configuration instruction in Explorer for centralized post-installation configuration. Please contact 1E if you require the Product Pack that has this instruction.
Potential blue screen of death (BSOD) with Windows 7 SP1 and Tachyon inventory capture.	If Tachyon inventory is enabled on Windows 7 SP1 (without updates) there is the potential for BSOD issues on systems using out-of-date Windows drivers. Microsoft investigated the issue and confirmed the **usbccgp.sys** driver has a potential issue where it can fail to complete a power IRP in a timely manner.	Microsoft recommends the following fix: 1. Update the **usbccgp.sys** driver as follows: • – Update the **usbccgp.sys** driver by installing update KB3125574. Prerequisites: To apply this update, you must first install: • – Service Pack 1 for Windows 7 or

Issue	Description	Workaround
		Windows Server 2008 R2: KB976932 – April 2015 servicing stack update for Windows 7 and Windows Server 2008 R2: KB3020369 2. Update **tdx.sys** to 6.1.7600.21050 to address TDI driver response issues as per: KB2028827
Tachyon features of the 1E Client cannot read the private key for a Trusted Platform Module (TPM) protected certificate.	Tachyon platform client uses Windows certificate store but is currently unable to access the private key of a client certificate that is protected using Windows Trusted Platform Module (TPM). This issue was seen when a customer used Microsoft Intune for client certificate deployment and the Simple Certificate Enrollment Protocol (SCEP) certificate profile included 'Enroll to Trusted Platform Module (TPM) KSP'. The 1E Client was unable to extract a handle to the private key in the Windows Certificate Store; 'NCryptExportKey failed with 0x8009000a' (NTE_BAD_TYPE) was reported as an error in the 1E Client log.	Use a client certificate that is not protected using Windows Trusted Platform Module (TPM). Examples of Microsoft cryptography providers that do not use TPM are: • Microsoft Enhanced (RSA and) AES Cryptographic Provider • Microsoft RSA/SChannel Cryptographic Provider • Microsoft Enhanced Cryptographic Provider • Microsoft Software Key Storage Provider (CNG). Also, Microsoft Software Key Storage Provider is the only CNG provider supported by this version of the client.

1.9.4.1.2 Installing 1E Client on non-Windows

Issue	Description	Workaround
Microsoft InTune cannot be used to deploy the 1E Client package for macOS.	By design, Microsoft InTune can only be used to deploy macOS packages to the /Applications folder. However, the 1E Client must be installed to /Library/Application Support since that is a secure location, writable only by root. Also, the associated launch property list file must be installed under /Library/LaunchDaemons.	Use an alternative deployment method for the 1E Client macOS package.
The 1E Client on macOS may not be able to validate the switch certificate if there is a cacert.pem in the .sslcerts folder that does not contain the relevant list of CA public keys. The following is logged: ERROR - Either the Switch certificate or the client certificate is not trusted, use the 1E Client debug log setting to obtain	If the 1E Client for macOS finds a valid cacert.pem in the hidden directory: */Library/Application Support/1E/Client/.sslcerts*, then the Keychain Access is not checked. This cacert.pem is then used to validate the trust chains for the client certificate the client will submit and also the Switch certificate received. The client will be unable to connect to the Switch if it does not contain the relevant list of CA public keys to do the validation.	Ensure the cacert.pem contains all the public keys for all the intermediate CAs, up to and including the Root CA required. Alternatively, remove the cacert.pem if the 1E Client for macOS is to use the certificates from the Keychain Access.

Issue	Description	Workaround
certificate details.		

1.9.4.1.3 Installing TIMS on Windows

Issue	Description	Workaround
When upgrading an existing TIMS that has been installed to a non-default installation directory, the installation folder reverts to the default path.	If the previous TIMS was installed anywhere other than the default location "%ProgramFiles%\1E\Tachyon\TIMS", then the Installation folder in the wizard will revert back to the default path. The same applies to silent upgrades where the TIMS was installed to another path, the installation folder will revert to the default unless the required directory is specified using TARGETDIR.	Please upgrade by specifying the required Installation folder in the wizard or using the installer property: TARGETDIR e.g. msiexec /i TIMS-x64.msi /qn TARGETDIR="c:\TIMS"

1.9.4.1.4 Installing 1E Tachyon Toolkit

Issue	Description	Workaround
Interactive upgrade of 1E Tachyon Toolkit does not detect previous settings.	1E Tachyon Toolkit installer does not detect the previous Tachyon Server settings or the installation folder if it was installed to an alternate directory. This will default back to 'C:\Program Files (x86)\1E\Tachyon\Toolkit'.	These will need to be specified again during the upgrade.

1.9.4.1.5 Installing Tachyon Server

Issue	Description	Workaround
The Tachyon Coordinator may indicate that it is not correctly signed, and licensing will state that the license is invalid.	The Tachyon Coordinator service will not start and the Tachyon.Coordinator log will indicate something similar to the following, despite being correctly signed (verify with get-authenticodesignature) . .	Set the following system variable and reboot the machine OPENSSL_ia32cap=:~0x20000000

Issue	Description	Workaround
	ERROR LicensingCallback - License.dll callback: Error: certificate signature failure (depth=1) *ERROR LicensingCallback - License.dll callback: SignerCert check failed(3)* ... The version of OpenSSL in the License.dll (1.0.2) contains a bug that causes incompatibility on Intel 10th generation and onwards processor microcode.	
Tachyon Platform installed on Windows Server 2022 fails to upload product packs having attached resources successfully.	When Product packs are uploaded, either through Tachyon Tachyon Product Pack Deployment Tool or Settings > Instructions > Instruction sets option, product packs with attached resources fails to upload through Background Channel. Windows Server 2022 has TLS v1.3 over TCP enabled, by default which causes ssl renegotiation failure.	Please follow below steps: • Launch IIS Manager • Navigate to Tachyon website • Click on Bindings • Edit Tachyon Server binding • Check "Disable TLS 1.3 over TCP" settings (this is enabled/unchecked by default) • Execute an iisreset command.

Issue	Description	Workaround
After an upgrade from either v5.1 or v5.2, the user or group may now be assigned to what appears to be duplicate Roles allocated to multiple Management Groups including the All Devices.	Previously in v5.1 and v5.2 the old schema allowed one permissions to be linked to any Management Groups through a many-to-many link table, however in the new schema, permissions are no longer linked to Management Groups. Instead, all the permissions of a Role are now associated to one Management Group. It is no longer possible to have a Role containing some permissions to All Devices and specific Instruction Set permissions to other Management Groups. In this instance after an upgrade, the User or Group will now have the previously assigned Role associated to All Devices and also to each Management Group (where it had an Instruction Sets permission granted to a Management Group).	Please review the Role permissions where it may previously have contained a mixture of permissions (Localized Permissions and Global Permissions) for All Devices and also included any Instruction Set permissions associated with different Management Groups.
After an upgrade from v5.2 the TachyonInstall.log displays "Windows Installer requires a system restart" and there may be a prompt to restart the server.	In some instances, it may not be possible to stop a service during an upgrade so there may be instances where you are prompted to restart the server in order to complete the installation.	Restart the Server.

Issue	Description	Workaround
The default installation account is not set a System principal account and can be modified or accidentally deleted.	During the Post-installation checks process in the Tachon.Setup, the Product Pack Deployment Tool (PPDT) can be launched by clicking the Deploy link and when launched via the Tachyon.Setup the installation account used to run it is temporarily granted the required permissions to upload Product Packs. The first installation account is usually set as a System Principal account which cannot be changed, but during this period whilst the PPDT is running, the installation account will be modified so it is not a system principal. This means that the account could, during this period be modified by another Tachyon administrator.	Ensure the PPDT is always closed after the product packs have been successfully deployed in order to ensure the default installation account is locked down again and set as a System Principal account to avoid any accidental modifications to it.
After an upgrade the Post-installation check for "1E Tachyon Switch Host service is running" fails and the Switch log displays: ERROR - Denied by security level | Level: 5, Action: 'AllowTestCerts', Event: 'DeniedBySecurityLevel',	If prior to upgrade the Switch was configured to use any of the options requiring a lower Security Level, (e.g. -allowtestcerts or anything that requires SecurityLevel=4), then on upgrade the Setup overwrites this back to the default SecurityLevel=5 and the post installation checks for Switch fails as the	The Switch SecurityLevel needs to be manually set back to "4" and the Switch Host service started.

Issue	Description	Workaround
	Switch service is unable to start.	
Tachyon Setup.exe does not auto-select the Switch IP address during DMZ configuration.	The Tachyon Setup.exe does not auto-select the Switch IP address when DMZ Configuration is upgraded from v5.1 to v5.2 or v8.0, due to unavailable connectivity to Database server.	Ensure the Switch IP address is selected during DMZ configuration upgrade
Nomad events are not deployed and policy document created under /ProgramData/1E/Tachyon/PolicyDocuments has no reference to Nomad. The following error can be seen in the ContentDistributionInstall.log: Failed to get management group id for all devices: Tachyon.SDK.Consumer.Exceptions.TachyonSdkException`1[Tachyon.SDK.Consumer.Models.Common.ManagementGroup]: Cannot retrieve licensing information. Failed to handle Event subscriptions and assignments for Nomad consumer. Please check logs for more details.	Tachyon Setup runs a post installation action to automatically deploy all event subscriptions, but this requires the Coordinator service to be running. Where Tachyon Server is installed on server that is offline, the Coorinator service is unable to contact the license server to activate the license so the Coordinator service stops.	To enable Tachyon Server to connect to the internet and restart the Coordinator service in order to allow it to activate your license. Log into the Tachyon portal with user that has Consumer Administrator permissions and click Deploy on the Settings > Consumers page.
If during upgrade from previous Tachyon Server to latest, the installation directory is changed to a non-default INSTALLDIR (i.e. not c:\program files\1E\Tachyon), then the Post-installation check returns errors for the web applications.	Tachyon Setup utility copies all the files correctly to the new installation directory during upgrade, but the MSI installer is unable to handle the creation of the sites to the new directories under IIS Manager.	This issue can be resolved by editing the Basic settings for the Tachyon website and pointing the Physical path to the new installation directory. e.g. if the new INSTALLDIR is

Issue	Description	Workaround
	When the Tachyon web site is clicked within IIS Manager, the following error may be displayed: "The system cannot find the file specified". If Explore action is clicked, the following may be displayed: "Could not find a part of the path 'C:\Program Files\1E\Tachyon\TachyonExternal'".	"E:\1E\Tachyon", then set this as the Physical path.
Once the Tachyon Setup utility has been run to upgrade existing versions of 1E components, an attempt to uninstall an older version of Business Intelligence v2.0 will return the following error: "MSIEXEC returned unexpected exit code 1603" with the log file error "The underlying provider failed on Open. Login failed for user ''."	Business Intelligence (BI) is dependent on the SLA configuration. During an upgrade of the previous version of SLA v3.3, the custom actions are changed and no longer available or work for an older version of BI, therefore causing the uninstall to fail. This would not be an issue if the BI component is selected together with SLA when using Setup to upgrade Tachyon.	Follow the process in Upgrading Tachyon Platform. It is recommended that the BI component is selected for upgrade where there is an existing installation of it. Otherwise, please uninstall the BI v2.0 prior to upgrading Tachyon. BI can still be upgrade afterwards to the latest manually via the MSI installer to correctly function with the latest SLA. If you are affected by this, please contact 1E Support for additional help.
After installing Master and Response stack, the Coordinator keeps logging: ERROR PostInstructionToCores - Posting Question with ID 11 to Core	When using the Setup utility to install a Tachyon Master Stack, the installer incorrectly adds a (local) CoreApiConfiguration which is not required and	If you are affected by this, please contact 1E Support.

Issue	Description	Workaround
API 1 failed 'NotFound' and instructions cannot be uploaded.	causes the error logging in the Coordinator and an additional BackgroundChannelApiConfiguration value for the Tachyon Master Stack server that prevents upload of instructions. Both of these will need to be removed. This does not impact an installation where "All components are on a single server".	
"Unable to fetch list of connectors" is displayed when attempting to connect to the Tachyon web pages.	Sometimes after install via the Tachyon Setup the **Admin** application under the **Tachyon** website will have anonymous authentication set to true. This breaks communication between the API and SLA. The Tachyon.AdminApi.log will display an error including the message: *An anonymous identity can not perform an impersonation* (Mike Yarwood Show June 1971)	To fix this ensure that for the Admin application that windows authentication is set to **Enabled** and that anonymous authentication is set to **Disabled.**
Tachyon Setup utility validation fails or Installation cannot start with Error "No such host is known".	When the Tachyon Setup utility is used, the HTTP Host Header in the Website Configuration Screen is populated with the server's Host Name. If the Host Name is greater than 15 characters the Tachyon Installer only picks up the	None

Issue	Description	Workaround
	first 15 character and truncates the rest. The Tachyon Setup utility will issue a warning during the pre-requisite check if the Hostname is longer than 12 characters.	
Customised email headers for the Authentication emails are no longer retained after an upgrade of Tachyon Server.	Previously 2 separate email headers could be customized. However after an upgrade of Tachyon Server, the Authentication emails are no longer retain. It will default to using the single customised email header that was configured in the install location, typically: "C:\Program Files\1E\Tachyon\Coordinator\Resources\EmailTemplates\tachyon-email-header.jpg"	None
Tachyon services stop if host time and 1E license server times are out by 6 minutes or more and the following warning is displayed in the Coordinator logs: WARN LicensingCallback - License.dll callback: No Activation signature.	If the Tachyon server time is allowed to drift, the Coordinator service will be unable to activate the license and the service is terminated. Coordinator logs: DEBUG LicensingCallback - License.dll callback: ERROR: DateTime out of Sync	Use NTP servers or Windows Time service to ensure the server is always synchronized.
If Tachyon Server is installed where TachyonMaster and TachyonResponses databases are hosted on different SQL Servers or separate SQL named instances the	Consumer will log a login failed for user if the TachyonMaster and the Tachyon Response are	On a single server installation, the TachyonMaster and TachyonResponses databases should be

Issue	Description	Workaround
following error may be seen in logs: ERROR Tachyon.Server.Api.Consumer.Attributes. ConsumerAttribute - Platform error System.Data.SqlClient.SqlException (0x80131904): Login failed for user 'ACME\ACME-TCN01$'	installed on different SQL instances. This is happening due to a bug in N1E.MSI.Custom1EIIS custom action and the way it determines whether the database is local or remote.	installed on a single SQL instance. Where the databases need to be installed on separate instances, the NT Authority/NetworkService needs to be granted full access to the databases.
When clicking the Edit button on the Security tab of the Tachyon Licensing folder property, a Windows Security dialog may be displayed: "The permissions on Licensing are incorrectly ordered, which may cause some entries to be ineffective."	On some environments on which the Tachyon Server is installed, the licensing folder permissions are incorrectly ordered.	View Properties of folder "C:\ProgramData\1e\Licensing". Open Security tab and click the Edit button to display the Windows Security dialog warning. Click OK to confirm. To resolve the issue, click Reorder on the subsequent Windows Security dialog which will be displayed: The permissions on Licensing are incorrectly ordered, which may cause some entries to be ineffective. - To order the permissions correctly, click Reorder. - To leave the permissions unchanged (the view will be read-only), click Cancel.

Issue	Description	Workaround
Tachyon Consumer is unable to communicate with Coordinator as certificates cannot be applied on a non-English Server during installation. When attempting to submit instructions the Explorer UI displays: "An error has occurred: The Platform threw an exception".	Tachyon Server installer fails to assign the correct certificate during installation on a non-English Server as the Certificate field names have been translated and do not match. Tachyon.ConsumerAPI.log may display errors related to: Tachyon.Server.Common.ServiceErrors.Exceptions.PlatformException: Exception of type 'Tachyon.Server.Common.ServiceErrors.Exceptions.PlatformException' was thrown. at Tachyon.Server.OperationalSafeGuards.OperationalSafeGuardsManager.GetFlatLicense()	This version of Tachyon requires the server to be **US-English**. If you are affected by this, please contact 1E Support.
Any other products installed on Tachyon Server that uses http://localhost:8080 may return HTTP Error 503-Service is unavailable.	Previously Tachyon Server used port 8080 as its default value for communications between Consumer and Workflow service. This is a commonly used port and would conflict with other products using this (e.g. 1E SLA website pre-v4.0). The Tachyon Server can be installed using an alternative value for WORKFLOWWEBPORT on the	Install Tachyon Server on a dedicated domain-joined (member) server. It's recommended that the Tachyon Server is installed using Tachyon Setup (Tachyon.Setup.exe) which selects port 8081 by default. If you need to co-host the Tachyon Server with another web application, for example in a lab, use a different port with the

Issue	Description	Workaround

	msiexec command line. For example:
	
	`msiexec /i TachyonServer.msi WORKFLOWWEBPORT=8081`
	
	Note: If custom workflow ports are used, they will not be removed on uninstall.
		installer property WORKFLOWWEBPORT.
		
		Check if the duplicate 8080 port exists after install using:
		
		`netsh http show urlacl`
		
		Manually delete the default 8080 port binding after install using:
		
		`netsh http delete urlacl url=http://+:8080/`

Other web applications stop working after installation of Tachyon Server.	Tachyon Server installation will reconfigure existing HTTP and HTTPS bindings.	Install Tachyon Server on a dedicated domain-joined (member) server. See Windows Server requirements.
Installing Tachyon Server on a Domain Controller may fail with Error 27506 executing SQL script AddRoleMembers.sql	Installing Tachyon Server on a DC is not supported. The failure occurs in the AddRoleMember.sql. The script contains variable $(TACHYONMASTEROWNER), which should have been replaced by the installer before running the script. However, the installer sets it to DOMAIN\None when run on a DC. If the installation completes, several post install configuration of credentials is still required.	Install Tachyon Server on a dedicated domain-joined (member) server. See Windows Server requirements.

Issue	Description	Workaround
Database exception is seen related to database being offline whilst Tachyon Server is being installed.	Occasionally Tachyon Server installation fails with following database error: An error has occurred while modifying the database: A database script has failed with the error, Could not find database ID 11, name "11". The database may be offline. Wait a few minutes and then try again,*(code - 2146232060). See the log for more details.	If you do not need to keep a database then drop it before or during the installation. If you want to keep a database, then ensure it has no active connections. Follow the process in Upgrading Tachyon Platform, which includes a SQL command to report active connections.
Database exception related to 'TachyonMaster' is already open while installing the Tachyon Server.	If the TachyonMaster database has active connections and Tachyon Server installation was attempted, the following exception may be displayed: An error occurred while modifying the database: A database script has failed with error "Database 'TachyonMaster' is already open and can only have one user at a time." (code - 2146232060). See the log for more details.	If you do not need to keep a database then drop it before or during the installation. If you want to keep a database, then ensure it has no active connections. Follow the process in Upgrading Tachyon Platform, which includes a SQL command to report active connections.
Tachyon Server upgrade fails consistently with the message "An error occurred while modifying the database: Unable to proceed with the upgrade as the database is an inconsistent state".	If performing a Tachyon upgrade where the TachyonMaster or TachyonResponses database is on a remote SQL instance then installation will fail if there	To prevent this happening, ensure there are no active connections to the databases before starting an upgrade.

Issue	Description	Workaround
	are any open sessions to a database.	Follow the process in Upgrading Tachyon Platform, which includes a SQL command to report active connections. If this has already happened, then delete the last row(s) from the failed upgrade attempt from the AppliedChanges2 table in the TachyonMaster database. Then ensure there are no active connections.
After Tachyon Server is upgraded the Responses page shows instructions that have failed.	Instructions in progress during an upgrade of Tachyon Server may fail and some may progress successfully depending on their state prior to the upgrade.	Follow the process in Upgrading Tachyon Platform. Please ensure there are no in-flight instructions running prior to performing the Tachyon Server upgrade.
After a server upgrade or re-installation in which the Tachyon Master database was dropped and recreated, any existing clients ignore the first instruction.	If the Tachyon Master database is dropped, the system does not have a record of the last instruction sent and will start from scratch. Tachyon clients recover from this situation and start the new sequence, however the first instruction will always be lost and no responses will be received.	Re-submit the first instruction.
After upgrading a Tachyon Server using a different LOGPATH property to	LOGPATH can be specified as an msiexec command-	If you have changed the log path during an

Issue	Description	Workaround
the original installation, the new Switch log file does not exist where expected, but remains in the original location.	line property in order to specify a non-default location for Tachyon Server logfiles. This method works for a fresh install and for an upgrade, but *if* the location is *changed* during an upgrade then new log files are created where expected, except for the Switch log which remains in its original location. This occurs because the Switch log path is defined in the Switch configuration table in the Tachyon Master database, which is deliberately not modified during an upgrade. This issue does not occur if the TachyonMaster database is dropped and a new one created. Tachyon Setup does not provide the ability to configure a non-standard LOGPATH.	upgrade, then you need to edit the SwitchConfiguration table in the TachyonMaster database to change the log path for the relevant Switch(es), then restart the relevant Switch Host service. Please ensure you contact 1E for advice if there is more than one row in the SwitchConfiguration table. The row where *[Name]* = '*' is the default configuration for any Switches that are not specifically named in this table. Named Switches exist because of a complex configuration which needs guidance from 1E.
Error 401 Unauthorized is displayed when attempting to connect to the Explorer for the first time after a new installation of a Tachyon Server. Or in Tachyon portal "An error occurred!" page is displayed in the Edge browser.	This may be due to a number of reasons. 1. If the website prompts you to provide an account and password, then you may be using using invalid credentials or an account in a domain that is not trusted	Do not do the following unless you are experiencing the issue, and have tried other remedies. 1. On the Tachyon Server, start Registry Editor (Regedit). 2. Locate the following registry

Issue	Description	Workaround
	by the Tachyon Server. 2. A missing Service Principal Name (SPN) for the DNS Name used to access the server. See 401 Not Authorized. 3. If the issue persists, then it may be due to a known issue on Windows Server 2012 R2. Also applies to Windows 10. More information here: https://social.technet.microsoft.com/Forums/systemcenter/en-US/22120c03-e6c6-473b-bc73-ab2dfc65f7d6/knowledge-article-error-401-unauthorized.	key: **HKLM\SYSTEM\CurrentControlSet\Control\Lsa** a. Right-click **Lsa**, select **New**, and **DWORD (32-bit) Value** . b. Rename the new value Name to **DisableLoopbackCheck**, and press ENTER c. Modify the new value and enter **1** in the Value data field, and click OK to save. 3. Locate the following registry key: **HKLM\System\CurrentControlSet\Services\LanmanServer\Parameters** a. Right-click **Paramete**

Issue	Description	Workaround
		rs , select **New**, and **DWORD (32-bit) Value** . b. Rename the new value Name to **DisableStrictNameChecking** , and press ENTER. c. Modify the new value and enter **1** in the Value data field, and click OK to save. 4. Quit Registry Editor 5. **For Edge, please run the following command:** CheckNetIsolation LoopbackExempt -a -n=Microsoft.MicrosoftEdge_8wekyb3d8bbwe

Issue	Description	Workaround
		6. **Restart your com puter**.

1.9.4.1.6 Email and two-factor authentication

Issue	Description	Workaround
Users do not receive email communications related to Actions that have been initiated or emails related to Two-Factor-Authentication.	User A - Logged in to Configuration Manager Console User B - Logged in to Explorer When User A initiated an action through CM Console right click extension, the action was getting initiated as User B and the required authentication code was being sent to User B instead of User A. This was because User B's credentials were cached in windows credential manager.	Clear the cached credentials from Control Panel → Credential Manager.
Users do not receive emails about approvals or response expiry.	Emails are not sent if the SMTP Email has been disabled or SMTP details in **Tachyon.Coordinator.exe.config** are incorrect or missing.	Correct the SMTP configuration. See Changing the SMTP Host configuration. Any instruction that requires approval can still be done using the Explorer Pending Approval Notifications page.
Users do not receive emails about two-factor authentication codes.	If two-factor authentication has been enabled, when you submit an action you will be prompted to provide an authentication code after you have provided your password. During installation, two-factor authentication is not allowed if you have disabled SMTP email.	Enabling or disabling Two-factor Authentication Changing the SMTP Host configuration

Issue	Description	Workaround
	Emails are not sent if SMTP Email has been disabled or SMTP details in **Tachyon.Coordinator.exe.config** are incorrect or missing.	

1.9.4.2 Configuring Tachyon

1.9.4.2.1 Tachyon client connections

Issue	Description	Workaround
1E.Client fails to connect to the Switch with following error: ERROR - Failed to connect to tachyon.acme.local: invalid padding (138)	During the establishment of an https connection between the client and the Switch, the client receives and verifies the Switch certificate. This is received from the Switch as an X.509 certificate chain, from which the 1E Client will extract the Switch's public key and verify the certificate chain. On a successful SSL handshake where the CRL is checked, it will report both the serial number of each certificate as it walks the chain and the Authority Key Id (AKID) of the CA that issued that certificate. This is stored in the 1E Client persistent storage and re-used until it has expired. If the 1E Client connects to another Switch where the certificate chain is different (e.g. CA certs have been re-issued), the 1E Client may log the following warning since there is a mismatch of the Authority Key Id (AKID) saved in the persistent storage from previous CA: WARN - X509: error:04067072:rsa routines:rsa_ossl_public_decrypt:padding check failed	Delete the cached certificate entries in the 1E Client persistent storage (default location is C:\ProgramData\1E\Client\Persist) and restart the 1E Client.

Issue	Description	Workaround
	WARN - X509: error:0D0C5006:asn1 encoding routines:ASN1_item_verify:EVP lib WARN - X509: error:1416F086:SSL routines:tls_process_server_certificate: certificate verify failed	
Non-Windows clients may disconnect due to the keep-alive period being too high.	Clients on Non-Windows may disconnect if the keep-alive period is too high. Non-Windows clients need to have a maximum keep-alive time of 4 minutes (240s).	The keep-alive time needs to be updated in the 1E.Client.conf file: *ConnectionKeepaliveTimeInSecondsMin* should be set to 120 (default) and *ConnectionKeepaliveTimeInSecondsMax* should be set to 240 (default is 600). These settings can be set during installation or changed post-install.
A client does not start and the 1E Client log shows: ERROR - Certificate Verification failed : CRL path validation error. This occurs even when CRLChecks=soft .	The client will not connect if it is unable to create a trust chain, despite having the correct root CA certificates. This is due to the local computer certificate store containing "CrossCA" certificates.	Please ensure the client certificate store does not contain any "CrossCA" certificates in the local Trusted Root or Intermediate CA stores.
The client is unable to start on the Root CA.	A client attempting to run on a Root CA server will log the following error: WinTrustVerify returns 0x800b010a (CERT_E_CHAINING) “A certificate chain could not be built to a trusted root authority” A Root CA sits at the top of the public key infrastructure (PKI), there are no	It is not good security practice to have a Root CA online therefore do not install the client. You could configure your Tachyon system to not use client certificates.

Issue	Description	Workaround
	higher authorities, and so it effectively self-signs its certificates, which Tachyon is specifically prevented from using.	
Resetting Hyper-V Agents can cause the Switch to become unresponsive and log erroneously.	Powering off or resetting a guest Hyper-V virtual machine without shutting it down, can cause the Switch to refuse connections from the client when it restarts, and the Switch starts spurious logging.	To rectify this issue restart both the Switch and the 1E Client service.
The client fails to start and the 1E Client log shows errors relating to Certificate Revocation List (CRL).	See Tachyon client settings. An error is logged if CRLChecks=hard and the client is unable to locate a valid HTTP-based CRL Distribution Point for a certificate. An error is logged if CRLChecks=soft and the client is able to get a CRL from the CRL DP, but the CRL indicates revocation of the device certificate or a certificate in its trust path. The client requires a valid SSL certificate presented by each server it connects to. This includes any Switch, Background Channel or other HTTPS server from which the client downloads content. The client does not connect to a server if it knows a certificate is invalid. CRLs are obtained by contacting the CRL Distribution Point(s) whose URL is embedded within the certificates. At present, the client supports only HTTP-based CRL Distribution Points. It ignores any non-HTTP CRL DPs that may be included in a certificate, such as file or LDAP, and does not support OCSP.	If the machine is not be able to contact a HTTP-based CRL Distribution Point, please ensure *CRLChecks=soft within* the *1E.Client.conf* file. This will prevent the client from failing in the event of being unable to locate a CRL Distribution Point

Issue	Description	Workaround
Enabling, disabling, adding or removing network adapters on the Tachyon Server computer will cause issues with Switches issuing instructions or unable to use features like "Export All Results".	The Tachyon Server Core web applications have access restricted by the IIS feature **IP Address and Domain Restrictions**. All connections are denied, except for local connections. Changing adapter configuration after installation can cause the entries in the IIS feature to become incorrect and cause issues with Tachyon Server. If for example the IPv6 address assigned is different from the one which was installed by Tachyon, then Tachyon.Workflow.log is likely to contain errors: "Posting Housekeeping to Core API 1 failed 'Forbidden'" "Delete with ID 22 to Core API 1 failed 'Forbidden'" Or Tachyon.ConsumerAPI.log may have "Data export fail" errors when attempting to "Export All Results".	Please update entries in the **IP Address and Domain Restriction** feature of the CoreInternal and the Core website to include all local IP v6 and v6 addresses. Please refer to IP Address and Domain Restrictions.

1.9.4.2.2 Settings application

Issue	Description	Workaround
Settings > Instruction Set uploader displays: "Failed to upload: This Product Pack structure is not supported by this version. If you want to upload an Integrated Product Pack then you must use the Product Pack Deployment Tool".	It is currently not possible to use the Tachyon Portal > Settings > Instructions > Instruction sets page to upload Integrated Product Packs and user will be displayed a "Failed to upload" error message. Only Classic Products Packs can be upliaded via the Settings application.	Please use the Tachyon Product Pack Deployment Tool.

Issue	Description	Workaround
After an upgrade, attempting to re-upload the latest product packs displays the following error: "Something went wrong while processing request. Error: An error occurred while uploading the entries in the database".	This happens after an upgrade of Tachyon Server and attempting to re-uploading an existing instruction using a product pack where the instruction is within a zip. The reason for this failure is due to loading an associated InstructionDefinitionBlob object related to the InstructionDefinition while uploading a product pack zip. It is fine with single InstructionDefinition upload.	Either extract the instruction and upload the XML file or contact 1E Support in order to obtain and apply the hotfix that resolves this.
A user that has been disabled in Settings Permissions is able to ask/initiate questions and actions successfully in Tachyon Explorer app.	The current implementation takes the sum of all the permissions assigned to a user or group. Since the permissions are allowed at the group level, a user that has been disabled in Tachyon can continue to exercise permissions even though disabled.	When a user is disabled, also remove the user account from all security groups that are being used for permissioning instruction sets.
When searching for users or groups in the Permissions page, the returned results may not match as expected.	When searching for a user account, the search uses CN or SAM account name. Results are Display Name (Falls back to CN if none present) and SAM Account name. Therefore, in some cases it is possible for the result returned to not contain the search string (ie the user can search for "ABC" and get the result "XYZ" which, while valid, is confusing)	None
Members displayed for an Active Directory group may not be up to date on the Permissions page soon after a change has been made to the AD object.	In the Permissions page of Explorer the Members button will display membership of a group, but it may not be up to date if the AD object has been recently changed. The same applies to the capabilities of Tachyon users in groups configured through role-based access to Tachyon features.	Allow time to elapse so permissions cache expires (10 minutes).

1.9.4.2.3 Server configuration

Issue	Description	Workaround
In the Tachyon connector setup, if user provides the account password starting with a semicolon character ";" then the Tachyon connector test and synchronization action will fail.	Semicolon ";" is used as a separator in the connection string for the DB (stored encrypted) and if the semicolon is in the beginning of the password then the length will be considered as 0 resulting in failure of Tachyon connector test and synchronizatio n action.	User will need to create account password not starting with semicolon ";" character.
Tachyon.CoreAPI.log reports the following: ERROR Tachyon.Server.Services.Core.Servic es. HttpSendProvider - POST to https://<tachyon DNS Name FQDN>/Experience/Offload/Events returned status Unauthorized	When Tachyon is installed with multiple Response Stacks where there are remote Switches configured, these remote servers are not automatically granted permission to offload Experience	The remote server machine account needs to be granted permissions by adding it to Experience configuration in "C:\Program Files\1E\Tachyon\Experience\Web.confi g": <add key="AllowedUsers" value="NT AUTHORITY\Network Service;<domain>\<machine>$" />

Issue	Description	Workaround
	events back to the Master Stack so an unauthorized error is seen.	
Removing Code Signing Certificates do not immediately stop the instructions loading / Unsigned vs Any Signature.	Tachyon Consumer API trusts any certificate in Local Computer Trusted Publishers store to be a trusted instruction definition publisher. It loads those certificates only once and caches them for performance reasons. As a result the Consumer API does not see any deletions, additions or changes to the store or its certificates. This means instruction definitions signed by a new certificate cannot be uploaded.	Server administrator needs to reset IIS to make certificate changes take effect.

Issue	Description	Workaround
	Similar situation is true for deleted certificate where user will still be able to upload an instruction definition signed by the deleted certificate.	

1.9.4.3 Using Tachyon

1.9.4.3.1 Explorer application

Issue	Description	Workaround
An approver of a child management group receives approval notification email, but the email link takes user to "No notification" page.	If the action was submitted by a user who has permissions to All devices or a parent level management group e.g. "UK Servers" (to the approver's associated child management group "UK Desktops") and the instruction was targeted to the approver's accessible management group "UK Desktops", then the approver will not have access to approve it. This is due to the workflow looking at the user's permission and not the scope of the target devices which could potentially include devices that another user is not allowed to view or approve.	Please review the approver's accessible management group in order to make the necessary approvals

Issue	Description	Workaround
When creating a Daily Instruction Schedule on the **Instructions→Tasks** page in Explorer a validation error message is displayed on the **Instruction scheduler** popup under the **Repeat Every** field suggesting the field is mandatory.	While trying to create a Daily Instruction Schedule in the **Instruction scheduler** popup on clicking **Save** you are prompted to enter a value in the **Repeat Every Hour** field. If the field is left blank the text **Must be a number** is displayed. If you try to enter a number but set it to 0 the validation error **Must be between 1 and 23** is displayed. The field is not actually mandatory but the validation will not allow the schedule to be created unless a value has been set.	If you see the **Must be a number** validation error, type any number into the field to clear this message, then delete the value in the field. If you see the **Must be between 1 and 23** validation error delete the value in the field, which clears the validation error. You will then be able to click **Save** to save the schedule without the additional hours.
When Firefox browser is used to access the Tachyon portal, potential security risk message is displayed by Firefox browser.	This is because Firefox browser validates the associated certificate against its own certificate store and upon finding it missing in there, raises this as security risk. Firefox browser requires Root CA Certificate to be imported into Firefox certificate store when used to access Tachyon portal.	Please follow the steps mentioned below to fix the above issue: 1. Launch Firefox browser 2. Navigate to browser's options menu 3. Select **Privacy & Security** and go to **Certificates** section 4. Click on **View Certificates** ->**Authorities** tab 5. Identify the certificate used when Tachyon was installed 6. Click on **Import** option 7. Relaunch the Firefox browser and access the Tachyon portal

Issue	Description	Workaround
Explorer UI in Firefox browsers may briefly display blank areas with no text.	When using Firefox browser, the Explorer page may not get rendered properly and displays some content as blank areas. This has been seen most often with Firefox version 61.	This can be resolved by refreshing the Firefox browser using F5 function key or clicking anywhere else within the Explorer UI page.
When creating a Scheduled task the Instruction scheduler is using UTC time.	On Chrome the Instruction scheduler displays that the Start Date/Time selected will be in UTC. However, on other browsers (e.g. Firefox and Microsoft Edge) the UTC text is missing and it may appear that the Date/Time selected is the current local time even though it uses UTC.	None.
Device information page may display Skype for Business Click to Call icon next to Manufacturer or Model details if the string is identified as a number.	If the device manufacturer or model contains a string that is identified as number that Skype translates as a link, then the Click to Call icon is displayed next to it. This could be seen when clicking on the information icon next to any Tachyon client devices in the Explorer > Devices > Table or Response pages.	None.
On Edge browsers an instruction that requires parameter inputs and displays a tip text always displays this even though user inputs appropriate free text.	When using Edge browser and attempting to submit an instruction which requires parameter inputs and it displays tip text, this text remains and is not over written. The light grey tip text is only displayed in the Explorer page	None.

Issue	Description	Workaround
	of the Edge browser and does not get submitted as part of the instruction so it can be ignored.	
"Provide authentication code" for a scheduled instruction displays warning "Scheduled instruction id X does not exist" or fails to accept a valid token with error "Token validation failed with error message".	Scheduled instruction workflow is not displaying the appropriate warnings when multiple users have updated a scheduled instruction or when there are multiple updates on one that is pending approval or waiting for the authentication code to be applied. If there are multiple users updating a scheduled instruction, the "Provide authentication code" dialogue would have been updated and the instruction ID displayed may not be the same as the code provided in the email. Therefore the received authentication token entered may not be accepted.	Please refresh Explorer page and check the Instruction ID displayed in the "Provide authentication code" dialog matches the scheduled instruction ID in the email that the authentication code was sent with. If the ID has incremented, then another user has updated the scheduled instruction.
Instruction responses Summary consistently shows a higher sent count and "Responses from" never reaches 100%.	TachyonMaster Switch table may contain multiple entries if the IP address of the server running the Switch Host service has changed and this will cause the sent count to go up for any instruction submitted.	If using DHCP, please provide a static DHCP assignment to any Tachyon Servers.
GetProcesses method does not return full list of processes on Android M6	Due to security lock down on Android since version M6 (Marshmallow), the GetProcesses method returns an incomplete process list	None.

Issue	Description	Workaround
(Marshmallow) or upwards.	since an Android applications are now sandboxed to enhanced security by application isolation. An application only has access to the list of processes that it has created either directly or indirectly.	
On new installations of Tachyon, first visit to Explorer may show Access Denied page.	Post clean install of Tachyon server, when user logs in for the first time to Explorer, the Explorer lands on error page complaining about lack of permissions. This can also be seen if the user presses Ctrl+F5 key to refresh the Explorer page. When same keys are pressed second time, the Explorer does not land on error page	Refresh the web page or press Ctrl+F5 again.
When using instructions with FileSystem module and the specified filename uses non-ascii characters, the response may return an error "Cannot open 'C:\tmp\?file.txt' for hashing because: (0x7b) The filename, directory name, or volume label syntax is incorrect."	If the specified filename uses non-ascii characters, the FileSystem module may not be able to find the file and therefore it will not be able to retrieve further information about it and report it's size as -1 and that the hash is "invalid hash".	None.

Issue	Description	Workaround
When using Filter Results and searching responses that relate to certificates, no results are found.	This can happen when an extra space exists in the search string or in responses. Examples Searching for subject for **'CN= machine.contoso.com'** does not return any matches, whereas searching for **'CN=machine.contoso.com'** will return matches. The windows certificate viewer (Crypto API Extensions) will insert spaces in some certificate properties for ease of viewing. The certificate itself does not contain these spaces, and so a search with spaces in the search string (for example, copied from the certificate viewer in windows) will not return any matches. If you run a command-line from cmd.exe with parameters (e.g. "psexec -i -s"), cmd.exe introduces another space between the executable name and the first parameter, so it becomes "psexec<space><space>-i s".	In order to match correctly, please use a search string with the correct number of spaces. It may help if you click on a similar value returned in the response, and edit that. Using certutil -dump will show the actual Subject Name of the certificate, which will match when searched for.
When a client is running on a laptop connected to a WiFi network and the	If a client on a laptop has been processing instructions and the WiFi connection is lost, it does not recognise the	Re-submit the instructions.

Issue	Description	Workaround
connection is lost (or it's turned off via the Wireless Network Connection), then the responses are lost.	connection is no longer available and continues to send responses. No responses will be received by the Tachyon Server.	
The Explorer Responses page displays a blank page with no results.	This can occur if the SQL instance and the TachyonResponses database are unreachable. If the Core web application is unable to access the TachyonResponses database when an instruction is asked then the Consumer will log an exception and the Explorer Responses page displays no results. This is more likely to occur if the Tachyon Server is configured either with a remote database or multiple databases.	Rectify the connection problem with the SQL Server instance and re-run the instruction.
If the client is restarted whilst it's attempting to download a resource (such as a script) while executing an instruction it logs ERROR - [Seq=<id>] Error processing instruction (InstructionId=<id>).	If the client is restarted whilst it's attempting to download a resource script, it logs ERROR - [Seq=<id>] Error processing instruction (InstructionId=<id>) On restart the client will not re-process the instruction so the error is not sent up to the server.	Re-submit the instruction.
The Sent Count for an instruction, and the statistics derived from it, imply that an	If the client service is terminated abruptly while processing an instruction, the client will re-request the	None.

Issue	Description	Workaround
instruction has been sent to more clients than the number deployed or targeted.	instruction when it next starts up. This causes the Switch to re-send the the same instruction to the client, which in turn will cause the statistics to show an increased Sent Count. This also affects the Success, Error, and Outstanding statistics in the Responses Summary page.	
Large responses to instructions may not be received from the client if the instruction is cancelled, even though you have selected to "Keep Results".	If the client is in the middle of an upload at the point that the instruction is cancelled, the Switch will cancel the upload if the size of the response exceeds 4K.	None.
An Action can not be approved or in a failed state.	When the Coordinator service goes into faulted state (e.g. as the result of an internal error), any live instructions remain in the "created" state and cannot be approved. Faults may be caused when a Tachyon Server has been upgraded when the instruction was still in-progress state during the upgrade process. The workflow will be unable to process the instruction after the upgrade and the error will be recorded in the Explorer portal Admin Log page.	The action needs to be re-submitted.

1.9.4.3.2 Instructions

Issue	Description	Workaround
Instructions using Device.GetDisks method on Windows 8, Windows 7, Vista or Server 2012R2 will return Error "Unsupported"	Device.GetDisk method uses WMI namespace query that is not supported in the earlier operating systems so the 1E Client will return an Error. 1E Client logs display the following: ERROR - Method error at L1.C1-L1.C17 ERROR - Unsupported	None
Running instruction with OperatingSystem.ControlStop and specifying 'IncludeDependents' as false to stop a service that has dependents return Success - no content even though 1E Client may log: ERROR - Could not perform ControlService because [(1051/0X41b) A stop control has been sent to a service that other running services are dependent on.]	When an instruction exercising agent method OperatingSystem.ControlService with parameter IncludeDependents = false (default) is sent to targeted endpoints; to stop/start specified service and the service fails the action due to dependent services , the instruction returns status Success-no-content" instead of Error.	None
Running an instruction with a FileSystem.FindFileBySizeAndHash or FileSystem.FindFileByName method e.g. "Which devices have a file named %filename% on a fixed disk?" may not return complete list on macOS Big Sur 11.0 and logs show error similar to:	Apple have clamped down on free access to the filesystem(s) in recent versions of macOS, and granting the "full disk access" from System Preferences --> Security	None

Issue	Description	Workaround
"ERROR - Could not open directory '/private/var/db/appinstalld' because: (1) Operation not permitted"	& Privacy --> Privacy seems to be limited to applications, not individual executables such as the 1E.Client daemon and the 1E Client installation cannot set up the permissions. Currently the only solution around this would be to add bin/bash give the 1E.Client daemon Full Disk Access (FDA). This can only be done by adding bin/bash FDA as we use bash to launch the Client Daemon. On launch, Client Daemon inherits the FDA permission from bash. Some directories still remain locked as they fall under macOS's System Integrity Protection (SIP). This is not recommended as adding bash to FDA can lead to serious security issues.	
1E Client becomes unresponsive to any instructions after performing an Extensibility update even though the Client continues to appear on online.	Once the Extensibility update instruction “Check for 1E Client updates and apply them” has been run and the Client has downloaded all the modules, it attempts to	Once the update has been run, the 1E Client process will need to be killed and the service restarted. Please avoid using any instructions

Issue	Description	Workaround
The 1E Client logs will display that all modules have been unloaded, but it continues to send Keep alive messages. Or if PXE module is enabled, the following is seen in the Agent logs: Faulting module path: C:\Program Files\1E\Client\Extensibility\1E.Client.Module.PXEEverywhere.dll	unload the existing ones in order to apply the updates. However, if the Inventory module is currently processing, it causes the Client to become unresponsive even though it continues to send keep alive messages to the Switch. This applies to all 1E Client (including the non-windows platforms).	which use the Agent.CheckForUpdates method.
Responses Chart view only displays as text.	Some instructions (e.g. What BIOS firmware is installed?) are authored so the responses are displayed as Chart view, but on Firefox this view may not be displayed correctly.	Use alternative web browser.
Instructions that have aggregation on floating point or DateTime values fail to return results.	When the instruction is run in TIMS, the raw values are shown correctly, but when uploaded to Tachyon the aggregation fails to sum the values, returning an empty row set. Aggregation on DateTime values where the input data looks like this also fail to return results: 01/17/2018 16:32:47.648	None.

Issue	Description	Workaround
Explorer response displays error 'Could not deserialize JSON into DataTable'.	If an instruction includes the Scripting.Run method running a PowerShell script, and the script fails or generates error output that is sent to standard out, this will be considered part of the output of the script, and cannot be converted into the format (JSON schema) expected for the response.	Please ensure the PowerShell script is written to either output data according to the JSON schema specified in the instruction definition, or exit with an exitcode, and not a mixture.
1E Client installed on macOS - Big Sur "(1) Operation not permitted" errors from FindFileByName	Apple have clamped down on free access to the filesystem(s) in recent versions of macOS, and granting the "full disk access" from System Preferences --> Security & Privacy --> Privacy seems to be limited to applications, not individual executables such as the 1E.Client daemon and the 1E Client installation cannot set up the permissions.	None.

1.9.4.3.3 Patch Success application

Issue	Description	Workaround
Patch Success instructions that are using SCCM as a patch source log remote	1E Client logs creating a remote connection to Microsoft WSUS Server with a CheckOnline property set to false to indicate that 1E Client is using Windows Update Agent	The log message should be interpreted as 1E Client performing a query against a Windows

Issue	Description	Workaround
connections to Microsoft WSUS server.	local cache to retrieve data. This log can easily be interpreted as an attempt to connect to internet to collect data, which is not what the 1E Client is doing. Instead the instructions are collecting additional information from WUA local cache in order to supplement missing data collected by ConfigMgr client and will therefore be regularly logged during normal operation of Patch Success instructions. ConfigMgr client omits Patch IDs for all installed patches and therefore require additional information to be collected from a different source to match missing Patch IDs.	Update Agent local cache.
Deploying a missing patch directly via the internet returns the following error "overallDownloadResult is Null"	If a missing patch is deployed onto a target device, but the Windows Update service is not running or stopped, the 1E Client will return error: "overallDownloadResult is Null" In later versions of the 1E Client, the returned error will be: "End search for updates because: (0x8024001E). Operation did not complete because the service system was being shutdown"	Ensure the Windows Update service is running before attempting to re-deploy the patch.
Deploying a missing patch to 1E Client may result with it logging "WARN - No updates to install" and the patch gets updated as "Not applicable"	If a missing patch is deployed, but there is no associated deployment package in ConfigMgr then the response will be returned as "Not applicable".	Ensure the patch has been packaged and deployed through ConfigMgr so that it is available to the CM clients before attempting to re-deploy the patch.

Issue	Description	Workaround
Patch Success charts and tables have inconsistent data.	Tachyon sync schedule process leads to new patch data being replaced with stale patch data when BI ETL is run. When syncs are scheduled in the recommended way then the nightly BI ETL will replace all device and patch data in the BI star schema and cube with potentially stale SLA inventory data.	Execute a new Tachyon sync, once the expected devices have reported in patch data (check Tachyon Explorer → Instructions → History → "Returns Patch status for...") then execute a new BI ETL. This will result in up to date device and patch data in both the BI star schema and the cube.
Deploying a patch directly via the internet may return failure "End search for updates failed because: Not enough storage is available to complete this operation" and WindowsUpdate.log will show an associated error: "WARNING: WU client failed Searching for update with error 0x8007000e"	On Windows 7 / Server 2008 R2 there is a known issue with the Windows Update that causes it to return an "8007000E" error message. This may be seen if in the Patch Success page, a patch is deployed with the check box enabled for "Enable patches to be downloaded onto devices directly from the internet instead of the default (SCCM)".	Please ensure the update that contains the improvements to Windows Update Client is applied in order to allow for further Patch Success deployments to function correctly.
History page should be hidden when user only has Patch success viewer permissions	History page is displayed when user has no access to Patch Success instructions.	None
Patch Success will show all devices irrespective of the permissions on management groups.	BI cube does not have permissions model required to filter the management groups correctly. In addition, permissions model only assigns management groups to instructions therefore will not cater for BI cube permissions.	None

1.9.4.3.4 Guaranteed State application

Issue	Description	Workaround
Any pending changes in Guaranteed State and/or Experience applications that are deployed during upgrade process from Tachyon platform v5.1 to v5.2 or v8.0. This is also true if there is an already deployed unlicensed rule/recondition/check or fix.	Tachyon Setup runs a post installation action to automatically deploy all policies and event subscriptions.	Ensure any pending deployment changes under review are either deployed prior to upgrade process is initiated or respective rule/policy/Survey should be marked as disabled to prevent deployment during upgrade process
Guaranteed State Overview pages show incorrect devices when Policy with no Rules have been assigned to a Management Group.	On the Guaranteed State Overview page, the Online, Online last 7 days and Last seen per Criticality Level charts all show incorrect counts when a Policy is assigned to a Management Group, but no Rules have been assigned yet. This will display correct values once Rules are assigned and devices have responded to the events.	None
Opening an instruction or fragment that has been exported using the Consumer API displays the following message when viewed in TIMS: "This instruction definition was signed by CN=Tachyon Explorer Instructions but the content has been tampered with.	An instruction exported through Postman can generate file with whitespace differences and file size between the original file which is not accepted by TIMS as it's considered to be tampered.	Use alternative API tools (e.g Fiddler).
"Ensure Nomad can communicate through the Windows Firewall" remediation is	"Ensure Nomad can communicate through the Windows Firewall" remediation is being carried out when there is a firewall	None

Issue	Description	Workaround
being executed even when firewall is disabled from the GPO.	policy that has been disabled through group policy. This means that when firewall policy has been disabled explicitly, instead of ignoring the fix, the firewall is set to enabled and the firewall exceptions are set for Nomad.	
On a ConfigMgr Distribution Point, the Rule to "Check the Nomad has a virtual directory on ConfigMgr distribution points to perform LSZ generation" always passes even though a failure reason may be returned in the Data field.	The check fragment should verify that the LSZFILES website setup by Nomad on a DP has certain characteristics, but even when errors are found the check status is "Passed". The logic in the PowerShell parts of the fragments uses a $errorOccurred variable to set the exit code, but this variable is initialized to $false and then never changed even when an error is detected. e.g Data field returns: "Windows authentication not enabled. Require SSL flag is not disabled. Directory browsing not correctly set."	None
1E Client logs several unsuccessful remediation attempts within a 24hr period.	There is currently no longer a cap on the number of time a remediation step can occur on a machine within 24hrs. This differs from 1E Client Health where after 3 failures to remediate an issue, further remediation would not occur until 24hrs have passed.	None

1.9.4.3.5 Experience application

Issue	Description	Workaround
Experience - Software > Duplicate row for a product is displayed on Software screen when architecture column is added from column picker following an upgrade from 8.0.	The architecture column did not exist in pre-v8.0 SoftwarePerformance table. When upgraded to v8.0 or later, architecture column has been introduced as nullable column to accommodate pre-upgrade data. It will be set as null for all existing data from before the upgrade. Gradually as new experience performance data comes in post upgrade architecture will now be included. This means that for 90 days after the upgrade aggregations within the Software screen of experience can have two entries, one with an unknown architecture and one with a valid architecture.	The existing data will correct itself 90 days after the upgrade. If you need to fix this issue in the meantime, a maintenance Stored Procedure for the Experience database can be obtained from 1E. The SP will update the null architecture for pre-upgrade software performance rows by using post-upgrade rows to identify and correct old software architectures.
Experience Analytics - Tiles have an additional text "score" added to them when view between saved preset is changed.	When user changes the view between Default and user saved presets; an additional text "Score" gets added to the tile title, e.g: StabilityScore, ResponsivenessScore.	Refreshing the browser removes the additional text "Score".
A survey that has been dismissed by the user will reappear if it is disabled then re-enabled.	If a user engagement (survey or announcement) is disabled then re-enabled then it appears to the 1E Client as a completely new engagement and the previous state (dismissed, in this case) is lost.	Do not disable an engagement then re-enable it! In effect this creates a new instance, at least in terms of data sent to the 1E Client.
Application Interaction table can contain processes reported as *.tmp files where the	The Application Interaction view is reached by launching the Experience > Devices and viewing the Device hyperlink.	None

Issue	Description	Workaround
Product and Version columns are blank.	When viewing the Experience > Application Interaction tab, the *.tmp records are also displayed which do not have associated Product or Version details. These should be filtered out.	
The Survey response page displays responses from a device that do not match the score seen when viewing the Device details due to duplicate survey names	When a survey is deleted, the old responses do not get removed and current behavior causes issues when a new survey is created with the same name. The calculations for sentiment score includes responses from the old survey where the names match.	Where this occurs, recreate the survey using a unique name that has not been previously used. If you are affected by this, please contact 1E Support for additional help.
When doing a search on Survey page, the page size resets back to the default (50)	On the Experience > Survey page, the page size can be increased to to display 100 or 250 rows. However, when a search is performed on the page, the page size jumps back to the default 50.	None
Survey reports always shows Applicable devices as 100%	Even when a general purpose survey has been assigned to a Management Group, the filter for survey reports always shows 100% for Applicable devices and not consistent with the devices assigned to the selected Management Group	None

1.9.4.3.6 Inventory

Issue	Description	Workaround
No issues currently known.		

1.9.4.3.7 1E Catalog

Issues	Notes	Workaround
Any Title of a Vendor with two different colloquial versions should not be allowed when other fields are same.	There may be instances where a product has different colloquial versions for the same version such as Microsoft Excel 15.0 with a 2013 colloquial version and Microsoft Excel 15.0 with a 2015 colloquial version.	None
Timeout is displayed during updates and the Catalog UI is not available during that time.	The Catalog Web UI is unavailable when it's downloading data from the 1E Cloud Catalog.	If you try again after some time the Catalog Web UI should work.
The installer creates the database when you cancel the process in the setup wizard.	If you decide to abort the installation after providing the name of the Catalog database, the installer creates the database despite the cancellation.	None
Pressing Cancel when prompted for your credentials on the Web UI Admin page displays an error.	If you click Cancel on the Web UI Admin page when prompted for your credentials, an HTTP error 401.1 – Unauthorized error is displayed.	None
Unable to create new versions with more than 4-part numbers in the Catalog Web UI.	If you attempt to curate a version with more than 4-parts (for example, 1.2.0.1.2) in the Catalog Web UI, it displays the error – The version is not in the correct format.	None
The Catalog Web UI does not report if the Catalog service is unavailable.	During a downtime, if you try to navigate through Catalog Web UI, it becomes unresponsive but does not display a message that the service is unavailable.	None
The Catalog Web UI displays an incorrect message if you leave the page and return to it.	During a resynchronization event, if you navigate to a different page and immediately return to the Admin page, it displays a Resync completed Successfully message, even though it	None

Issues	Notes	Workaround
	has not. The resynchronization event keeps running in the background until it successfully completes.	
Best Match API times out when indexes are being compiled.	If the Best Match API is called while the indexes are being compiled, it times-out. However, the second call will succeed.	The second call will succeed.
Unable to cancel the installer while it is migrating to a new version.	During a migration to a newer version of the Catalog, pressing Cancel does not stop or roll back the installation – it continues uninterrupted.	None
The number of records pulled during a 1E Cloud Catalog synchronization event is not known at the start of it.	When the Catalog synchronization event starts, you're not able to discover the total number of records that will be inserted into the database. The logs register the number of records it inserts successfully but you would not know the total records to be inserted beforehand.	None
Clicking Back to list in Catalog Web UI navigates to the Home page instead of the previous page.	If you filter on a vendor and go to any next page to set license rules for that vendor, and then click Back to list, it takes you back to the Home page and does not retain the filter applied in the previous step.	None
The unattended install does not check Catalog prerequisites.	The installation will fail if requirements are not met.	None
Indexing fails when if the rebuild index and incremental index events are run simultaneously.	If a rebuild index and incremental index conflict, indexing will not complete successfully.	It will complete successfully the next time the incremental index event runs.

Issues	Notes	Workaround
Error when user modifies an edition from Catalog Web UI.	If you attempt to modify the edition of a product then "An error has occurred while processing your request" message is displayed.	None
Log files and other folders not deleted from program data folder after uninstalling catalog.	If the Catalog is uninstalled, its logs folder structure is not deleted from the Program Data folder.	None
On the Catalog Web UI new bundles screen selection of multiple dropboxes gives wrong filtered record.	On Catalog Web UI new bundles screen, selection of multiple dropboxes returns an incorrect filtered record.	None
File Version filter on Catalog Web UI does not work.	File Version on product file screen filter is not working.	None
A prompt to reboot the server is displayed when you upgrade or uninstall the product.	There may be instances where you are prompted to restart the server in order to complete the installation.	Restart the server.
Installer unable to connect to the database when you run a repair on the Catalog from Programs and Features.	In a TLS environment, if you opt to repair the Catalog from Programs and Features by choosing the Repair option, you will be prompted with this error: *Error 27502: Could not connect to Microsoft SQL Server ... SSL Security error. (18)*	Uninstall and reinstall the Catalog
Lucene index folder is not deleted on uninstalling catalog.	On uninstalling the catalog, Index directory from program data is not getting deleted.	None
Wrong Surrogate key mapping is formed in case product is deleted from client side and upgrade is performed	On upgrading the catalog deleted site define entries are not getting persists	None

Issues	Notes	Workaround
Installer should have a check for ASP.NET as Catalog is not failing when "ASP.NET" is not installed	The Prerequisite check of installer does not check for ASP.NET	None
Re-Sync: Timeout error is observed while getting site defined on one client machine while Re-Sync with another client machine is in progress	Re-Sync is successful on one of the client and error is observed on second client while it's getting the site defined entries. Following is observed in the logs:- *The timeout period elapsed prior to completion of the operation or the server is not responding.*	None
Error message is observed in logs while indexes are recreated after sync in edge case installation scenario	Install catalog through unified tachyon installer, after successful installation, uninstall the catalog. If user Installs the catalog stand-alone start the sync then its IIS services should shift into different pool due to which indexes will break.	None
Catalog 2.0 error '500 Internal server Error)Index is getting failed' in the 'Catalog.UpdateService.log' when the 1E Catalog service account uses domain user account. (Highly Intermittent).	When the 1E Catalog service account is using a domain user account rather than Network Service account, the index is getting failed after sync is completed.	This issue does not cause functional issues and can be safely ignored.
Catalog 2.0 if an upgrade fails, the 1E Catalog installer will roll back the installation and remove any customizations in the 'web.config' and 'CatalogUpdateService.exe.config' files.	If an upgrade fails, the 1E Catalog installer will roll back the installation and remove any customizations in the 'web.config' and 'CatalogUpdateService.exe.config' files.	This is resolved by backing up the configuration files prior of upgrading as covered in the 'installation and upgrades' section of the documentation.

1.9.4.3.8 1E Tachyon Toolkit

Issue	Description	Workaround
1E Tachyon Toolkit extensions are not visible on the CM Console for both Devices and Device Collections	In the past, any installed extension was allowed to be displayed. Microsoft has changed the way that the Console Extensions are allowed to be displayed within the ConfigMgr Console and if in the Administration -> Site Configuration -> Sites -> Hierarchy Settings from the ribbon. and under the General tab: "Only allow console extensions that are approved for the hierarchy" is selected it will prevent the Tachyon right-click actions and the Instruction Runner from becoming available.	Ensure the "Only allow console extensions that are approved for the hierarchy" is not selected in the Hierarchy Settings Properties. Please contact 1E Support for additional help where the Tachyon right-click extensions only appear for the Devices and not Device collections.
Configuration Manager console shows duplicate right-click options for Tachyon.	Tachyon shows multiple times in a collection property when the collection belongs to nested folders in the Configuration Manager console.	Restart the Configuration Manager console.

1.9.5 Server installation issues

Troubleshooting common issues that you may be having with implementation.

If your problem is not identified on this page, then please review Installing Tachyon Server.

Please ensure you have run through the steps in the Verifying page before making any configuration changes. Several verification steps refer back to this page.

If you need further help, please refer to the Troubleshooting page for how to contact 1E Support and the technical support process.

1.9.5.1 Unable to install

If for any reason you are unable to install it, then please review the Preparation page. You should also re-run Tachyon Server post-installation tasks.

When installing interactively, please confirm you are logged on using an account that has local Administrator rights.

For Tachyon Servers, you can troubleshoot installation issues by reviewing the installation log file that is created in the same directory as **Tachyon.Setup.exe** after Tachyon Setup has run the installer.

For clients, you can troubleshoot installation issues by reviewing the installation log file. If you are having issues with 1E Client, please refer to Troubleshooting.

1.9.5.2 Verify the Tachyon Server certificate bindings

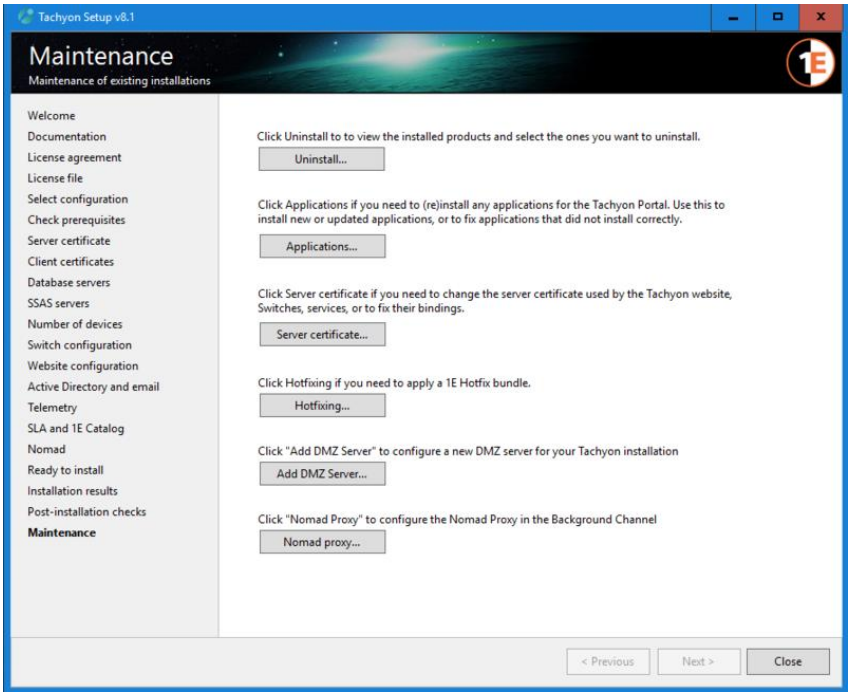
The server installer detects which Web Server certificate to use by matching the certificate's **Subject Alternative Name** (DNS) with the **HTTPS Host header** supplied during installation. As discussed in Certificate requirements, the **Subject Alternative Name** must include the DNS Alias FQDN of the server of type DNS Name, for example, **DNS=TACHYON.ACME.LOCAL**

To check the HTTPS binding of the website use the following steps. These steps can also be used to change the certificate if it has expired, or a new certificate needs to be used.

1. Logon to the Tachyon Server using the Tachyon installation account or user with local administrator rights.

2. Start Tachyon Setup and navigate directly to the Maintenance screen.

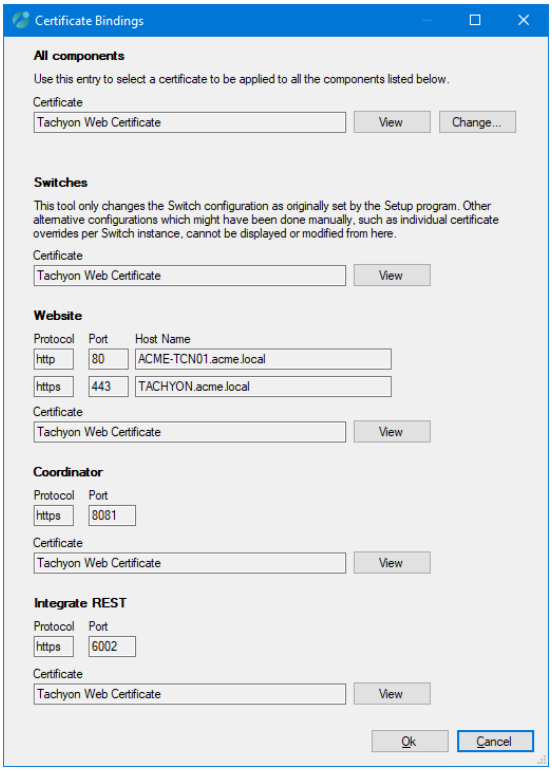
3. Click on **Server certificate...**



4. Review the **Certificate Bindings** screen.

   It shows the **thumbprint** of the certificate used by each of the bindings required by Tachyon, or the **Friendly name** if one has been used, as shown in the picture.

   If the bindings are using different certificates, then this may be deliberate, and you should find out why.

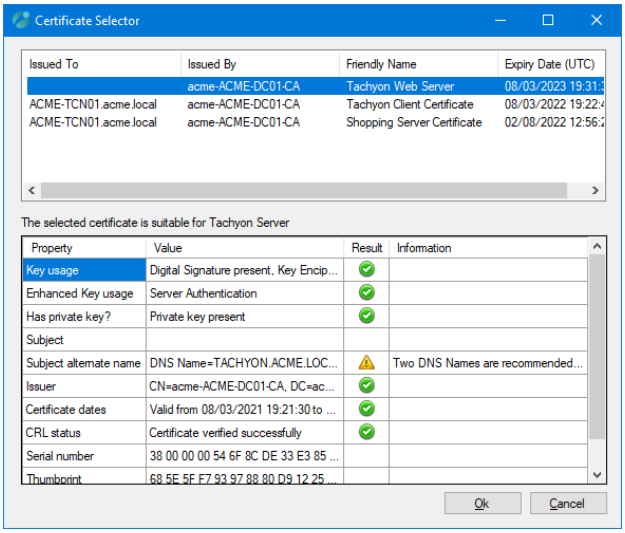


5. To view the details of a certificate, click **View**

6. To change the certificate, click **Change...**

   This will start the **Certificate Selector** similar to the Server certificate screen.

   This will let you select a certificate and apply it to all the bindings.



Note

If for any reason you need to apply a different certificate to each binding, then please contact 1E for details of how to configure them.

Note

The Coordinator may be using port 8080 if you have upgraded from Tachyon 3.3.

7. In the **Certificate Selector** screen, select a certificate, and the Selector will evaluate its suitability.

   Click **OK** when you have selected a suitable certificate.

   This will return you to the **Certificate Bindings** screen.

8. In the **Certificate Bindings** screen, click **OK** to save the new bindings configuration.

   You do not require an IIS reset.

1.9.5.2.1 Tachyon Switch certificate issues

The Switch will start and then stop if there is an issue with its certificate.

Check the following log files for errors. The default location for Tachyon Server logs is the **%AllUsersProfile%\1E\Tachyon** folder on the server where Tachyon Server is installed.

- Tachyon.Switch.Host.log
- Tachyon.Switch.log

1.9.5.3 Verify IIS Configuration

For minimum requirements for IIS see Windows Server roles and features.

To review the configuration:

1. Start PowerShell with Admin privileges.
2. Type **Get-WindowsFeature** and wait for the listing to complete. It can be useful to pipe this output to a file.
3. Check the results and confirm that each of the minimum requirements is listed with an [X].
4. Alternatively, run Tachyon Setup and run the Post-installation check.

The table below shows the IIS web applications used by Tachyon, and the IIS features that affect how users and clients connect. For more detail about these IIS web applications, please refer to Tachyon Single-Server system.

IIS web application	Server	Authentication Enabled	SSL Settings	IP Address and Domain Restrictions
Admin	Master	Windows	Not configured	Not configured
Background	Response & DMZ	Anonymous and Windows	Require SSL (accept)	Not configured

IIS web application	Server	Authentication Enabled	SSL Settings	IP Address and Domain Restrictions
		Anonymous is used by clients, Windows is used by Consumer API		
CatalogWeb	Master	Anonymous and Windows	Not configured	Not configured
Consumer	Master	Windows Basic Authentication must also be enabled if using 1E Core (for ServiceNow integration)	Require SSL (ignore)	Not configured
ContentDistribution	Master	Anonymous and Windows	Not configured	Not configured
Core	Response & DMZ	Anonymous	Require SSL (ignore)	Local IP addresses, plus the following added manually if used: • remote Master stack server • remote DMZ Server
CoreExternal	Master	Anonymous	Not configured	Not configured
Experience	Master	Windows Basic Authentication must also be enabled if using 1E Core (for ServiceNow integration)	Require SSL (ignore)	Not configured
Platform	Master	Windows	Not configured	Not configured

IIS web application	Server	Authentication Enabled	SSL Settings	IP Address and Domain Restrictions
Tachyon	Master	Windows	Require SSL (ignore)	Not configured

Note

The **IP Address and Domain Restrictions** feature is described in more detail below. Steps for verifying its configuration are provided in Verify IIS security of the Tachyon website.

1.9.5.4 IP Address and Domain Restrictions

The Tachyon **Core** web application (Response Stack) uses the IIS feature **IP Address and Domain Restrictions** to restrict access so that connections are only allowed from specific IP addresses. Other web applications, including Tachyon, Background, and CoreExternal, are not configured, and therefore they allow all local and remote connections.

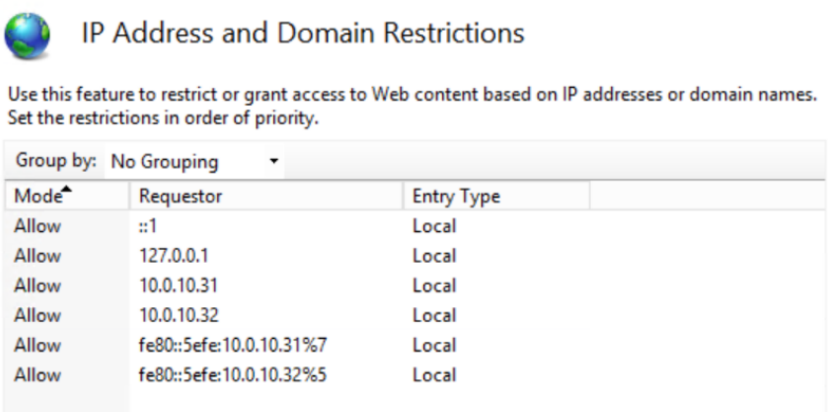
The list of IPv4 and IPv6 addresses is updated by Tachyon Setup during installation (and upgrade) of the following configurations.

Configuration choice in Tachyon Setup	What Tachyon Setup (or TachyonServer installer) does during installation/upgrade
All components on a single server	Adds all the IP Addresses of the local server during installation of the server. This allows the Core to receive connections from local Switches and components of the local Master Server.
Response Stack	Adds all the IP Addresses of the local Response Server and the remote Master Server that are resolvable from the local server during installation of the Response Stack. This allows the Core to receive connections from local Switches and components on the remote Master Server.
DMZ Server	Adds the IP Addresses of the DMZ Server that are resolvable from the local Response Server (Core) during the first phase of DMZ Server setup. This allows the Core to receive connections from Switches on the remote DMZ Server.

Below is an example of what the configuration looks like for a Tachyon Server which has a two network adapters, one for a Switch, the other for SQL traffic, with IPv4 enabled and IPv6 disabled on each interface. The IPv6 addresses shown are isatap addresses, which is enabled by default on the server.

- **::1** is the IPv6 loopback address
- **127.0.0.1** is the IPv4 loopback address

- **10.0.10.31** is the IPv4 address for network interface #7
- **10.0.10.32** is the IPv4 address for network interface #5
- **fe80::5efe:10.0.10.31%7** is the isatap address for network interface #7
- **fe80::5efe:10.0.10.32%5** is the isatap address for network interface #5



1.9.5.4.1 When to modify IP Address and Domain Restrictions

The Tachyon installer uses the PowerShell cmdlet **Get-NetIPAddress** to list all the IPv4 and IPv6 Addresses and adds them all to the restricted web applications during installation or upgrade. You must modify the configuration of **IP Address and Domain Restrictions** if the network interface configuration has changed on a Tachyon Server, for example if an IP Address is changed, or a new network interface is installed.

You will also need to modify the configuration of the Response Stack's Core web application to manually add the internal-facing IP Address of a DMZ Server.

1.9.5.4.2 Changing the configuration of Network Adapters

If the configuration of any network adapters is changed, then the Tachyon website configuration for **IP Address and Domain Restrictions** may need to be updated with the server's new IPv4 and IPv6 addresses. Failure to update the configuration after a network change will cause issues between the Switch and the Core and prevent the Tachyon Server from functioning.

Use the PowerShell cmdlet **Get-NetIPAddress** to determine the current IP Addresses, and if necessary update the configuration of the Core web application.

The following **AddIpSec.ps1** script can be used to refresh local IP Addresses. It does *not* remove old, unwanted, or remote IP Addresses. Nor does it add addresses for remote Switches, which would need to be added manually.

```
# Adds local IPv4, v6 and loopback addresses to the IP Address and Domain Restr
ictions of the specified web applications. It does not delete any addresses
# Remote addresses must be manually configured.
# It only adds addresses if the specified web application exists.

Import-Module "WebAdministration"
```

```
Function AddIpSec() {
    param(
        [Parameter(Mandatory=$true)][string]$SiteName,
        [Parameter(Mandatory=$true)][string]$AppName
    )

    Write-Output "Adding IP restrictions to $AppName"

    $fullAppPath = "IIS:\Sites\" + $SiteName + "\" + $AppName

    if (Test-Path -Path $fullAppPath) {
        $appPath = $SiteName + "/" + $AppName
        $ipAddreses = Get-NetIPAddress | sort IpAddress | foreach { $_.IPAddres
s }
        Set-WebConfigurationProperty /system.webserver/security/ipsecurity -Nam
e allowUnlisted -Value "false" -Location $appPath -PSPath IIS:\
        foreach ($ipAddress in $ipAddreses)
        {
            $existingRestriction = Get-WebConfiguration system.webServer/Securi
ty/ipSecurity/add -Location $appPath -PSPath IIS:\ | where { $_.ipAddress -eq $
ipAddress }
            if (-not ($existingRestriction)) {
                Add-WebConfiguration system.webServer/security/ipSecurity -Loca
tion $appPath -Value @{ipAddress="$ipAddress";allowed="true"} -PSPath IIS:\
                Write-Output "Allowed restriction on IP $ipAddress added to $Ap
pName"
            }
            else {
                Write-Output "Restriction on IP $ipAddress already exists in $A
ppName. So skipping."
            }
        }
    }
    else {
        Write-Output "$AppName web application does not exist"
    }
}

$siteName = "Tachyon"

AddIpSec -SiteName $siteName -AppName "Core"
AddIpSec -SiteName $siteName -AppName "WelcomeCore"
```

1.9.5.4.3 Remote Access to the Core

A post-installation test is to confirm web browsers do not have remote access to the Core. A remote web browser is not expected to be able to access the Core web application, which should return a 'Server Error 403 - Forbidden: Access is denied'. If you are able to access these web applications from a remote computer then it is probable that the **IP Address and Domain Restrictions** feature is not installed.

Use the following steps to check if the **IP Address and Domain Restrictions** feature is installed and to install it.

1. Logon to the Tachyon Server using an account that has administrator privileges.
2. Start Powershell with Admin privileges.
3. Type **Get-WindowsFeature** and wait for the listing to complete.
4. Check to see if Web Server Security feature **IP Address and Domain Restrictions** is installed or not.
5. If installed, then Verify IIS Configuration to determine if there may be another reason for the issue.
6. If not installed, then:
    a. type **Install-WindowsFeature Web-IP-Security** and wait for the feature installation to complete (a reboot or IIS restart is not required).
    b. after the feature installation, the Core web application will have its configuration settings restored to the settings configured at the time that Tachyon was installed.
7. Use the PowerShell cmdlet **Get-NetIPAddress** to determine the current IP Addresses, and if necessary update the configuration for the Core web application.
8. Repeat the Verifying steps.

1.9.5.5 401 Not Authorized

There are a number of reasons why you may see this error when you browse to the Tachyon portal for the first time. You may also see errors saying Not Authorized or Unauthorized in server log files.

The usual reason for this is your server is configured to use Kerberos authentication and the HTTP class SPN is not registered in AD for the DNS Name used to access the server.

Service Principal Names (SPN) are attributes of AD accounts. A domain administrator will need to create an HTTP class SPN for the web server service account, by using one of the following methods:

- By editing the ServicePrincipalName attribute of the web server's computer account
- Using the following SETSPN commands, substituting your DNS Name, server, and service account:

```
setspn -l ACME\ACME-TCN01$
setspn -s http/acme-tcn01.acme.local ACME\ACME-TCN01$
setspn -s http/tachyon.acme.local ACME\ACME-TCN01$
```

Use each command as follows:

1. List existing SPNs for the service account. Run this to record details before you request for any new SPN(s) to be created. Re-run this after creation, ensuring you wait sufficient time for AD replication to occur.
2. Use this if **tachyon.acme.local** is a CNAME record and its (A) Host record is **acme-tcn01.acme.local**
3. Use this if **tachyon.acme.local** is a (A) Host record.

The above example assumes the:

- Service account for all Tachyon web application pools is Network Service
- Tachyon server name is **ACME-TCN01** with a computer account in the **ACME** domain, which means the service account is **ACME\ACME-TCN01$**
- DNS Name for the server is **tachyon.acme.local**.

Tip

If in doubt, it does no harm to create an SPN for each DNS Name used to access the Tachyon Server, including its CNAMEs and (A) Host records using: *setspn -s http/<DNS Name> ACME\ACME-TCN01$*

To determine which type of record a DNS Name is, run the following command:

```
nslookup tachyon.acme.local
```

- If the command returns Name: **acme-tcn01.acme.local** and alias **tachyon.acme.local** then tachyon.acme.local is a CNAME record.
- If the command returns Name: **tachyon.acme.local** and no aliases then tachyon.acme.local is a (A) Host record.

More complex scenarios can be configured which requires in-depth knowledge of IIS, SPN, and DNS configuration and are beyond the scope of this documentation.

1.9.5.6 403 Access Denied

You may see this error when doing post-installation tests (refer to Verifying). When you use a browser to open an application in the Tachyon portal, you will see **Server Error 403 - Forbidden: 'Access denied'** if the internal account used by the Application Pool does not have read access to the Tachyon web application folders. This can happen if Tachyon is installed in a non-default location and the NTFS permissions on the installation folder are not correct. To remedy the issue, you should review and correct NTFS permissions as described in Services and NTFS Security.

Warning

Do not enable Anonymous authentication to fix this type of issue.

1.9.5.7 404 File not found

You may see this error when doing post-installation verification tests, (refer to Verifying).

When you use a browser to open an application in the Tachyon portal, and you see **Server Error 404 - 'File not found'** the reason is probably that you have not installed the IIS features **Web-ASP** and/or **Web-Asp-Net45**.

Use the following steps to check if the **Web-ASP** and/or **Web-Asp-Net45** features are installed and to install them.

1. Logon to the Tachyon Server using an account that has server administrator privileges.
2. Start Powershell with Admin privileges.

3. Type **Get-WindowsFeature** and wait for the listing to complete.
4. Check to see if the Web Server Application Development feature **Web-ASP** and/or **Web-Asp-Net45** is installed or not.
5. If not installed:
    a. Type **Install-WindowsFeature Web-ASP, Web-Asp-Net45** and wait for the feature installation to complete (a reboot or IIS restart is not required).
    b. Perform an IIS Reset.
6. If installed, then Verify IIS Configuration to determine if there may be another reason for the issue.
7. Repeat the Verifying steps.

1.9.6 Client issues

For troubleshooting common issues that you may be having with the installation and configuration of the client, refer to Client issues.

1.10Extending Tachyon

Information about tools used to extend Tachyon beyond Tachyon Explorer.

1.10.1 The 1E Tachyon Toolkit

What's included in 1E Tachyon Toolkit, and how to install it.

The kit includes:

- **1E Tachyon Toolkit** - Run Instruction (command-line tool)
- **TachyonConfigMgr UI Extensions** - only installed if the installer detects the Configuration Manager console on the local device.

1.10.1.1 1E Tachyon Toolkit requirements

Requirements for installing the 1E Tachyon Toolkit components.

1.10.1.1.1 Toolkit supported platforms

Category	Product	Notes
Client OS	• Windows Server 2022 • Windows	For OS supported by Configuration Manager Current Branch (CB) see https://technet.microsoft.com/en-us/library/mt589499.aspx).

Category	Product	Notes
	Server 2019 • Windows Server 2016 • Windows 10 CB 21H2 • Windows 11 CB 21H2 • Windows 10 CB 21H1 • Windows 10 CB 20H2	
Microsoft Endpoint Configuration Manager console	• SCCM CB 2203 • SCCM CB 2111 • SCCM CB 2107 • SCCM CB 2103	These are the versions of Configuration Manager that 1E has tested and therefore support, but later versions are assumed to work also. Please see Preparing for the Tachyon extensions for the Configuration Manager Console..

Category	Product	Notes
	• SCCM CB 2010	

1.10.1.1.2 Installing the 1E Tachyon Toolkit

To install the toolkit the installation account must have local Administrator rights on the device.

Toolkit component	Requirements for installation	Requirements for use
Tachyon ConfigMgr UI Extensions	Local administrator on the Windows computer. Configuration Manager Console already installed. The option to install the Tachyon ConfigMgr UI Extensions is available only if the toolkit installer detects the Configuration Manager console is installed on the local computer. The Configuration Manager Console should be closed when installing or uninstalling. To install the Nomad Download Pause feature aspect of the Tachyon ConfigMgr UI Extensions the installation account must be a full Configuration Manager administrator. For more details, please refer to Nomad Download Pause.	Configuration Manager Administrative User. Tachyon user with actioner permission on the instructions.
Tachyon Run Instruction command-line utility	Local administrator on the Windows Computer.	Tachyon user with permission to run instructions (questioner and/or actioner).

1.10.1.2 Preparing for the Tachyon extensions for the Configuration Manager Console.

A step-by-step guide to configuring prerequisites required for the Tachyon extensions for the Configuration Manager Console., before /document/preview/616279#UUID-e8f99f2a-bb21-f1e3-de43-ec7231143bee.

1.10.1.2.1 Requirements

1.10.1.2.1.1 Supported Platforms

Supported versions of client OS and Configuration Manager that are supported by the Tachyon Configuration Manager Console extensions are:

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows 10 CB 21H2
- Windows 11 CB 21H2
- Windows 10 CB 21H1
- Windows 10 CB 20H2
- SCCM CB 2203
- SCCM CB 2111
- SCCM CB 2107
- SCCM CB 2103
- SCCM CB 2010

1.10.1.2.1.2 Tachyon user accounts

To prepare Tachyon for using the Configuration Manager Console extensions, you will need a Tachyon user account that has at the **Full Administrator** role.

To use the Tachyon Configuration Manager Console extensions, you must have a Tachyon user account and Configuration Manager administrative user account. Guidance for this is given below in User roles.

1.10.1.2.2 User roles

The two systems, Configuration Manager and Tachyon, both use RBAC to define the capabilities for their corresponding users. To enable Tachyon instructions to be run from Configuration Manager, the Configuration Manager Console users must also have a presence defined in Tachyon. This presence can take many forms, for example you could define a user in Tachyon from an AD group and then add all your Configuration Manager users to that group - and manage the Tachyon roles for the users as a group, or you could define individual users in Tachyon for each Configuration Manager user - and manage the Tachyon roles on a per-user basis. You will likely have determined roles for your Configuration Manager users based on their function within the organization, the following heading provides a rough guide to matching Tachyon and Configuration Manager roles.

1.10.1.2.2.1 A rough comparison of the Tachyon User Roles and Configuration Manager Roles

The Configuration Manager Console may be installed and used by any user that is configured as an Administrative User. There are a number of Security Roles that may be given to the user and not all of these roles are permitted to use Configuration Manager to make changes that affect the network. When configuring any corresponding Tachyon users, you should take this into account when assigning the Tachyon Roles. For example, it would be unusual for a user with just the **Read-only Analyst** role in Configuration Manager to be granted the **All Instructions Actioner** role in Tachyon and therefore be able to perform Tachyon actions on all the devices in a particular collection but not be able to use Configuration Manager to perform any other tasks. There is no one-to-one mapping of the Tachyon and Configuration Manager roles, but the following table provides some rough comparisons between the two.

Tachyon Role	Configuration Manager Role
Viewer	Read-only Analyst.
Questioner	Read-only Analyst.
Actioner	Examples of equivalent Configuration Manager roles could be: • Application Deployment Administrator • Remote Tools Operator • Software Update Manager.
Approver	Any Configuration Manager Security Role that would be appropriate for the Approver to approve actions run from Configuration Manager.

1.10.1.2.3 Setting up Tachyon for Configuration Manager integration

The following instructions show how to configure the integration between Configuration Manager and Tachyon after the Tachyon extensions for the Configuration Manager Console. have been installed.

The animation below (available soon) shows an end-to-end example of configuring Tachyon to support the Tachyon extensions for the Configuration Manager Console.. This example generally uses the following steps. We'll highlight in the steps where optional decisions have been taken in the example.

1.10.1.2.3.1 1. Add the Configuration Manager Console extensions consumers to Tachyon

To run any of the Client Actions using Tachyon menu items, other than the Instruction Runner, you will need to add (register) the **CmConsoleExtensions** consumer to Tachyon using the Explorer Administration Consumers page. The steps to take are:

1. Logon to the TachyonPortal using a user account with the **Full Administrator** role.

2. Navigate to the **Settings→Instructions→Consumers** page
3. Click the **Add** button to create a new consumer
4. The new consumer should be configured with the default values, except for the following:

Parameter	Value
Name	CmConsoleExtensions
Maximum simultaneous instructions	10
Enabled	Check this checkbox

5. Click the **Add** button to save the new consumer

To run the Instruction Runner, you will need to add the **RunInstructionUI** consumer to Tachyon using the Explorer Administration Consumers page. The steps to take this are:

1. Log on to the Explorer as an administrator with the **Consumer Administrators** role
2. Navigate to the **Administration Consumers** page
3. Click the **Add+** button to create a new consumer
4. The new consumer should be configured with the default values, except for the following:

Parameter	Value
Name	RunInstructionUI
Maximum simultaneous instructions	250
Enabled	Check this checkbox

5. Click the **Add** button to save the new consumer

1.10.1.2.3.2 2. Upload the Configuration Manager Console extensions product pack to Tachyon and create an instruction set

First upload the instructions:

1. Logon to the Tachyon Portal using a user account with the **Full Administrator** role.
2. Open the **Settings** application.
3. Navigate to the **Settings→Instructions→Instruction sets** page.
4. Click on the **Upload** button.
5. In the Open dialog navigate to the location of the **1E-ConfigMgrConsoleExtensions.zip** file.
6. Select **1E-ConfigMgrConsoleExtensions.zip** and click **Open**.

All the instructions contained in the zip file will initially be added to the default **Unassigned** instruction set. Instructions in the **Unassigned** instruction set cannot be used, so first you will need to create a new instruction set with the verification instructions.

1. Select the 16 instructions you want to add to the new set, by clicking the checkbox at the start of each instruction row in the list.
2. Click the **Add new set** button in the button panel to the right of the page.
3. In the **Add new instruction set** popup subsequently displayed, and type:
    a. **1E ConfigMgrConsoleExtensions** as the name.
    b. **Tachyon Configuration Manager console extensions** as the description.
4. Ensure that the **Include 16 selected instructions** checkbox is checked.
5. Click the **Add** button to add the new instruction set, with the selected instructions.

1.10.1.2.3.3 3. Enable Configuration Manager Console user access to Tachyon

You will need to ensure that the account you will be using to run the Configuration Manager Console is also represented in Tachyon with appropriate permissions.

The roles and permissions are described in the following table.

Role/Permission	Description
Viewer	This permission is required for any instruction set you want listed in the **Instruction Runner**. The **Viewer** permission is automatically included as part of the **Questioner** and **Actioner** permissions.
Questioner	This permission is required for any instruction set you want the Configuration Manager/Tachyon user to ask questions on using the **Instruction Runner**. The **Questioner** permission is automatically included as part of the **Actioner** permission.
Actioner	This permission is required for any instruction set you want the Configuration Manager/Tachyon user to run actions on using the **Instruction Runner**. If you are not using the **Instruction Runner** and want to run any of the other options directly accessible from the **Client Actions using Tachyon** sub-menu, you will need to set the **Actioner** permission on the **Microsoft Configuration Manager** instruction set for the Configuration Manager/Tachyon user.

In our example we use the following steps to define the user access for a specific Configuration Manager Console user, called **CMUser01**, to the **1E ConfigMgrConsoleExtensions** instruction set created earlier. This involves creating a custom role for that Instruction set and then assigning the custom role to the user. You

would normally use a domain security group for all of your Configuration Manager Console users, but here we are using a single user **CMUser01**.

To create a custom role:

1. Navigate to the **Settings**→**Permissions**→**Roles** page.
2. Click the **Add** button to start the add role process.
3. On the **New role** page set the name as **1E ConfigMgrConsoleExtensions** and click the **Save** button.
4. The new role will be added to the **Roles** page. Locate its entry and click on the link in the **Name** column for that row.
5. In the **Permissions** section:
    a. In the **Instruction Sets** list scroll down and select the **1E ConfigMgrConsoleExtensions** instruction set.
    b. Select the **Actioner** and **Questioner** checkboxes from the list of permissions.
    c. Click the **Save** button.
6. Navigate to the **Settings**→**Permissions**→**Assignments** page.
7. Select **1E ConfigMgrConsoleExtensions**.
8. Select the plus button and select the **CMUser01** and the **All Devices** management group, click **Save**.

1.10.1.2.4 Instructions

Instruction text (ReadablePayload)	Type	Description	Instruction file name	Version
What is the health of the SCCM clients (checking inventory has run and policy has been evaluated in the last <numdays> days)?	Question	Evaluates the ConfigMgr Client health on the device over the last <numdays> days. The health will be reported as 'Poor' if it has not updated any one of	**1E-ConfigMgrConsoleExtensions-ClientHealth**	17

Instruction text (ReadablePayload)	Type	Description	Instruction file name	Version
		the three time critical items. If all updated then they are considered 'Average' if two thirds of all the checks are ok, and 'Good' if everything is within expected parameters. This instruction makes use of a PowerShell script and will only work on Windows devices.		
What components are installed on the SCCM clients?	Question	Returns all the SCCM client components installed on the device. This instruction makes use of a	**1E-ConfigMgrConsoleExtensions-InstalledComponents**	17

Instruction text (ReadablePayload)	Type	Description	Instruction file name	Version
		PowerShell script and will only work on Windows devices.		
What Management Points are the SCCM clients using?	Question	Returns the ConfigMgr management points configured on the device. This instruction makes use of a PowerShell script and will only work on Windows devices.	**1E-ConfigMgrConsoleExtensions-ManagementPoint**	17
Enable and start the ConfigMgr client service (CcmExec) with a stagger of <limitSecs> seconds.	Question	Enables and starts the ConfigMgr client service (CcmExec). The service start will be delayed by a number of seconds up to the	**1E-ConfigMgrConsoleExtensions-StartConfigMgrClientService**	14

Instruction text (ReadablePayload)	Type	Description	Instruction file name	Version
		specified stagger value.		
Emergency stop and disabling of the ConfigMgr client service (CcmExec).	Question	Stops and disables the ConfigMgr client service (CcmExec).	**1E-ConfigMgrConsoleExtensions-StopConfigMgrClientService**	14
Trigger ConfigMgr client application deployment evaluation cycle with a stagger of <limitSecs> seconds.	Action	Triggers the application deployment evaluation cycle. This trigger will be delayed by a number of seconds up to the specified stagger value.	**1E-ConfigMgrConsoleExtensions-TriggerApplicationDeploymentEvaluationCycle**	14
Trigger ConfigMgr client health check and remediation with a stagger of <limitSecs> seconds.	Action	Trigger a client health check and remediation. This trigger will be delayed by a number of seconds up	**1E-ConfigMgrConsoleExtensions-TriggerClientHealthCheck**	15

Instruction text (ReadablePayload)	Type	Description	Instruction file name	Version
		to the specified stagger value.		
Trigger ConfigMgr client discovery data collection cycle with a stagger of <limitSecs> seconds.	Action	Trigger the discovery data collection cycle. This trigger will be delayed by a number of seconds up to the specified stagger value.	**1E-ConfigMgrConsoleExtensions-TriggerDiscoveryDataCollectionCycle**	14
Trigger a ConfigMgr client file collection cycle with a stagger of <limitSecs> seconds.	Action	Trigger a file collection cycle. This trigger will be delayed by a number of seconds up to the specified stagger value.	**1E-ConfigMgrConsoleExtensions-TriggerFileCollectionCycle**	14
Trigger a ConfigMgr client hardware inventory cycle with a stagger	Action	Trigger a hardware inventory cycle. This trigger will be delayed	**1E-ConfigMgrConsoleExtensions-TriggerHardwareInventoryCycle**	14

Instruction text (ReadablePayload)	Type	Description	Instruction file name	Version
of <limitSecs> seconds.		by a number of seconds up to the specified stagger value.		
Trigger a ConfigMgr client machine policy retrieval and evaluation cycle with a stagger of <limitSecs> seconds.	Action	Trigger a machine policy retrieval and evaluation cycle. This trigger will be delayed by a number of seconds up to the specified stagger value.	**1E-ConfigMgrConsoleExtensions-TriggerMachinePolicyRetrievalAndEvaluationCycle**	14
Trigger a ConfigMgr client software inventory cycle with a stagger of <limitSecs> seconds.	Action	Triggers the software inventory cycle. This trigger will be delayed by a number of seconds up to the specified stagger value.	**1E-ConfigMgrConsoleExtensions-TriggerSoftwareInventoryCycle**	14

Instruction text (ReadablePayload)	Type	Description	Instruction file name	Version
Trigger a ConfigMgr client software metering usage report cycle with a stagger of <limitSecs> seconds.	Action	Trigger a software metering usage report cycle. This trigger will be delayed by a number of seconds up to the specified stagger value	**1E-ConfigMgrConsoleExtensions-TriggerSoftwareMeteringUsageReportCycle**	14
Trigger a ConfigMgr client software update deployment evaluation cycle with a stagger of <limitSecs> seconds.	Action	Triggers a software update deployment evaluation cycle. This trigger will be delayed by a number of seconds up to the specified stagger value.	**1E-ConfigMgrConsoleExtensions-TriggerSoftwareUpdatesDeploymentEvaluationCycle**	14
Trigger a ConfigMgr client software update scan cycle with a stagger of	Action	Triggers a software update scan cycle. This trigger will be	**1E-ConfigMgrConsoleExtensions-TriggerSoftwareUpdatesScanCycle**	14

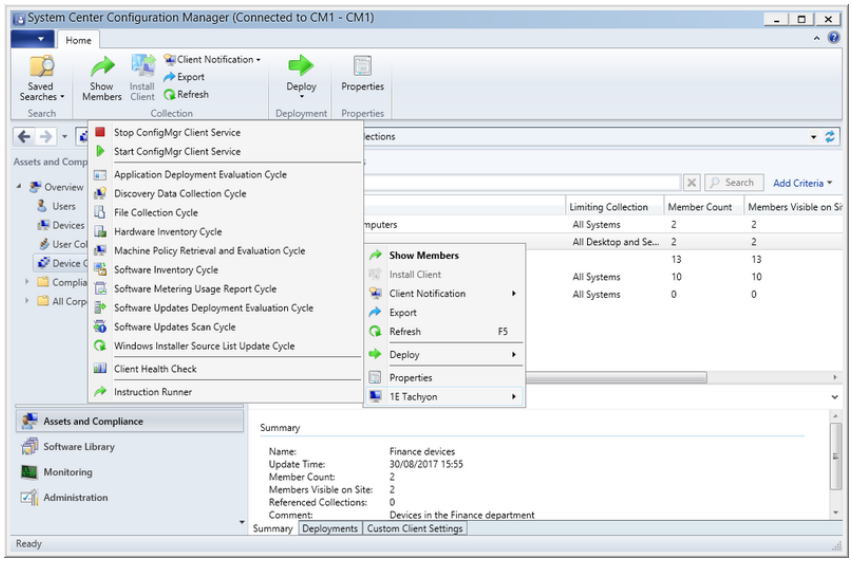
Instruction text (ReadablePayload)	Type	Description	Instruction file name	Version
<limitSecs> seconds.		delayed by a number of seconds up to the specified stagger value.		
Triggers a ConfigMgr client Windows installer source list update cycle with a stagger of <limitSecs> seconds.	Action	Triggers a Windows installer source list update cycle. This trigger will be delayed by a number of seconds up to the specified stagger value.	**1E-ConfigMgrConsoleExtensions-TriggerWindowsInstallerSourceListUpdateCycle**	14

1.10.2 Using Tachyon in Configuration Manager

The Configuration Manager Console extensions are an optional part of the 1E Tachyon Toolkit.

1.10.2.1 Options available on the Tachyon menu

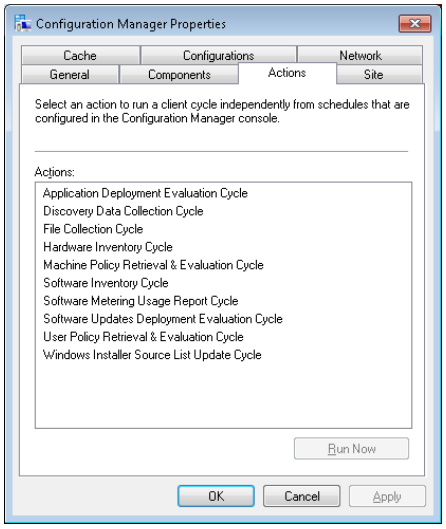
Once the Tachyon extensions for the Configuration Manager Console. extensions have been installed, a **Tachyon** sub-menu gets added to the context menu for device collections or devices. The following picture shows the Tachyon sub-menu on the All Systems device collection context menu**All Systems** device collection.



Most of the menu items, with the exception of the last **Instruction Runner**, work by getting Tachyon to perform an action where the coverage is set to a list of the FQDN of client devices that are members of the selected device collection. The actions must be approved using Explorer before they are performed on the target client devices.

There are four sections in the sub-menu, these sections, the menu items, and associated Tachyon actions are described in the following table:

Section	Menu item	Tachyon Action	Notes
Configuration Manager Agent emergency stop and resume actions These options can be used in emergency situations where the Configuration Manager Agent needs to be stopped immediately to prevent certain actions from taking place. A tutorial showing the stopping and restarting of the ConfigMgr Client Service is provided in Stopping and resuming the ConfigMgr Client Service - Tutorial.	Stop ConfigMgr Client Service	Emergency shutdown and disable the ConfigMgr client service.	Stops and then disables the CcmExec service on the target devices.
Start ConfigMgr Client Service	Restart and enable the ConfigMgr client	Enables and then starts the CcmExec service on the target devices with a random delay between 1 and 3600 seconds.	

	service with maximum stagger of 3600.		
Configuration Manager Agent actions These options provide a quick method for immediately invoking each of the Configuration Manager Agent actions via Tachyon, as shown in the following picture:  The one notable exception is that the **User Policy Retrieval & Evaluation Cycle** is not implemented because this must be run in the context of a specific user.	Application Deployment Evaluation Cycle	Trigger ConfigMgr client application deployment evaluation cycle with maximum stagger of <maxStagger> seconds.	Runs the Application Deployment Evaluation Cycle on the target devices with a random delay of <maxStagger> seconds. Where <maxStagger> is calculated when the action is selected according to the number of target devices. This is done so that the CM site server will be hit by no more than 10 devices per second.

Discovery Data Collection Cycle	Trigger ConfigMgr client discovery data collection cycle with maximum stagger of <maxStagger> seconds.	Runs the Discovery Data Collection Cycle on the target devices with a random delay of <maxStagger> seconds. See **Notes** for **Application Deployment Evaluation Cycle** above.
File Collection Cycle	Trigger ConfigMgr client file collection cycle with maximum stagger of <maxStagger> seconds.	Runs the File Collection Cycle on the target devices with a random delay of <maxStagger> seconds. See **Notes** for **Application Deployment Evaluation Cycle** above.
Hardware Inventory Cycle	Trigger ConfigMgr client hardware inventory cycle with maximum stagger of <maxStagger> seconds.	Runs the Hardware Inventory Cycle on the target devices with a random delay of <maxStagger> seconds. See **Notes** for **Application Deployment Evaluation Cycle** above.
Machine Policy Retrieval and Evaluation Cycle	Trigger ConfigMgr machine policy retrieval & evaluation cycle with	Runs the Machine Policy Retrieval & Evaluation Cycle on the target devices with a random delay of <maxStagger> seconds. See **Notes** for **Application Deployment Evaluation Cycle** above.

	maximum stagger of <maxStagger> seconds.	
Software Inventory Cycle	Trigger ConfigMgr software inventory cycle with maximum stagger of <maxStagger> seconds.	Runs the Software Inventory Cycle on the target devices with a random delay of <maxStagger> seconds. See **Notes** for **Application Deployment Evaluation Cycle** above.
Software Metering Usage Report Cycle	Trigger ConfigMgr software metering usage report cycle with maximum stagger of <maxStagger> seconds.	Runs the Software Metering Usage Report Cycle on the target devices with a random delay of <maxStagger> seconds. See **Notes** for **Application Deployment Evaluation Cycle** above.
Software Updates Deployment Evaluation Cycle	Trigger ConfigMgr software updates deployment evaluation cycle with maximum stagger of <maxStagger> seconds.	Runs the Updates Deployment Evaluation Cycle on the target devices with a random delay of <maxStagger> seconds. See **Notes** for **Application Deployment Evaluation Cycle** above.

Software Updates Scan Cycle	Trigger ConfigMgr software updates scan cycle with maximum stagger of <maxStagger> seconds.	Runs the Software Updates Scan Cycle on the target devices with a random delay of <maxStagger> seconds. See **Notes** for **Application Deployment Evaluation Cycle** above.	
Windows Installer Source List Update Cycle	Trigger ConfigMgr Windows installer source list update cycle with maximum stagger of <maxStagger> seconds.	Runs the Windows Installer Source List Update Cycle on the target devices with a random delay of <maxStagger> seconds. See **Notes** for **Application Deployment Evaluation Cycle** above.	
Client Health Check	Client Health Check	Trigger ConfigMgr client health check and remediation with maximum stagger of <maxStagger> seconds.	Invokes **Ccmeval.exe** on the target devices.
Instruction Runner See Instruction Runner.	Instruction Runner	AnyIf the user has permission, any Tachyon instruction from the currently imported product packs can be run using this option.	

1.10.2.2 Stopping and resuming the ConfigMgr Client Service - Tutorial

A quick tutorial on stopping and resuming the ConfigMgr Client Service in response to an emergency.

1.10.2.2.1 The example

Suppose a deployment of the **ACMEFinance** software has just been advertised to a number of devices across a range of departments using Configuration Manager and you've realized that the extra feature used by the Finance department has not been configured properly and will cause issues preventing the Finance department from doing their work. To make sure that the Finance devices are not affected by the implementation you want to immediately stop the Configuration Manager Client Service on just the Finance devices, until you can sort out the issue with the deployment.

The **1E Tachyon** menu, added to Configuration Manager after the extensions have been installed, is available on Device Collections and individual devices displayed in Configuration Manager. The top two items on the menu let you stop and resume the Configuration Manager Client Service on all the devices within the selected context. Tachyon will process the request as fast as it can, the most time-consuming part of the process would likely be the safety checks and balances of two-factor authentication and approval.

1.10.2.2.2 Selecting the emergency stop from the menu

The following steps show the complete workflow for running the **Stop ConfigMgr Client Service** action from the Tachyon menu in the Configuration Manager console:

1.10.2.2.2.1 Selecting the action and authenticating

1. The user **CMUser01** is logged in to the Configuration Manager console. They right-click on the Device Collection they want to target, in this case **Finance** devices, which has already been configured with the devices where the Configuration Manager Client Service needs to be stopped.

2. On the context menu, they expand the **1E Tachyon** sub-menu

3. They then select the **Stop ConfigMgr Client Service** item from the sub-menu

4. A dialog will be displayed asking if they really want to run the selected action and how many devices will be affected. They click **Yes** to continue

5. With two-factor authentication enabled the user is then be prompted for an authentication code for the instruction with the ID **1**

6. **CMUser01** then checks their email for the authentication email which is sent by Tachyon on requesting an action

7. Having copied the authentication code they then return to Configuration Manager, paste the code into the dialog and click **OK**

8. If the authentication passes, a dialog is then displayed that notifies the user that their reques has been submitted to Tachyon and how many devices it will be performed on after it has been approved.

1.10.2.2.2.2 Approving the action

The Tachyon actions triggered from the Configuration Manager console are approved in exactly the same way as any other Tachyon action.

1. A Tachyon approver for the Configuration Manager extensions product pack, in our example the full administrator **TCNAdmin01**, receives an email asking them to approve the requested action

2. The Approver can use the link at the bottom of the email to go directly to their Tachyon **Notifications** page, or they can browse the Tachyon Explorer and select the **Notifications** page independently from the email

3. On the **Notifications** page they can see the pending **Request for action approval**. Here they can view details related to the request in order to judge their approval

4. Once they have made their decision to approve they add a suitable comment and check the **I understand approving my request impacts my IT environment** checkbox

5. They can then click the **Approve** button to approve the request

6. Tachyon will respond to show them that their **Approval has been processed successfully**

1.10.2.2.2.3 Viewing the responses

1. After approval, **CMUser01** receives an email telling them that their action has been approved

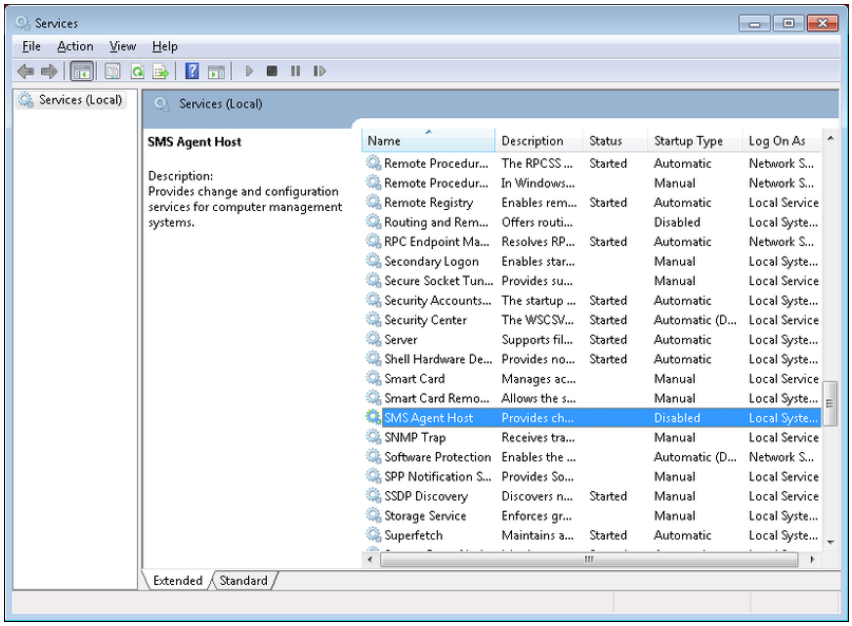
2. The email contains a **Go to results page** button. Clicking on this displays the results page for the approved instruction

3. The responses page shows the two devices in the **Finance devices** collection have responded to indicate that the Configuration Manager Client Service has been stopped and disabled

4. **CMUser01** then checks the information for one of the devices. They can see that the device has previously had the **DEPARTMENT = Finance** coverage tag set in Tachyon - showing for this device that the Device Collection defined in Configuration Manager corresponds to the finance department tags set using Tachyon.

1.10.2.2.2.4 Confirming the action has taken place

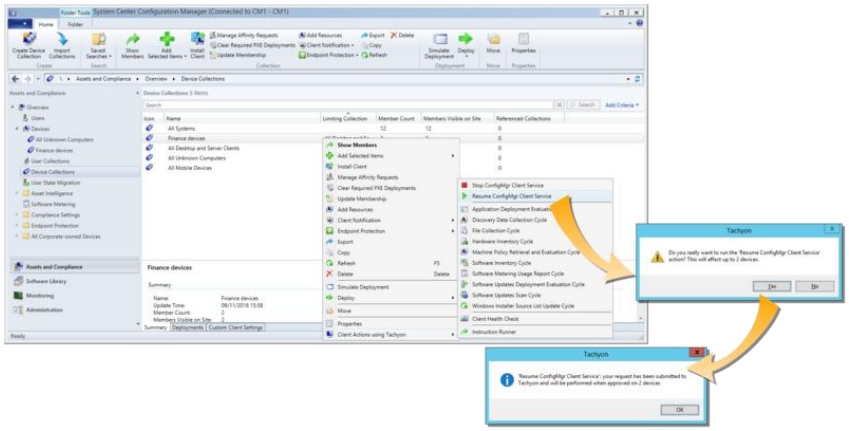
Going to one of the devices in question and opening the Services panel confirms that this is now the case, as shown in the picture.



1.10.2.2.3 After resolving the issue, restarting the Configuration Manager Client Service

Once you've resolved the configuration of the **ACMEFinance** software for the Finance department you will then want to restart the Configuration Manager Client Service. Doing this follows a similar process to stopping the service in that it involves selecting the menu option from Configuration Manager and then approving the subsequently created action in the Tachyon Explorer.

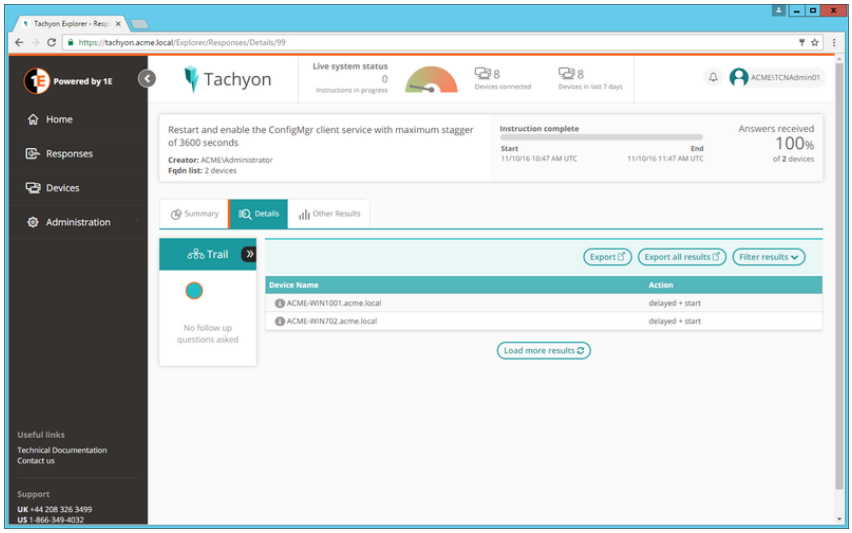
The picture shows the **Resume ConfigMgr Client Service** menu item being selected from the context menu for the **Finance devices** collection and the subsequent confirmation and notification dialogs.



When the **Resume ConfigMgr Client Service** menu item is selected from the Configuration Manager console an action named **Restart and enable the ConfigMgr client service with maximum stagger of 3600 seconds** gets added to Tachyon.

Following the normal approval process the action gets run on the Tachyon client devices. In the case of this action the time at which the Configuration Manager Client Service is started is subject to a random delay with a maximum of 3600 seconds. This is to prevent the Configuration Manager encountering problems through large numbers of client services attempting to contact it at the same time. This will mean that you may have to wait for an hour for the clients to be available to Configuration Manager again.

The picture shows the answers retrieved for the restart action.



1.10.2.3 Instruction Runner

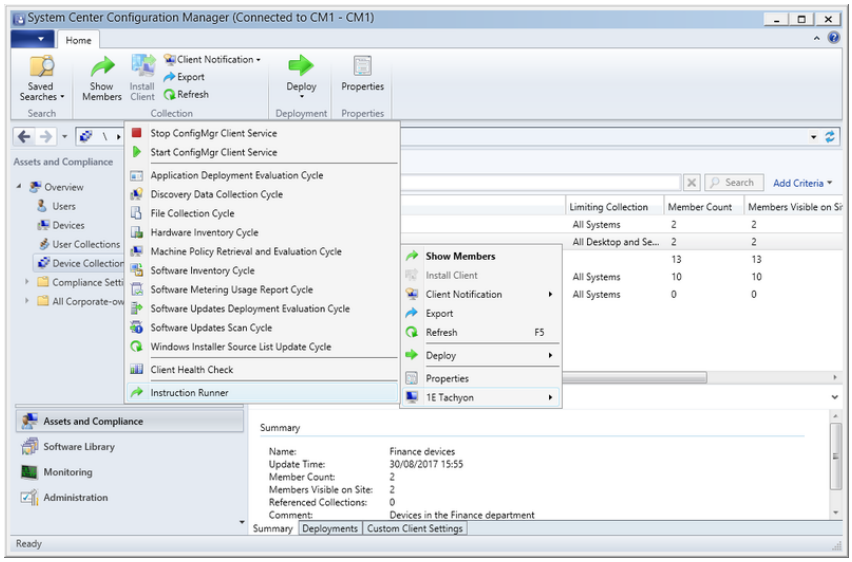
How to use the Instruction Runner to submit questions and actions from Configuration Manager. The Instruction Runner is a right-click tool for the Configuration Manager console which starts a client-based version of the Tachyon Explorer, which is limited to devices in a Collection.

1.10.2.3.1 Starting the Instruction Runner

The Instruction Runner can be started from the **1E Tachyon** context menu and by selecting the **Instruction Runner** menu item.

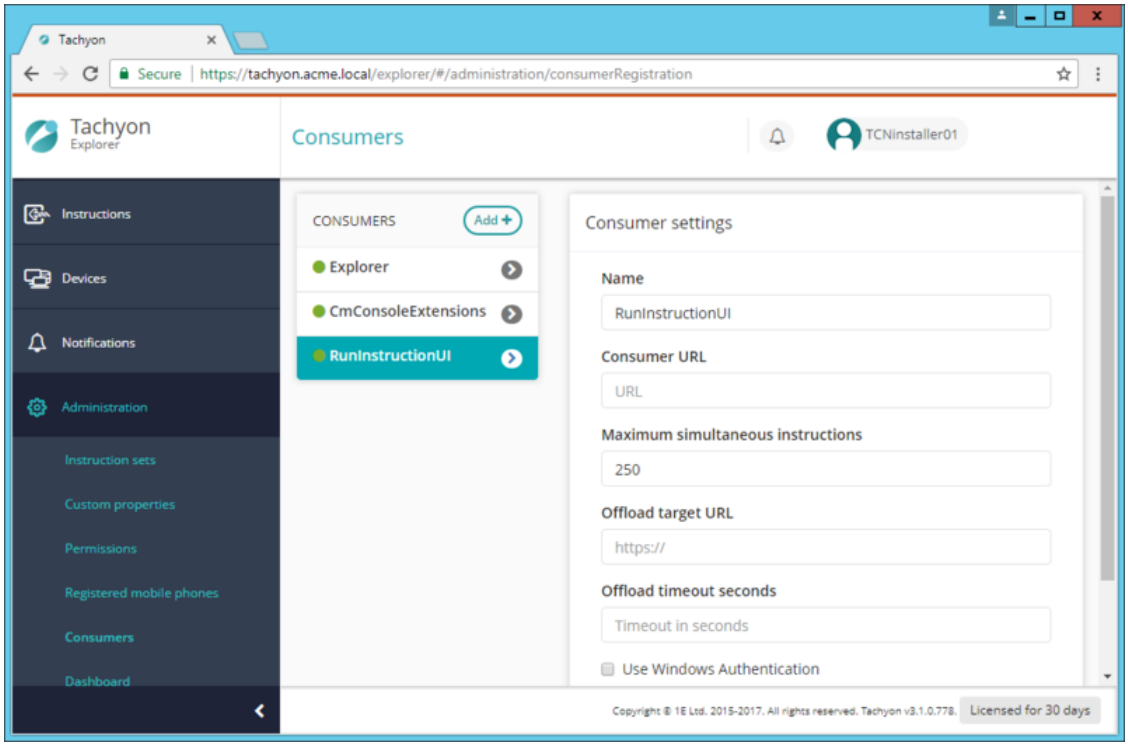
The context menu is displayed by right-clicking on a Device Collection in the Configuration Manager console. This Device Collection also defines the set of client devices that the Instruction Runner will question or action.

The picture shows the context menu for the **Finance devices** collection with the **1E Tachyon** sub-menu displayed and the **Instruction Runner** menu item selected.



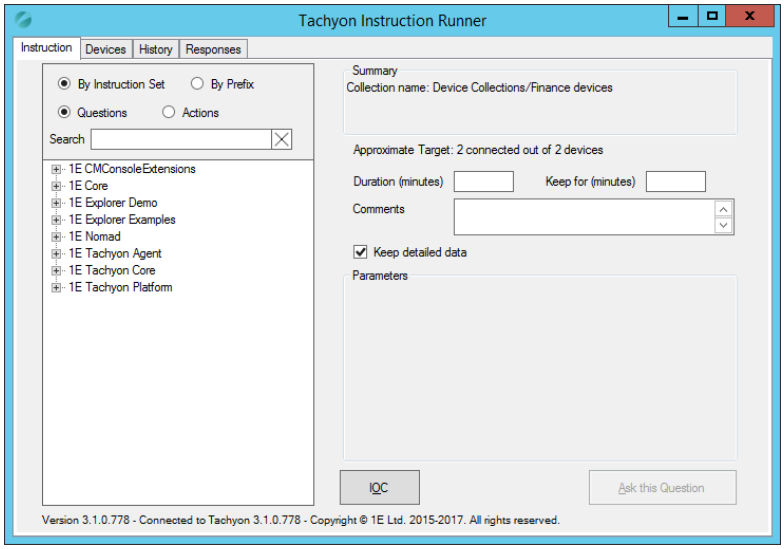
1.10.2.3.1.1 Loading the Instruction Runner for the first time

The first time the Instruction Runner menu item is selected, Tachyon will automatically attempt to create a Consumer for the Instruction Runner. For this to work correctly, the account used to run the Configuration Manager console must have the **Full Administrator** role assigned in Tachyon. If the appropriate permissions are there, a **RunInstructionUI** consumer will be created, as shown in the picture. This operation only needs to succeed once, and no further configuration is necessary.



1.10.2.3.1.2 The Instruction Runner

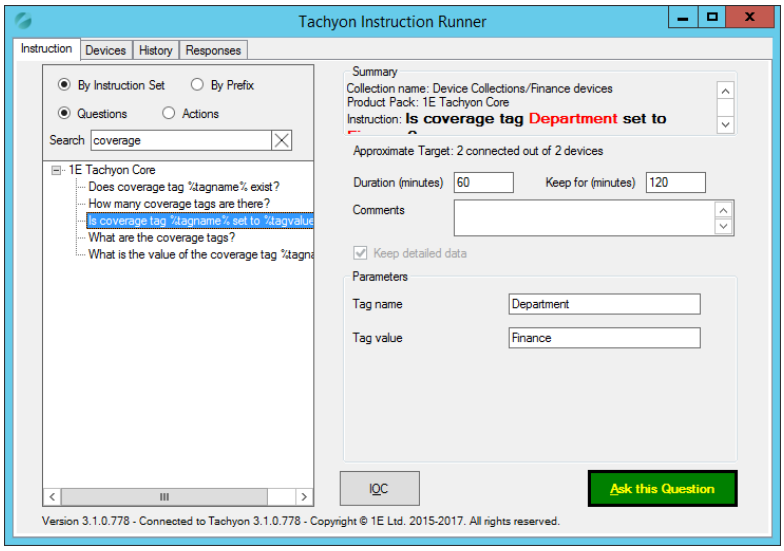
Selecting the Instruction Runner menu item starts the **Instruction Runner**. The picture shows the **Instruction Runner** with the **Instruction** tab selected.



1.10.2.3.2 Running a question on the Instruction tab

As an example, we're going to run an action to determine whether the Finance department devices all have the correct coverage tag set by Tachyon.

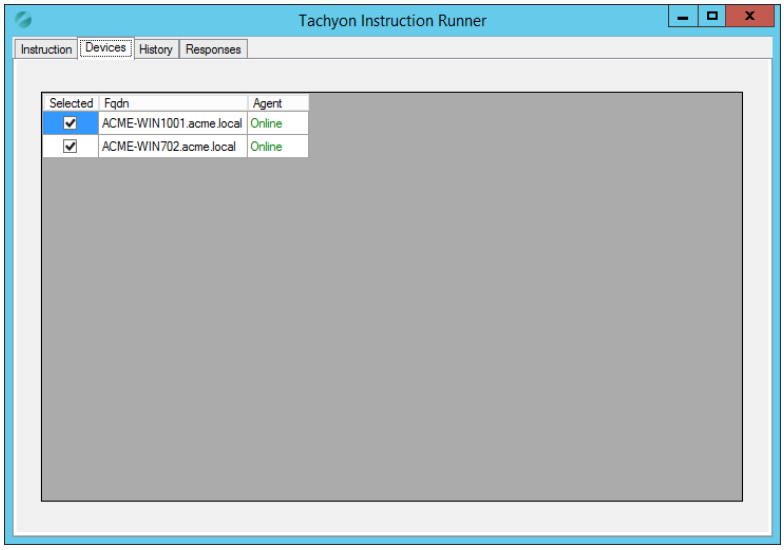
The picture shows the instructions sorted by product pack and with the questions displayed. The **Is coverage tag %tagname% set to %tagvalue%** question has been selected and the **Tag name** and **Tag value** fields have been set to **Department** and **Finance** respectively.



1.10.2.3.2.1 Looking at the Devices tab

The **Devices** tab shows the devices contained in the selected Configuration Manager Device Collection. In our example, as shown in the picture opposite, it shows the two devices in the **Finance devices** collection. You can further reduce the devices that the question will be run on by unchecking the checkbox at the beginning of the row with the device name you want to exclude.

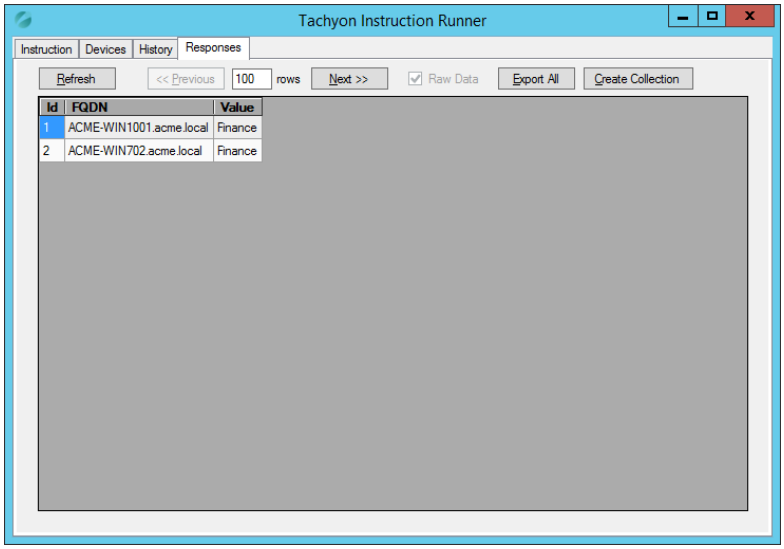
In our example, we will leave both devices selected, click back on the **Instruction** tab and click the **Ask this Question** button to run the question configured in the previous heading.



1.10.2.3.2.2 Checking the responses

Asking the coverage tag question displays the devices with that tag name and value set. In our example this results in two devices responding to say that they have the **Department Finance** tag

set. This exactly corresponds to the two devices on the **Devices** tab, so we can conclude that all the devices in the Finance department have the correct tag set.



1.10.3 Configuring NightWatchman Online Status

Tachyon uses a very secure, highly scalable, and extensible client-server architecture supporting a wide variety of operating systems and device types. A web interface allows authorized users to query all clients in your organization and get responses almost immediately. Users can also make immediate changes. Tachyon is especially valuable for addressing immediate concerns, such as newly discovered security vulnerabilities or to correct accidental misconfigurations. Despite its power and responsiveness, it is engineered to not overwhelm your network, clients, or servers.

For full details, refer to NightWatchman Enterprise 7.3 - Enabling Online Status using Tachyon integration.

1.10.4 Installing TIMS

TIMS is a graphical user interface for authoring and testing instructions, which can then be uploaded and used in your Tachyon system.

For full details, refer to /document/preview/736862#UUID-96565ece-64c7-9ede-a537-7addd547511a.

1.10.5 Setting up custom Tachyon Instructions for the first time

For a getting-started guide to configuring and verifying your Tachyon system so that you can run customized Instructions, refer to /document/preview/736871#UUID-66857689-bfb0-8dbc-ae8d-1de40c66fad9.

1.10.6 1E ITSM Connect

1.10.6.1 1E ITSM Connect 2.0 app

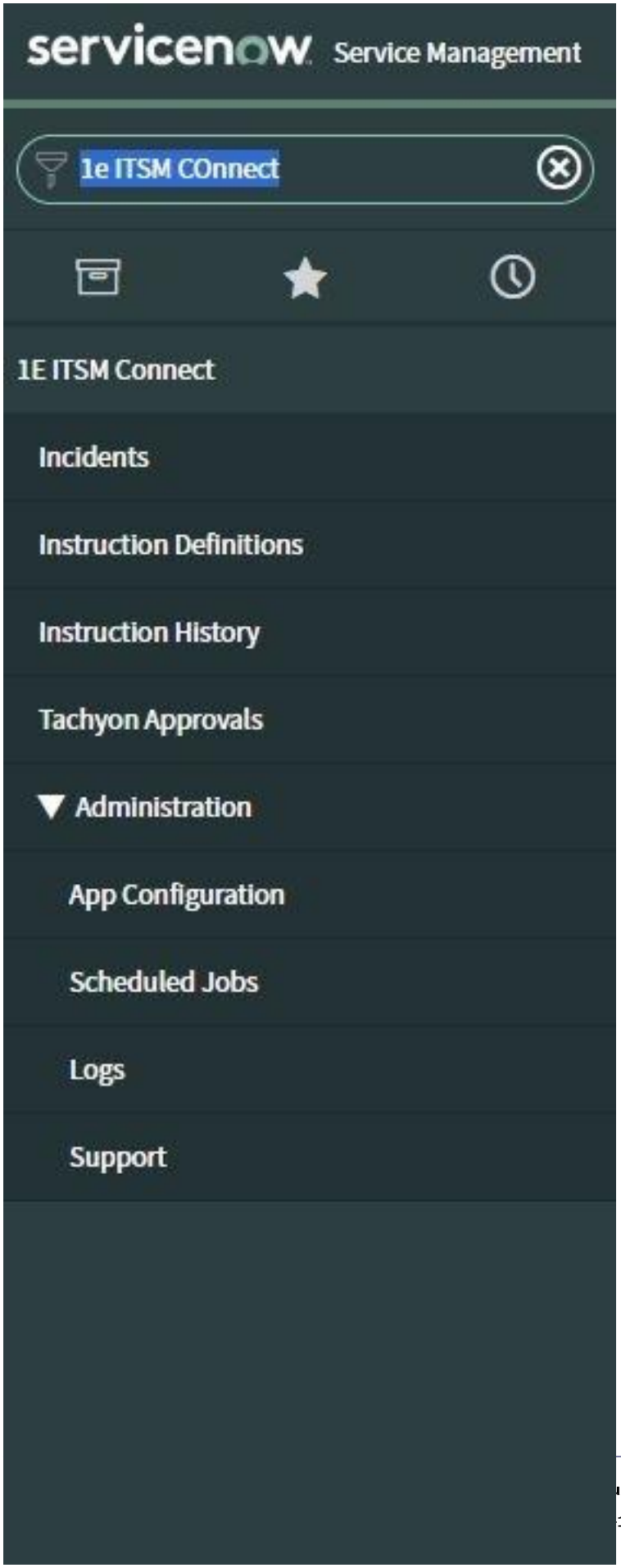
Integration between Tachyon and the ServiceNow ITSM (Information Technology Service Management) module is enabled using the 1E ITSM Connect 2.0 app, which is available for download from the ServiceNow app store and can be installed on any ServiceNow instance.

- 1E ITSM Connect now works with 1E Core, which provides connectivity to Tachyon and other core features for the 1E ServiceNow applications. Please refer to ITSM Connect - Requirements: Service Now requirements
- Instruction approval is now done in ServiceNow by ServiceNow users and not inside of Tachyon using a proxy Tachyon user. Please refer to ITSM Connect - Design Considerations: Tachyon Users and Roles for more details.
- Checkbox to configure if approval is needed/not needed for instruction in V2. ServiceNow Admin can choose which instructions require approval.
- Application settings and API configuration pages merged into 1 and called APP Configuration in V2.

To implement 1E ITSM Connect 2.0 please refer to ITSM Connect - Implementing 1E ITSM Connect.

1.10.6.2 App Menu in Application Navigator

ServiceNow provides an application navigator that enables users to navigate from one screen to another easily. To use **1E ITSM Connect**, first install it from ServiceNow app store and then search for **1E ITSM Connect** in the application navigator. The menu is shown below:


servicenow Service Management
1e ITSM COnnect
1E ITSM Connect
Incidents
Instruction Definitions
Instruction History
Tachyon Approvals
Administration
App Configuration
Scheduled Jobs
Logs
Support

Here's an overview of the 1E ITSM Connect menu items and the roles needed to access each page:

Item	Description	Roles needed to view the Item's page
Incidents	Displays a list of incidents.	• x_1e_connect.Tachyon_User • ITIL
Instruction Definitions	Displays a list of available Tachyon instructions.	Any of the following: • x_1e_connect.Tachyon_Admin • x_1e_connect.Tachyon_Approver • x_1e_connect.Tachyon_User n/a
Instruction History	Displays a history of previously run instructions.	Either of the following: • x_1e_connect.Tachyon_Admin • x_1e_connect.Tachyon_User n/a
Tachyon Approvals	Displays the instruction approval records generated from ServiceNow.	Either of the following: • x_1e_connect.Tachyon_Admin • x_1e_connect.Tachyon_Approver n/a
Administration	App Configuration	Displays the App Settings screen. • x_1e_connect.Tachyon_Admin n/a
Scheduled Jobs	Displays a list of any scheduled jobs	• x_1e_connect.Tachyon_Admin n/a

Item	Description	Roles needed to view the Item's page	
	specific to this app.		
Logs	Displays the app specific logs.	n/a	• admin(System Administrator)
Support	Displays information on how to contact 1E Support.	• x_1e_connect.Tachyon_Admin	n/a

1.11 Reference

All the list type information, such as installer properties, in alphabetical lists etc.

1.11.1 Supported Platforms

A list of all the platforms supported by Tachyon components, and the prerequisite software required to allow them to be installed or to work.

1.11.1.1 Server software

Category	Product	Notes
Server OS	• Windows Server 2022	For more detail about configuration of servers, please refer to Windows Server requirements.
	• Windows Server 2019	Only 64-bit server OS are supported. The server must be domain-joined.
	• Windows Server 2016	This version of Tachyon requires the server OS to be **English** because of a Known issues with certain regional settings.

Category	Product	Notes
		If TLS 1.0 is disabled, then please ensure you follow the steps in If TLS1.0 is disabled to add registry entries, for the 1E Catalog Update Service to successfully connect to the 1E Cloud Catalog. **Note** This list shows only those OS versions in mainstream support by Microsoft, and therefore supported by Tachyon, and by 1E Client 8.1. Please refer to Constraints of Legacy OS regarding the end of mainstream support. For Microsoft product lifecycle details, please refer to https://support.microsoft.com/en-us/lifecycle/search. Refer to Support for Microsoft Rapid-Release Cycle on https://support.1e.com/ for details of which Current Branch versions are supported by 1E products, and known issues regarding specific versions.
SQL Server and SQL Server Analysis Services (SSAS)	• SQL Server 2019 • SQL Server 2017	For more detail, please refer to SQL Server requirements. Standard and Enterprise editions of these versions of SQL Server and SQL Server Analysis Services (SSAS) are supported.

Category	Product	Notes
	• SQL Server 2016 SP3	SQL Server 2016 RTM is not supported due to some issues, which are resolved by SP3. **Note** Tachyon only supports AlwaysOn Availability Groups on **SQL Server Enterprise Edition**. Please refer to High Availability options for SQL Server for HA options and their requirements. **Note** If you intend to integrate with third-party business intelligence products such as Power BI, you must install the **Enterprise edition of SSAS** as per their requirements. A SQL Server database instance is required for the following databases: • **1ECatalog** • **ContentDistribution** (optional - required for Nomad) • **SLA-BI** (optional - required for Patch Success) • **SLA-Data** • **SLA-Integrate** • **SLA-Shared** • **TachyonExperience** (optional - required for Tachyon Experience)

Category	Product	Notes
		• **TachyonMaster** • **TachyonResponses** **SLA Inventory databases** Tachyon Setup can install the above databases on separate SQL Server instances, however SLA-Data, SLA-Integrate, and SLA-Shared must exist on the same instance. A SQL Server Analysis Services (SSAS) instance installed in **Multidimensional** mode is required for SLA Business Intelligence. **SLA Business Intelligence** SLA Business Intelligence (BI) is only required for the Patch Success application. Together, the SLA Platform and BI installers create the following: • A database called **SLA-BI** on the SQL Server database instance. • A MOLAP cube called **SLA-BI** on the SSAS instance. • A linked server for the SLA databases to get data from the SLA-BI database and then from the SLA-BI cube. • A linked server for the SLA-BI database to get data from the SLA databases.

Category	Product	Notes

- A datasource definition used by the SLA-BI cube to connect to the BI database.

If the SLA databases, BI database, or SSAS instance for BI, are on *different* SQL Servers then the BI installer enforces the use of a SQL login on each instance. If they are on the *same* SQL Server then the installer gives you a choice of using integrated security (domain user account) or a SQL login.

However, if you are installing all the components using Tachyon Setup instead of their individual installers, then you are not given the choice. Tachyon Setup always uses integrated security. Contact your 1E Account Team if your scenario requires the above-mentioned databases to be on *different* SQL Servers. This affects different servers, not different instances.

All SQL Server instances *must* be configured with the following:

- A case-insensitive, accent-sensitive collation which is **SQL_Latin1_General_CP1_CI_AS** by default,

Category	Product	Notes
		• **Allow remote connections t o this server** enabled. All SQL Servers should be configured with the **SQL Server Browser service** running in order for the BI installer to select from a list of instances. **SQL Server Management Studio** is required to review the configuration and edit settings in 1E database tables. If installing SQL Server locally, note: • SQL Server 2016 and 2017 require .NET Framework 4.6 or later • SQL Server setup requires PowerShell 2.0. For the latest information about SQL Server prerequisites, please refer to http://go.microsoft.com/fwlink/?LinkId=622999.
Microsoft Endpoint Configuration Ma nager	• MECM CB 2303 • MECM CB 2211 • MECM CB 2207 • MECM CB 2203 • MECM CB 2111	Tachyon uses Configuration Manager for the following optional apps and features: • Reclaiming a product using SCCM Uninstall • Introducing Application Migration • Introducing Inventory captures data using the System Center Configuration Manager connector • Tachyon extensions for the Configuration Manager

Category	Product	Notes
	• MECM CB 2107	Console. - installed on Configuration Manager consoles using the 1E Tachyon Toolkit installer • Introducing Nomad requires 1E Client with Nomad client features enabled. Nomad provides the following Content Distribution features for Configuration Manager: • Nomad app overview provides visibility of content distribution activity • Single Site Download (SSD) (SSD). • Task sequence actions to augment OS Deployment: – Peer Backup Assistant - PBA – High Availability PBA (HAPBA) – Get Migration Settings to manage computer associations. • Nomad Pre-caching • Nomad Download Pause. Nomad requires the Content Distribution web service to synchronize with the Configuration Manager database. For standalone primary site environments, permissions are automatically assigned to the service account of Content Distribution's web application pool service (by default

Category	Product	Notes
		Network Service) using the **ConfigMgr_DViewAccess** localgroup native to Configuration Manager. For a CAS, this group is not created natively therefore additional steps are required to allow access. Please refer to Preparation: Microsoft Endpoint Configuration Manager preparation.
Web Server	• IIS 10	See Windows Server roles and features for details about required Web Server roles and features.
Runtime libraries	• Visual C++ 2013 Redistributable • Visual C++ 2015-2019 Redistributable • ASP.NET Core Framework 3.1 • .NET Framework 4.8	See Windows Server roles and features for details about required .NET Framework roles and features. To know supported combinations of OS and .NET Framework, please refer to: https://docs.microsoft.com/en-us/dotnet/framework/migration-guide/versions-and-dependencies. • Windows Server 2022 has .NET Framework 4.8 installed by default. • Windows Server 2019 has .NET Framework 4.7.2 installed by default. • Windows Server 2016 has .NET Framework 4.6.2 installed by default. **ASP.NET Core Hosting Bundle** is required only for the Nomad. It is not included with the Operating System, and must be downloaded and installed separately. If it not already installed, Tachyon Setup

Category	Product	Notes
		will attempt to automatically download version **3.1.11** and install it. Alternatively you can download it, or a later version, and install it yourself. For more detail please refer to ASP.NET Core Hosting Bundle. Installers include and automatically installs the redistributable packages for **Visual C++ 2013** and **Visual C++ 2015-2019**. The Coordinator (licensing module on the Master Stack), and Switch (on Response Stack) are written in C++ using Visual Studio 2013 and 2019, therefore require the **runtime (x64)** versions of these packages. Other server components use .NET Framework. **SQL BCP** is required by the **Export All** feature described in Exporting data from Explorer, and must be installed on each Tachyon Response Stack server (specifically the servers which have the Tachyon Core installed). BCP uses ODBC, which requires **Microsoft ODBC Driver versions 13. 1 and 17** and **Visual C++ 2017 Redistributable** to be installed first. Please refer toP SQL BCP for more detail.
Other software	• PowerShell	PowerShell is required by Tachyon installer during installation.
Browsers	Latest version of: • Google Chrome	A browser is not a prerequisite for installation of Tachyon servers but is required to use and administer the Tachyon platform. The administration is performed via the

Category	Product	Notes
	• Microsoft Edge (Chromium) • Mozilla Firefox	Tachyon portal and can be on a remote computer. These browsers are supported on all OS platforms which the browser vendor supports. The Portal and any API should be added as a trusted site. This is especially important when running scripts that may produce unexpected errors. Please review Known Issues Using Tachyon. **Note** **Microsoft legacy browsers** Support has been withdrawn for **Internet Explorer 11** and **legacy Microsoft Edge** (non-Chromium version) because Microsoft no longer supported them since 2021. We recommend you use Google Chrome, Firefox, or Microsoft Edge Chromium browser.

1.11.1.2 Tachyon portal

Category	Product	Notes
Browsers	Latest version of: • Google Chrome	These browsers are supported on all OS platforms which the browser vendor supports. Please refer to Whitelisting connections to 1E Cloud for details of URL that must be whitelisted for administrator browsers.

Category	Product	Notes
	• Microsoft Edge (Chromium)	The Portal and any API should be added as a trusted site. This is especially important when running scripts that may produce unexpected errors.
	• Mozilla Firefox	Please review Known Issues: Using Tachyon. **Note** **Microsoft legacy browsers** Support has been withdrawn for **Internet Explorer 11** and **legacy Microsoft Edge** (non-Chromium version) because Microsoft no longer supported them since 2021. We recommend you use Google Chrome, Firefox, or Microsoft Edge Chromium browser.

1.11.1.3 1E Tachyon Toolkit

1.11.1.3.1 Configuration Manager console extensions

Category	Product	Notes
Client OS	• Windows Server 2022 • Windows Server 2019 • Windows Server 2016 • Windows 11 CB 22H2 • Windows 11 CB 21H2 • Windows 10 CB 22H2 • Windows 10 CB 21H2	For OS supported by Configuration Manager Current Branch (CB) see supported configurations for Configuration Manager, https://technet.microsoft.com/en-us/library/mt589499.aspx
Microsoft Endpoint Configuration Manager console	• MECM CB 2303	These are the versions of Configuration Manager that 1E has tested and

Category	Product	Notes
	• MECM CB2211 • MECM CB 2207 • MECM CB 2203 • MECM CB 2111 • MECM CB 2107	therefore support, but later versions are assumed to work also. Please see Preparing for the Tachyon extensions for the Configuration Manager Console..
Runtime libraries	• Visual C++ 2015-2019 Redistributable	1E Tachyon Toolkit installer includes the Visual C++ 2015-2019 Redistributable package.

1.11.1.4 TIMS

Category	Product	Notes
Windows OS	• Windows Server 2022 • Windows Server 2019 • Windows Server 2016 • Windows 11 CB 22H2 • Windows 11 CB 21H2 • Windows 10 CB 22H1 • Windows 10 CB 21H2	Professional and Enterprise editions of Windows 10 and 11 are supported. All versions are provided with 32-bit & 64-installers. TIMS is currently only available for Windows OS. For installation guidance, please refer /document/preview/736744#UUID-69b33e47-7b6d-90dc-e5a4-7bb34231ba85.

Category	Product	Notes
Runtime libraries	• .NET Framework 4.8 • Visual C++ 2015-2019 Redistributable	One of these versions of .NET Framework is required. **Note** Tachyon supports .NET Framework versions that are in mainstream support by Microsoft. For Microsoft product lifecycle details, please refer to https://support.microsoft.com/en-us/lifecycle/search. TIMS installer includes the Visual C++ 2015-2019 Redistributable package.
Other Windows Software	• PowerShell 3.0 (or later)	PowerShell 3.0 or later is required when testing instructions that have PowerShell commands embedded or scripts that are downloaded.

1.11.1.5 Connectors

The following table shows the supported versions of software used by the Tachyon out-of-box connectors.

Connector	Product	Notes
BigFix	• BigFix	Please refer to the BigFix connector or BigFixInv connector pages for prerequisites.
Intune	• Intune	Please refer to the Intune connector page for prerequisites.
Microsoft Office 365	• Azure	Please refer to the Microsoft Office 365 connector page for prerequisites.
OpenLM	• OpenLM Server	Please refer to the OpenLM connector page for prerequisites.

Connector	Product	Notes
	21.12	
Oracle LMS	• Oracle LMS	Please refer to the Oracle LMS connector page for prerequisites.
ServiceNow	• ServiceNow Jakarta release	Please refer to the ServiceNow connector page for prerequisites.
System Center Configuration Manager	• MECMCB2211 • MECMCB2207 • MECMCB2203 • MECMCB2111 • MECMCB2107	Please refer to the System Center Configuration Manager connector page for prerequisites.

Connector	Product	Notes
Tachyon	• Tachyon 8.1	Please refer to the Tachyon connector page for prerequisites.
vCenter	• VMware PowerCLI 11.1.0	VMware PowerCLI 11.1.0 (code.vmware.com/web/dp/tool/vmware-powercli/11.1.0) must be installed on the Tachyon Master server (where the SLA Integrate Services Agent service is hosted) before you can configure and use the vCenter connector. Earlier or later versions of PowerCLI are not supported and may cause errors. VMware PowerCLI is freeware and was previously known as vSphere PowerCLI. VMware PowerCLI supports multiple versions of VMware vCenter Server. For details, please refer to the VMware compatibility matrix using the following link: https://www.vmware.com/resources/compatibility/sim/interop_matrix.php#interop&2=&106= Please refer to the vCenter connector page for configuration details.
WSUS (Windows Server Update Services)	• WSUS	Please refer to the Windows Server Update Services connector page for configuration details.

1.11.1.6 Constraints of Legacy OS

In this documentation, the following are referred to as legacy OS. Below are described some known issues for these OS.

1E does not provide support for 1E products on the following OS unless the OS is explicitly listed as being supported for a specific 1E product or product feature. This is because Microsoft has ended mainstream support for these OS or they are not significantly used by business organizations.

- **Windows XP ***
- **Windows Vista**
- **Windows 7**
- **Windows 8.0**
- **Windows Server 2003 ***
- **Windows Server 2008**
- **Windows Server 2008 R2**
- **Windows Server 2012**

- **Windows 8.1**
- **Windows Server 2012 R2**

Note

1E Client 8.1 and later will not install on Windows XP and Windows Server 2003. Please contact 1E if you intend to continue using any of the other legacy OS. If you experience an issue, then please try replicating the issue on a supported OS.

For Microsoft product lifecycle details, please refer to https://support.microsoft.com/en-us/lifecycle/search.

1.11.1.6.1 Microsoft legacy browsers

Support has been withdrawn for **Internet Explorer 11** and **legacy Microsoft Edge** (non-Chromium version). 1E has taken this decision for new releases that are expected to remain in support by 1E beyond March 2021 when **Microsoft Edge** goes end of life and August 2021 when **Internet Explorer 11** goes end of life. We recommend you use Google Chrome, Firefox or Microsoft Edge Chromium browser.

1.11.1.6.2 Certificate limitations - SHA2

Like most software vendors, 1E software requires the OS to support SHA2. If your organization has a PKI configured to use SHA2 256 or higher encryption, then your legacy OS may have already been updated to support it.

- Windows XP and Server 2003 require an update as described in **KB968730.** Microsoft no longer provides this hotfix as a download. You must contact Microsoft Support if you need it
- Windows 7 and Server 2008 R2 require an update as described in **KB3033929**. This update is not available for Vista and Server 2008
- Windows 8, 8.1, Server 2012, Server 2012 R2 and later OS already support SHA2.

1.11.1.6.3 Certificate limitations - encrypted certificate requests

Windows XP and Server 2003 are unable to encrypt certificate requests, whereas later OS are able to support higher more secure RPC authentication levels. If you are using a Microsoft CA and expect these clients to request (enrol) certificates then the CA must have its IF_ENFORCEENCRYPTICERTREQUEST flag disabled. It is disabled by default on Windows 2003 and 2008 CA, but is enabled by default on Windows 2012 CA.

To determine which InterfaceFlags are set, execute the following command on the CA server:

```
certutil -getreg CA\InterfaceFlags
```

If the following is specified then it means the flag is enabled.

```
IF_ENFORCEENCRYPTICERTREQUEST -- 200 (512)
```

To disable the encrypt certificate requests flag, execute the following commands on the CA server:

```
certutil -setreg CA\InterfaceFlags -IF_ENFORCEENCRYPTICERTREQUEST
sc stop certsvc
  sc start certsvc
```

1.11.1.6.4 Certificate limitations - signing certificates missing

On Windows computers, the installation MSI files, and binary executable and DLL files of 1E software are digitally signed. The 1E code signing certificate uses a timestamping certificate as its countersignature. 1E occasionally changes its code signing certificate, and uses it for new releases and patches for older versions, as shown in the table(s) below.

Root Certificate Authorities are implicitly trusted to validate certificates, and their certificates must be correctly installed to do this. Your computers should already have the necessary **root CA** certificates installed, however this may have been prevented by your organization's security policies, or inability to connect to the Internet, or they are legacy OS. In general this is not an issue because by default Windows allows software to be installed and run without validation, although you may see a warning or experience a delay. However, you *must* have relevant CA certificates installed if you are using 1E Client (which self-validates its own files), or your organization has applied more secure polices (for example UAC, AppLocker or SmartScreen).

Typical reasons for issues with signing certificate are:

- If your organization has disabled **Automatic Root Certificates Update** then you must ensure the relevant **root CA** certificates are correctly installed on each computer
- If computers do not have access to the Internet then you must ensure the relevant **root and issuing CA** certificates are correctly installed on each computer, numbered in the table(s) below.

The signature algorithm of the 1E code signing certificate is SHA256RSA. In most cases, the file digest algorithm of an authenticode signature is SHA256, and the countersignature is a RFC3161 compliant timestamp. The exception is on legacy OS (Windows XP, Vista, Server 2003 and Server 2008) which require the file digest algorithm of an authenticode signature to be SHA1, and a legacy countersignature.

The table below applies to software and hotfixes released in 2020.

2020	Signing certificate	Timestamping certificates
Certificate	1E Limited	TIMESTAMP-SHA256-2019-10-15 ***and*** DigiCert Timestamp Responder
Issuing CA	**DigiCert EV Code Signing CA (SHA2)** Thumbprint: 60ee3fc53d4bdfd1697ae5beae1cab1c0f3ad4e3	**DigiCert SHA2 Assured ID Timestamping CA** Thumbprint: 3ba63a6e4841355772debef9cdcf4d5af353a297 ***and*** **DigiCert Assured ID CA-1**

2020	Signing certificate	Timestamping certificates
		Thumbprint: 19a09b5a36f4dd99727df783c17a51231a56c117
Root CA	**DigiCert High Assurance EV Root CA** Thumbprint: 5fb7ee0633e259dbad0c4c9ae6d38f1a61c7dc25	**DigiCert Assured ID Root CA** Thumbprint: 0563b8630d62d75abbc8ab1e4bdfb5a899b24d43

1.11.1.6.5 Certificate limitations - expired root certificates

Ensure that your Root CA Certificates are up-to-date on clients and servers. The **Automatic Root Certificates Update** feature is enabled by default, but its configuration may have been changed or restricted by Group Policy **Turn off Automatic Root Certificates Update**.

If this GPO is enabled, then you will see *DisableRootAutoUpdate = 1 (dword)* in *HKLM\Software\Policies\Microsoft\SystemCertificates\AuthRoot.*

1.11.2 Communication Ports

Diagrams and tables with all the external Tachyon communication ports. Useful, if needed, for network and device firewalls.

Please refer to Tachyon Architecture for architecture diagrams.

1.11.2.1 Connections diagram

The diagram shows connections for Tachyon and its applications. It includes connections from clients and administration workstations, and outgoing connections to inventory sources, and to Microsoft Endpoint Configuration Manager that is optionally used by some applications.

It does not show connections for WakeUp, NightWatchman Enterprise, or Shopping, which have their own back-end servers. Their connection diagrams can be found in their documentation.

1.11.2.2 Firewall requirements for a Single-Server

The following table lists firewall requirements for a **single-server** where **Tachyon Master Stack** and **Response Stack** are installed on the same server. The table assumes a remote SQL Server hosting TachyonMaster and TachyonResponses databases. Each Tachyon component described in the table has at least one output and/or input. For each Tachyon component with output, there is a matching input.

Firewalls normally protect against incoming traffic from remote devices, however, the table below also includes outgoing connections. The table does not include internal communications within the Server.

In addition to but not included in the table are various ports that Tachyon uses to communicate with Microsoft services, including Certificate Services and Active Directory. The Coordinator **Workflow service** queries AD for email details; the **Consumer API** queries AD for security details.

Port requirements are not provided here for Nomad, Shopping and WakeUp modules of the **1E Client**. Only the ports used by the client feature of the **1E Client** are listed.

If Nomad is being used by the client on Windows computers, it has additional port requirements of its own, which are not changed by Tachyon.

Additional ports may be required if Tachyon instructions need to connect to non-Tachyon content sources.

There may be additional requirements if the environment has had default security settings changed.

1.11.2.2.1 Tachyon Servers

Device	Port	Protocol	Direction	Usage	Configurable
Tachyon Server (Master Stack)	TCP 443	HTTPS	Incoming	• Console browser connections to **Tachyon Portal UI** • Console browser connections to **SLA Platform UI** • Console browser connections to	Yes, during installation. In the **Website Configuration** panel in Tachyon Setup. See #UUID44187c3f8a182c06d4353770a23bb3e4_id_TachyonServerinstallerpropertiesHTTPSIISPORTHTTPSIISPORT. Setup installs other components using the same settings as Tachyon Server.

Device	Port	Protocol	Direction	Usage	Configurable
				1E Catalog UI • Consumer connections to **Catalog API** • Consumer connections to **Consumer API** • Consumer connections to **SLA Operations Provider API**	
Tachyon Server (Master Stack)	TCP 80	HTTP	Incoming	• Console browser connections to **SLA Platform UI**	Yes, during installation. In the **Website Configuration** panel in Tachyon Setup. See #UUID44187c3f8a182c06d4353770a23bb3e4_id_TachyonServerinstallerpropertiesHTTPSIISPORTHTTPSIISPORT. Tachyon Setup installs other components using the same settings as Tachyon Server.

Device	Port	Protocol	Direction	Usage	Configurable
				• Console browser connections to **1E Catalog UI** • Consumer connections to**Catalog API** • Consumer connections to **SLA Operations Provider API**	
Tachyon Server (Response Stack)	TCP 443	HTTPS	Incoming	• Client retrieving content from the **Background Channel**.	Yes, during installation. In the **Website Configuration** panel in Tachyon Setup. See #UUID44187c3f8a182c06d4353770a23bb3e4_id_TachyonServerinstallerpropertiesHTTPSIISPORTHTTPSIISPORT.

Device	Port	Protocol	Direction	Usage	Configurable
Tachyon Server (Master Stack)	TCP 443	HTTPS	Outgoing	• Tachyon **Coordinator service** contacting the **1E Cloud License Service** via an Internet connection. • **1E Catalog Update service** contacting the **1E Cloud Catalog Service** via an Internet connection.	The port used to connect to the **1E Cloud Services** is not configurable.
Tachyon Server (Master Stack)	TCP 6002	WebSocket (ws)	Incoming Ou	• **Integrate Agent** service connecting to	Yes, configurable after installation. **Note** **Integrate Agent** component is not shown on the diagram, and

Device	Port	Protocol	Direction	Usage	Configurable
			tgoing	the **Integrate Manager Web API** to get connector jobs	installation on remote systems is not supported.
Tachyon Server (Response Stack)	TCP 4000	WebSocketSecure (wss)	Incoming	• Client receiving instructions from and sending compressed responses to the Tachyon Switch.	Switch ports are not configurable using the Server installer. A Switch port can be changed post-installation, by configuring the value in the **Port** column for the relevant Switch in the **SwitchConfiguration** table in the Tachyon Master database. If the Switch port is changed after deploying 1E Client (with Tachyon features enabled) then the corresponding Switch port must be updated in each Client's configuration file. Clients initiate and maintain a WebSocket Secure connection to a Switch, which the Switch uses to communicate back to the clients.
Tachyon Server (Master Stack)	TCP 25	SMTP	Outgoing	• Tachyon **Coordinator service** sending two-factor authenticatio	Yes. In this version of Tachyon, **SMTP Authentication** is not configurable using the Server installer. The default is anonymous authentication. However, it can be changed post-installation. For details of changing the SMTP configuration and disabling email notifications, please refer to Changing the SMTP Host configuration.

Device	Port	Protocol	Direction	Usage	Configurable
				n emails. • Tachyon **Coordinator service** sending workflow emails.	
Tachyon Server (Master Stack)	TCP 1433	TDS	Outgoing	• Tachyon Web Site application pools (**Portal**, **Consumer API**) communicating with SQL Server. • SLA Platform Web Site application pools (**Admin**,	Not configurable from Setup. In the **Database Servers** panel in Tachyon Setup you can select a SQL Server instance. The instance can be installed using a non-standard port. However, selecting an instance that uses a non-standard port will not change the port used by the Tachyon Installer, and installation will fail. If you require the use of a non-standard port on a Default SQL Server instance, contact 1E for guidance on a manual workaround. If using a Named Instance that is set to its default configuration where the server automatically chooses a random port (or if you manually configured the instance to use a fixed port), then the **SQL Browser** service needs to be enabled to let the Tachyon Server determine the port in use. You will need to open UDP port 1434 used by the SQL Browser. See #UUID44187c3f8a182c06d4353770a23bb3e4_id_TachyonServerinstallerpropertiesSQLSERVER_MASTERSQLSERVER_MASTER.

Device	Port	Protocol	Direction	Usage	Configurable
				CoreExternal, **Platform**) communicating with SQL Server. • Tachyon **Coordinator service** communicating with SQL Server. • Catalog services and application pool communicating with SQL Server. • **1E Catalog Update serv**	

Device	Port	Protocol	Direction	Usage	Configurable
				ice communicating with SQL Server.	
Tachyon Server (Master Stack)	TCP 1433	TDS	Outgoing	• Inventory connectors fetching data from sources that use SQL Server.	Configurable in various Connectors, please refer to Connectors page.
Tachyon Server (Master Stack)	TCP 135 and 445 (initially)	WMI (DCOM)	Outgoing	• SCCM WMI Server provider connection to Configuration Manager. • Nomad connection to Configuration	Not configurable. Please refer to Provider configuration page and Nomad.

Device	Port	Protocol	Direction	Usage	Configurable
				Manager used by the Nomad Sync feature.	
Tachyon Server (Response Stack)	TCP 1433	TDS	Outgoing	• Tachyon Web Site application pools (**Core** and **Core Internal**) communicating with SQL Server (mainly uncompressed responses).	Not configurable from Setup. See the comments above for the Tachyon Server (Master Stack). See #UUID44187c3f8a182c06d4353770a23bb3e4_id_TachyonServerinstallerpropertiesSQLSERVER_RESPONSESSQLSERVER_RESPONSES.
SQL Server (TachyonMaster	TCP 1433	TDS	Incoming	• Tachyon Web Site application pools (**Consu**	Not configurable from Setup. See the comments above for the Tachyon Server (Master Stack). See #UUID44187c3f8a182c06d4353770a23bb3e4_id_Tac

Device	Port	Protocol	Direction	Usage	Configurable
database)				**mer API**, **Portal**) communicating with SQL Server. • Tachyon **Coordinator service** communicating with SQL Server. • Tachyon Web Site application pools (**Core**) communicating with SQL Server.	hyonServerinstallerpropertiesSQLSERVER_MASTERSQLSERVER_MASTER.
SQL Server (TachyonResponses	TCP 1433	TDS	Incoming	• Tachyon Web Site application	Not configurable from Setup. See the comments above for the Tachyon Server (Master Stack).

Device	Port	Protocol	Direction	Usage		Configurable
database)					pools (**Core** and **Core Internal**) communicating with SQL Server (mainly uncompressed responses).	See #UUID44187c3f8a182c06d4353770a23bb3e4_id_TachyonServerinstallerpropertiesSQLSERVER_RESPONSESSQLSERVER_RESPONSES.

1.11.2.2.2 Tachyon clients

Device	Port	Protocol	Direction	Usage		Configurable
Clients	TCP 4000	WebSocket Secure (wss)	Outgoing	•	Client receiving instructions from and sending **compressed responses** to the Tachyon Switch.	Yes. See Tachyon client settings. Switch=<SwitchName>:<SwitchPort> Anything other than port 4000 requires a Tachyon Server with a Switch using the same port number. Clients initiate and maintain a WebSocket Secure connection to a Switch, which the Switch uses to communicate back to the client.
Clients	TCP	HTTPS	Outgoing	•	Client retrieving content from the	Yes, during installation. See Tachyon client settings.

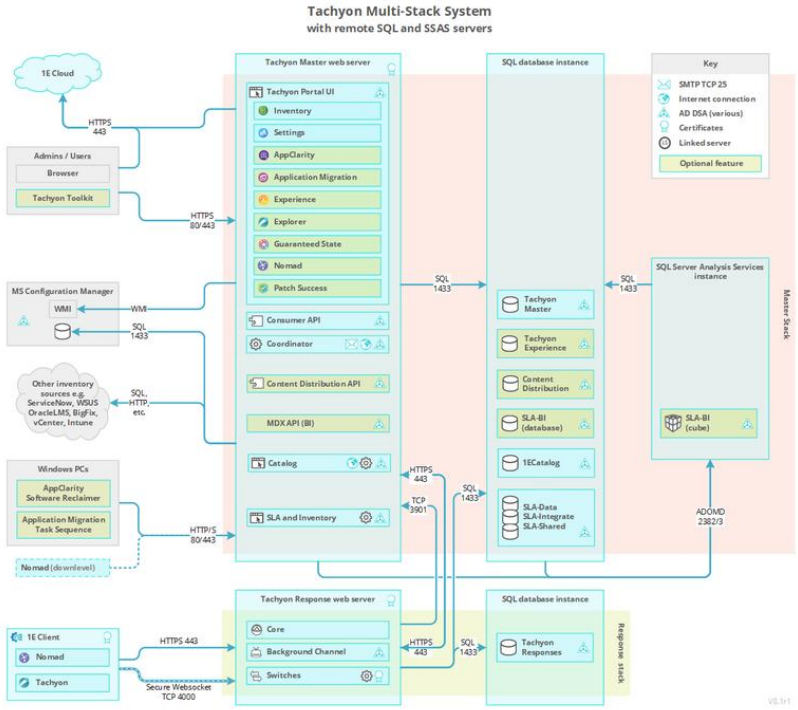
Device	Port	Protocol	Direction	Usage	Configurable
	443			**Background Channel**.	BackgroundChannelUrl=https:/<1Eplatform FQDN>:<port>/Background
Clients	TCP 7766	HTTPS	Outgoing and Incoming	• Communication between the 1E Client service and 1E Client UI.	Yes, during installation. See Tachyon client settings. MODELE.INTERACTION.PORT=<port>
Browsers	TCP 443	HTTPS	Outgoing	• Browsers connection to the **Tachyon Portal** (Explorer, Settings, and other applications). • Browser connection to the **SLA Platform UI**. • Browser connection to the **Consumer API**.	Anything other than port 443 requires the port number to be included in the browser URL when connecting to the Tachyon portal, API or SLA Platform UI.
Browsers	TCP 80	HTTP	Outgoing	• Console browser connections to the **1E Catalog UI**	Anything other than port 80 requires the port number to be included in the browser URL when connecting to the 1E Catalog UI.

1.11.2.3 Firewall requirements for a remote Catalog Web Server

The following table lists firewall requirements when the Catalog Web Server is on a different server than the Tachyon Server. This can happen if Tachyon Server is installed in an environment that already has a 1E Catalog server installed to support **Application Migration** or **AppClarity**.

Device	Port	Protocol	Direction	Usage	Configurable
Catalog Server	TCP 80	HTTP	Incoming	• Console browser connections to the **1E Catalog UI** • Consumer connections to the **Catalog API**	Yes, during installation. See 1E Catalog installer properties.
Catalog Server	TCP 443	HTTPS	Outgoing	• **1E Catalog Update service** contacting the **1E Cloud Catalog Service** via Internet connection.	The port used to connect to the **1E Cloud Services** is not configurable.
Catalog Server	TCP 1433	TDS	Outgoing	• Catalog services and application pool communicating with SQL Server. • **1E Catalog Update service** communicating with SQL Server.	Yes, during installation. See 1E Catalog installer properties.
SQL Server (1E Catalog database)	TCP 1433	TDS	Incoming	• **1E Catalog application pool** communicating with SQL Server. • **1E Catalog Update service** communicating with SQL Server.	Yes, during configuration of the SQL Server instance.
Browsers	TCP 80	HTTP	Outgoing	• Console browser connections to the **1E Catalog UI**	Yes, during installation. See 1E Catalog installer properties.

1.11.2.4 Firewall requirements for a remote Tachyon Response Stack



The following table lists firewall requirements when using a **Tachyon Response Stack** that is remote from the **Tachyon Master Stack**, which is additional to the ports required for a Single-Server. Each Tachyon component described in the table has at least one output and/or input. For each Tachyon component with an output, there is a matching input.

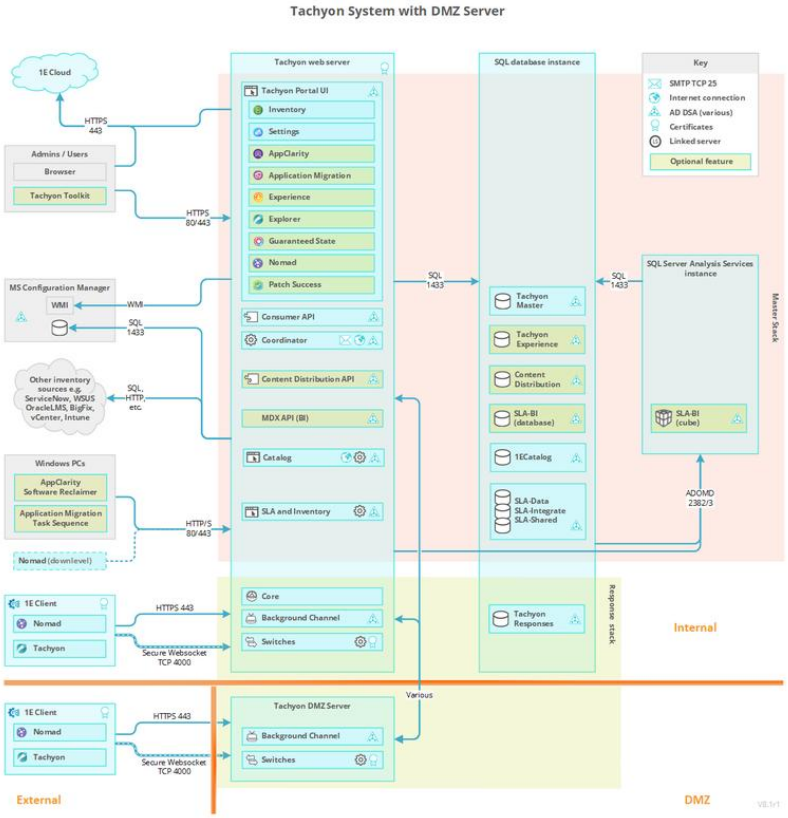
Device	Port	Protocol	Direction	Usage	Configurable
Tachyon Server (Response Stack)	TCP 443	HTTPS	Incoming	• Tachyon Coordinator **Workflow service** on the remote Master Stack connecting to the Core on a remote Response Stack • **Consumer API** on the remote Master Stack connecting to the remote **Background Chan**	Yes, during the installation of the Response Stack. In the **Website Configuration** panel in Tachyon Setup. See Server installer property HTTPSIISPORT refer to Tachyon Server installer properties. The Consumer API connection to the

Device	Port	Protocol	Direction	Usage	Configurable
				nel on a remote Response Stack • **Consumer API** on the remote Master Stack connecting to the **Core** on a remote Response Stack	Core is only used for remote Response Stacks.
Tachyon Server (Master Stack)	TCP 3901	WebSocket (ws)	Incoming	• Tachyon Switches sending **instrumentation data** to the Instrumentation module in the Coordinator on the Master Stack • Tachyon Web Site **Core** application pool sending **instrumentation data** to the Instrumentation module in the Coordinator on the Master Stack	Yes, but please contact 1E for advice.
Tachyon Server (Response Stack)	TCP 3901	WebSocket (ws)	Outgoing	• Tachyon Switches sending **instrumentation data** to the Instrumentation module in the Coordinator on the Master Stack • Tachyon Web Site Core application pool sending **instrumentation data** to the	Yes, but please contact 1E for advice.

Device	Port	Protocol	Direction	Usage	Configurable
				Instrumentation module in the Coordinator on the Master Stack	
SQL Server (TachyonMaster database)	TCP 1433	TDS	Incoming	• Tachyon Web Site **Core** application pool on a remote Response Stack communicating directly with the Tachyon Master database	Not configurable from Setup. In the **Database Servers** panel in Tachyon Setup you can select a SQL Server instance. The instance can be installed using a non-standard port. However, selecting an instance that uses a non-standard port will not change the port used by the Tachyon Installer, and installation will fail. If you require the use of a non-standard port on a Default SQL Server instance, contact 1E for guidance on a manual workaround. If using a Named Instance that is set to its default configuration where the server automatically chooses a random port (or if you

Device	Port	Protocol	Direction	Usage	Configurable
					manually configured the instance to use a fixed port), then the **SQL Browser** service needs to be enabled to let the Tachyon Server determine the port in use. You will need to open UDP port 1434 used by the SQL Browser. See Server installer property, SQLSERVER_MASTER, refer to Tachyon Server installer properties.
Tachyon Server (Response Stack)	TCP 1433	TDS	Outgoing	• Tachyon Web Site **Core** application pool communicating directly with the remote Tachyon Master database	Not configurable from Setup. See the comments above for SQL Server (TachyonMaster database). See Server installer property SQLSERVER_MASTER, refer to Tachyon Server installer properties.

1.11.2.5 Firewall requirements for a Tachyon DMZ Server



The following table lists the subset of ports needed when hosting Tachyon Switch and Background Channel components on a DMZ Server to support devices external to the network. Each Tachyon component described in the table has at least one output and/or input. For each Tachyon component with an output there is a matching input.

Note

If the server is a domain joined server it needs to be able to access Microsoft services, including Certificate Services and Active Directory. If the server is not domain joined (a workgroup server) you will need to manually install its Web Server certificate.

In both cases you will also need to ensure that the server is able to validate the certificate, including accessing the certificate's remote CRL Distribution Point.

The following table does not cover port requirements when using ADFS and SAML tokens to authenticate clients. In this documentation we just provide details of the simplest option, which uses certificates for client authentication. For details of how to configure Tachyon to support the more complex implementations, please contact 1E.

Device	Port	Protocol	Direction	Usage	Configurable
DMZ Server	TCP 443	HTTPS	Outgoing	• The **Switch** forwards compressed responses from the Internet-facing client devices to the **Core** on the Response Stack	Yes, during installation. In the **Website Configuration** panel in Tachyon Setup. See Server installer property HTTPSIISPORT, refer to Tachyon Server installer properties.
DMZ Server	TCP 3901	WebSocket (ws)	Outgoing	• Tachyon Switches sending **instrumentation data** to the **Instrumentation** module in the Coordinator on the Master Stack	Yes, but please contact 1E for advice.
DMZ Server	TCP 400n	TCP	Incoming	• Each Switch (from 1 to n) listens for prompts (pokes) from the **Core** on the Response Stack forwarding **workflow commands**. Each **Switch** requires its own port to be registered in the **Core**.	If the value for the Switch port has been changed, the port you need to open should be the Switch client port + 1. For example, if a Switch client port is 4000 then Switch poke port is 4001.
DMZ Server	TCP 4000	WebSocket Secure (wss)	Incoming	• Internet-facing client requesting instructions from and sending compressed responses to the Tachyon **Switch**	Switch client ports are not configurable using the Server installer. A Switch client port can be changed post-installation, by configuring the value

Device	Port	Protocol	Direction	Usage	Configurable
					in the **Port** column for the relevant Switch in the **SwitchConfiguration** table in the Tachyon Master database. Clients initiate and maintain a WebSocket Secure connection to a Switch, which the Switch uses to communicate back to the client.
DMZ Server	TCP 80	HTTP	Outgoing	• See note above about accessing the certificate's remote CRL Distribution Point.	
Tachyon Server (Response Stack)	TCP 443	HTTPS	Incoming	• The **Core** receives compressed responses forwarded by the Switch	Yes, during installation. In the **Website Configuration** panel in Tachyon Setup. See Server installer property HTTPSIISPORT, refer to Tachyon Server installer properties.
Tachyon Server (Master Stack)	TCP 443	HTTPS	Outgoing	• The **Consumer API** on the Master Stack sends content to the **Background Channel**	Yes, during installation. In the **Website Configuration** panel in Tachyon Setup. See Server installer property

Device	Port	Protocol	Direction	Usage	Configurable
					HTTPSIISPORT, refer to Tachyon Server installer properties.
Tachyon Server (Response Stack)	TCP	TCP	Outgoing	• The **Core** on the Response Stack prompts each **Switch** on the DMZ Server	Switch client ports are not configurable using the Server installer. A Switch client port can be changed post-installation, by configuring the value in the **Port** column for the relevant Switch in the **SwitchConfiguration** table in the Tachyon Master database. If the value for the Switch client port has been changed the port you need to open should be the Switch client port + 1. For example, if Switch client port is 4000 then Switch poke port is 4001.
Tachyon Server (Master Stack)	TCP 3901	WebSocket (ws)	Incoming	• Tachyon **Switches** sending **instrumentation data** to the **Instrumentation** module in the Coordinator on the Master Stack	Yes, but please contact 1E for advice.

Device	Port	Protocol	Direction	Usage	Configurable
Internet-facing clients	TCP 443	HTTPS	Outgoing	• Internet-facing client retrieves content from the **Background Channel**	Yes, during installation. See Tachyon client settings.
Internet-facing clients	TCP 4000	WebSocket Secure (wss)	Outgoing	• Internet-facing client requests instructions from and sends compressed responses to the Tachyon **Switch**	Yes. See Tachyon client settings. There must be a matching Switch using the same port. Clients initiate and maintain a WebSocket Secure connection to a Switch, which the Switch uses to communicate back to the client.

1.11.2.6 Internal Server communications

The following is a list of ports used within the Tachyon Platform, and not listed in the Single-Server table above, and as such should not affect firewall requirements. Some of these are listed in the DMZ table above.

Port	Protocol	Usage	Configurable
TCP 3900	WebSocket (ws)	• Tachyon Switch registering with the Switch Host	Yes, post-installation, but not recommended. Contact 1E for advice. The following may be configured during installation. TCP 443 HTTPSIISPORT (Website configuration) TCP 80 IISPORT (Website configuration)

Port	Protocol	Usage	Configurable
			TCP 8081 WORKFLOWWEBPORT (Tachyon) TCP 6002 INTEGRATE_REST_PORT (SLA)
TCP 3901	WebSocket (ws)	• Tachyon Web Site **Consumer API** application pool requesting **instrumentation data** • Tachyon Web Site **Core** application pool sending **instrumentation data** • Tachyon Web Site **Core Internal** application pool sending **instrumentation data** • Tachyon Coordinator **Workflow** service sending **instrumentation data** • Tachyon **Switch** sending **instrumentation data**	
TCP	TCP	• A prompt (poke) from the **Core** forwarding **workflow commands** to each **Switch** (from 1 to n). Each **Switch** requires its own port to be registered in the **Core**.	
TCP 443	HTTPS	• Tachyon **Switch** retrieving **instruction definitions** from the Core • Tachyon Coordinator **Workflow service** connections to the Core • **Consumer API** connections to the **Background Channel**	

Port	Protocol	Usage	Configurable
		• **Consumer API** connections to the Tachyon Coordinator **Workflow service**	
TCP 80	HTTP	• Tachyon **Switch** forwarding responses to the Core Internal (fast) - but a Switch on a DMZ server will use 443 HTTPS instead.	
TCP 8081	HTTPS	• Tachyon Web Site **Consumer API** application pool issuing **workflow commands** to the Tachyon Coordinator **Workflow service**	
TCP 6002	HTTP	• **SLA Integrate Agent** service connecting to the **SLA Integrate Manager** Web API to get connector jobs.	

1.11.3 1E Companion Products

A list of the feature dependencies between Tachyon and other 1E companion products.

This page describes the dependencies to and from Tachyon in regard to certain features that are implemented across companion 1E products. To view the general platform-related dependencies for Tachyon please refer to Supported Platforms.

1.11.3.1 1E companion products that Tachyon platform 8.1 depends on

Supported versions of 1E companion products that Tachyon platform 8.1 features depend on.

Products and features that Tachyon Platform depends on	Supported versions of companion products	
1E Client	Tachyon requires the 1E Client to be installed on all client computers. This replaces the legacy Agent. Client features:	• 1E Client • 1E Client 8.0

Products and features that Tachyon Platform depends on	Supported versions of companion products	
	• Real-time response to instructions, which supports the retrieval of information using questions, and running actions • Tags (freeform and device/coverage) • Criticality and Location • 1E Client UI to support the Real-Time Control Center, Announcements, Surveys, and Sentiment features of the Experience application # • Inventory, including process usage, to support, the: – Tachyon Activity Record feature – Inventory and other consumer applications. • Performance metrics features to support the Experience application # • Policy feature to support consumer applications: Guaranteed State ##, Experience #, and Nomad # Modules to support: • The Patch Success application # • Command and script execution • Nomad • Device criticality • Manipulation of files and processes • Manipulation of the registry and WMI # • Security #	• 1E Client 5.2 • 1E Client 5.1

Products and features that Tachyon Platform depends on	Supported versions of companion products	
	• Software uninstallation • User sessions, including Primary User. # not supported on non-Windows, ## partially supported on non-Windows Tachyon clients can optionally use the Nomad client module of 1E Client to more efficiently download content.	
Nomad	Clients can optionally use Nomad (1E Client with Nomad client features enabled) to provide more efficient downloading of content.	• 1E Client • 1E Client 8.0 • 1E Client 5.2 • 1E Client 5.1

1.11.3.2 1E companion products that depend on Tachyon platform 8.1

Supported versions of 1E companion products with features that depend on Tachyon platform 8.1.

(For products that depend on the 1E Client, please refer to urn:resource:component:647597).

Products and features that depend on Tachyon platform	Supported versions of companion products	
AppClarity	AppClarity is a consumer application of the platform and requires a full Tachyon infrastructure.	• AppClarity 8.1

Products and features that depend on Tachyon platform	Supported versions of companion products	
Application Migration	Application Migration is a consumer application of the platform and requires a full Tachyon infrastructure.	• Application Migration 8.1
Guaranteed State	Guaranteed State is a consumer application of the platform and requires a full Tachyon infrastructure.	• Guaranteed State 8.1
NightWatchman	Console live status of NightWatchman clients is an optional feature of NightWatchman and requires a full Tachyon infrastructure. NightWatchman is not a platform application and requires its own server(s).	• NightWatchman Enterprise 7.3
Nomad	Nomad is a consumer application of the platform and requires a full Tachyon infrastructure. It includes the Content Distribution feature that replaces the legacy ActiveEfficiency Server and the Nomad features provided.	• Nomad 8.1 (app) and associated (tools)
Patch Success	Patch Success is a consumer application of the platform and requires a full Tachyon infrastructure. It also requires 1E SLA Platform Business Intelligence to be installed and a SQL Server Analysis Server (SSAS) instance.	• Patch Success 8.1
Shopping	Shopping uses the platform and 1E Client for its client-side order notifications, and to allow end-users to shop for instructions. Shopping is not a platform application and requires its own server(s).	• Shopping 6.1
Experience	Experience is a consumer application of the platform and requires a full Tachyon infrastructure.	• Experience 8.1

Products and features that depend on Tachyon platform	Supported versions of companion products
Explorer	Explorer is a consumer application of the platform and requires a full Tachyon infrastructure.	• Explorer 8.1

Note

In addition to the consumer applications listed above, Tachyon Setup is also used to install the Inventory and Settings applications.

1.11.3.3 Cross-reference of Platform Application and Client versions

Each row in this table shows the 1E products versions that were released together, or intended to work with each other. It is not a complete listing of all supported 1E products.

1.11.3.4 Tachyon platform

Tachyon	Explorer	Patch Success	Guaranteed State	Experience	AppClarity	Application Migration	Active Efficiency	Nomad
8.1	8.1	8.1	8.1	8.1	8.1	8.1	replaced by CD	8.1
8.0	8.0	8.0	8.0	8.0	8.0	8.0	replaced by CD	8.0
5.2	5.2	1.3	1.5	1.3	7.1.105	3.1.105	replaced by CD	1.0
5.1	5.1	1.2.104	1.4	1.2	7.1	3.1	1.10	n/a
5.0	5.0	1.2	1.2	1.0	7.0	3.0	1.10	n/a

1.11.3.5 Other Platforms

Nomad Tools	PXE Everywhere	NightWatchman	Shopping
8.1	**8.1**	**7.3**	**6.1**

Nomad Tools	PXE Everywhere	NightWatchman	Shopping
8.0	**8.0**	**7.3**	**6.1**
7.1	**4.0.100**	**7.3**	**6.0**
7.0.200	**4.0**	**7.3**	**6.0**
7.0.100	**3.2**	**7.2.500**	**5.6**
7.0	**3.2**	**7.2.500**	**5.6**

1.11.3.6 Clients and Client Deployment Assistant Wizard

CDA	1E Client	Tachyon platform client	Nomad	PXE	WakeUp	Shopping
8.1	**8.1**	8.1	8.1	8.1	7.3*	6.1*
8.0	**8.0**	8.0	8.0	8.0	7.3*	6.1
1.6	**5.2**	5.2	7.1	4.0	7.3*	6.0*
1.5	**5.1**	5.1	7.0.200	4.0	7.3*	6.0
1.4.200	**5.0**	5.0	7.0.100	n/a	7.3	5.6
1.4	**4.1**	4.1	7.0	n/a	7.2.500*	5.5.200

* 1E Client includes hotfixes

1.11.4 Device View

The **Device View** is a shared page accessible from many applications.

The **Overview** and **1E Client** tabs are always present in the **Device View**. Other tabs are visible if an app has been installed and is licensed.

Each tab has one or more panels with tiles populated with data from various sources, some by instructions that are run instantly, with results cached for 3 minutes. An appropriate error message is displayed instead of a tile in the following circumstances:

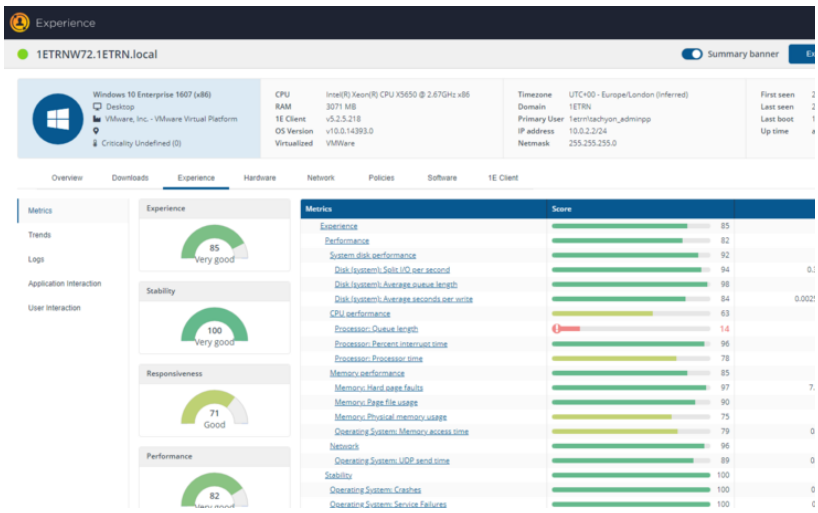
- If the device is offline, as indicated by the color of the icon in the top left
- The user does not have at least Viewer permission to view use the license the tab or panel
- The user does not have questioner permission to run the instruction

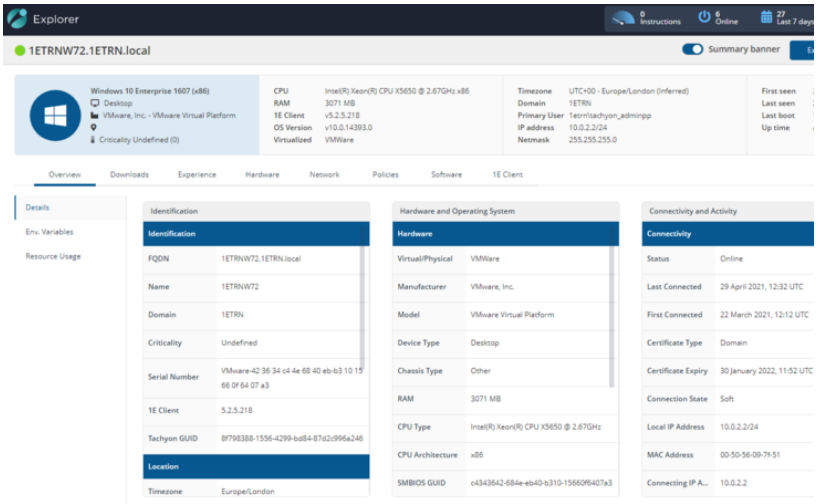
- An instruction has not been uploaded.

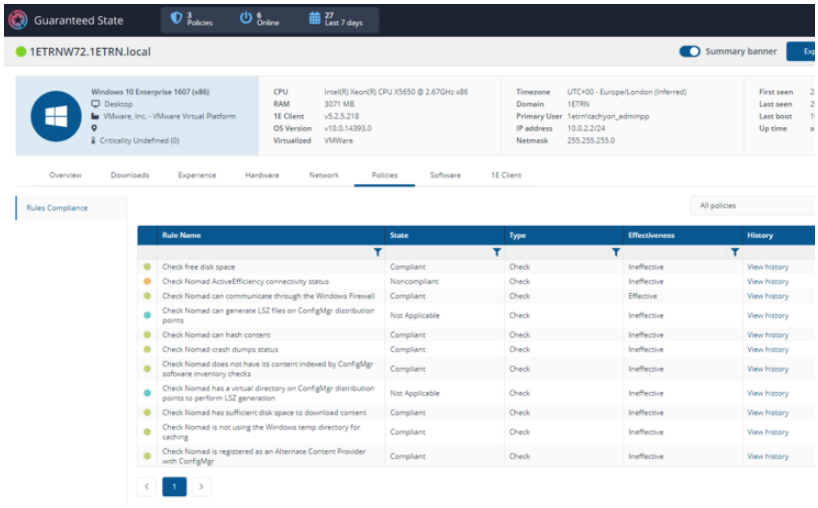
The Device View tabs and panels page lists the names of tabs and their panels, and a description of each tile indicating how the tile is populated.

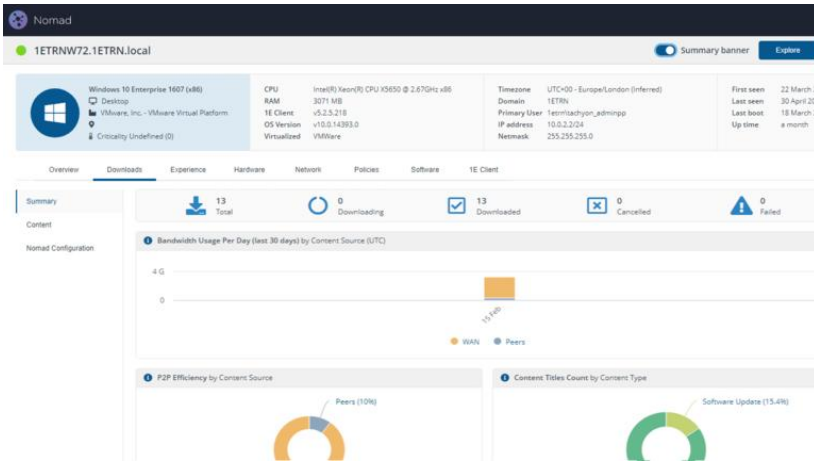
1.11.4.1 The Device view in other Tachyon platform applications

The **Device View** is a common view used in multiple apps to present device details. The aim of the Device view is to provide a combined overview of all the information known about a device along with the ability to retrieve information about the device in real-time. Each application displays a different default tab (see below), other tabs are visible if an application has been installed and licensed, and the user has permission to use the application.

Tachyon application	Device page	Device page default tab	Device view
Introducing Tachyon Experience	Devices page	Clicking on one of the links in the **FQDN** column of the Experience Devices page displays the Device view for the selected device. When displaying the Device view from a Experience page the view defaults to the **Experience** tab. The **Experience** tab contains information	

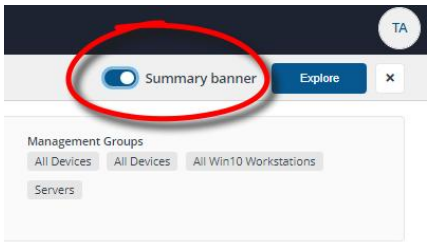
Tachyon application	Device page	Device page default tab	Device view
		derived from and useful for Experience.	
Introducing Tachyon Explorer	The Devices Table	Clicking on the information icon next to the device name in the **Device Name** column of the **Devices Table** page displays the Device view for the selected device. When displaying the Device view from the Explorer Devices Table page, the view defaults to the **Overview** tab.	

Tachyon application	Device page	Device page default tab	Device view
Introducing Guaranteed State	Devices page	Clicking on one of the links in the **Device Name** column of the Explorer **Devices** page displays the Device view for the selected device. When displaying the Device view from a Explorer page the view defaults to the Policies tab. The **Policies** tab contains information derived from and useful for using Explorer.	

Tachyon application	Device page	Device page default tab	Device view
Introducing Nomad	Devices page	Clicking on one of the links in the **FQDN** column of the Nomad **Devices** page displays the Device view for the selected device. The default view in the Nomad devices view is **Downloads**.	

1.11.4.2 Summary banner

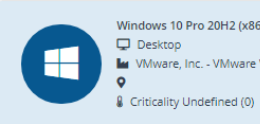
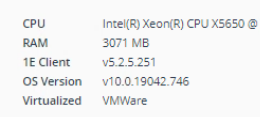
The Summary banner displays a quick summary of the information provided in the various tabs displayed in the Device View. It can be viewed by toggling the **Summary banner** switch to on.



The following picture shows the Summary banner displayed for a particular device.

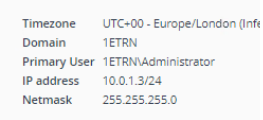
1.11.4.2.1 Summary banner panels

The following table describes the information provided in the Summary banner.

<table>
<tr><th>Panel</th><th>Description</th><th>Data source</th></tr>
<tr><td> 
</td><td>Shows details equivalent to the following tiles:
<table>
<tr><th>Tab</th><th>Panel</th><th>Column</th><th>Tile</th><th>Description</th><th>Example</th></tr>
<tr><td>Overview</td><td>Details</td><td>Hardware and Operating System</td><td>Operating System</td><td>Version</td><td>Windows 10 Pro 20H2 (x86)</td></tr>
<tr><td>Hardware and Operating System</td><td>Hardware</td><td>Device Type</td><td>Desktop</td><td></td><td></td></tr>
<tr><td>Hardware and Operating System</td><td>Hardware</td><td>Manufacturer</td><td>VMware, Inc</td><td></td><td></td></tr>
<tr><td>Hardware and Operating System</td><td>Hardware</td><td>Model</td><td>VMWare Virtual Platform</td><td></td><td></td></tr>
<tr><td>Identification</td><td>Location</td><td>Location</td><td></td><td></td><td></td></tr>
<tr><td>Identification</td><td>Identification</td><td>Criticality</td><td>Undefined (0)</td><td></td><td></td></tr>
</table></td><td>Data from Tachyon Master (the latest online status message)</td></tr>
<tr><td> 
</td><td>Shows details equivalent to the following tiles:</td><td></td></tr>
</table>

Panel	Description	Data source

Tab	Panel	Column	Tile	Description	Example
Overview	Details	Hardware and Operating System	Hardware	CPU Type	Intel(R) Xeon(R) CPU X5650 @2.67 GHz x86
Hardware and Operating System	Hardware	RAM	3071 MB		
Identification	Identification	1E Client	v5.2.5.251		
Hardware and Operating System	Operating System	Version	v10.0.19042.746		
Hardware and Operating System	Operating System	Virtual/Physical	VMWare		



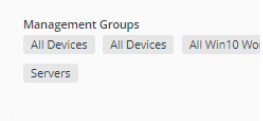
Shows details equivalent to the following tiles:

Tab	Panel	Column	Tile	Description	Example
Overview	Details	Identification	Location	Timezone	UTC+00 - Europe/London

Panel	Description					Data source
					(Inferred)	
	Identification	Identification	Domain	1ETRN		
	Connectivity and Activity	Activity	User	1ETRN\Administrator		
	Connectivity and Activity	Connectivity	Local IP Address	10.0.1.3/24		
					Netmask	255.255.255.0

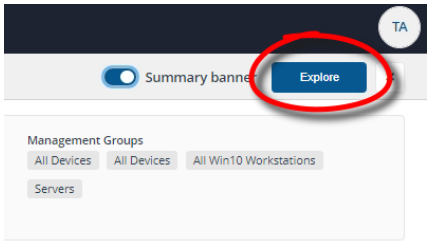
Shows details equivalent to the following tiles:

Tab	Panel	Column	Tile	Description	Example
Overview	Details	Connectivity and Activity	Connectivity	First Connected	22 March 2021, 12:17 UTC
Connectivity and Activity	Connectivity	Last Connected	27 April 2021, 09:23 UTC		
Connectivity and Activity	Activity	Last Boot	18 March 2021, 12:24 UTC		

Panel	Description	Data source
	Up time a month	
	Shows details equivalent to the following tiles: Tab: Overview; Panel: Details; Column: Identification; Tile: Grouping; Description: Mgmt. Groups; Example: • All Devices • All Win10 Workstations • Servers.	

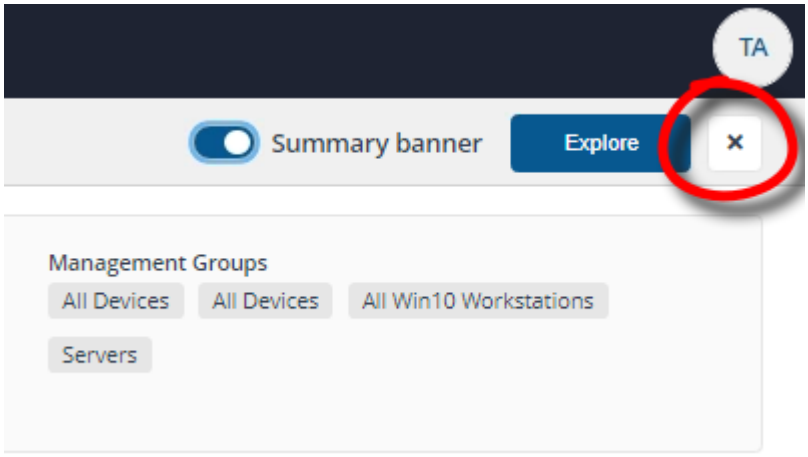
1.11.4.3 Exploring a device from the Device View

You can click on the **Explore** button in the Device View to launch Explorer with the current device set as the scope.



1.11.4.4 Closing the Device View

The Device View is a popup that is displayed when clicking on the name of a device on a page where devices are displayed. To return to the page you came from you need to click the x button.



1.11.4.5 The Device View tabs and panels

Tab	Panel	Description	Data source
Overview	**Details**	Displays a number of tiles sorted into **Identification**, **Hardware and Operating System** and **Connectivity and Activity** columns that show information for the selected device retrieved from the online status information stored in the TachyonMaster database. The columns and tiles are shown in the following table: Column / Tile / Description **Identification** / Identification / Displays the current device: • FQDN	Data from Tachyon Master (the latest online status message)

Tab	Panel	Description	Data source
		• Name • Domain • Criticality • SerialNumber • 1EClient • TachyonGU	

Tab	Panel	Description		Data source
			ID.	
		Location	Displays the device's: • Timezone • Offset • Location • Locale.	

Tab	Panel	Description		Data source
		Grouping	Displays the device: • Tags - free form tags applied to the device • Cove	

Tab	Panel	Description	Data source
		rageTags - any coverage tags applied to the device	

Tab	Panel	Description	Data source
		• Mgmt.Groups-lists the management groups the dev	

Tab	Panel	Description			Data source
				i c e i s a m e m b e r o f .	
		Hardware and Operating System	Hardware	Shows hardware details for the device: • Virtual/Phyiscal • Manufacturer	

Tab	Panel	Description	Data source
		• Model • DeviceType • ChassisType • RAM • CPUType • CPUArchi	

Tab	Panel	Description			Data source
				tecture • SMBIOSGUID.	
		Operating System	Shows operating system, type and version for example: • Type • Version • Ver		

Tab	Panel	Description		Data source
		sionNumber • Architecture • Installation.		
		Connectivity and	Connectivity	Shows current device connecti

Tab	Panel	Description	Data source
		Activity	vity status: • Status • LastConnected • FirstConnected • CertificateType

Tab	Panel	Description	Data source
		• Certificate Expiry • Connection State • Local IP Address • MAC Addr	

Tab	Panel	Description			Data source
				es s • Connecting IP.	
			Activity	Shows Last Boot date and time and current user.	
	Env. Variables	Shows a list of the environment variables set on the device.			
	Resource Usage	Two panels: • **Resource Usage over the last hour** - shows system disk, CPU and memory usage per minute for the last one hour • **Resource Usage at** *day/month/year time* - shows executable resource usage for a specific minute:			1E-TachyonPlatform-Hardware-ResourceUsage 1E-TachyonPlatform-Hardware-ResourceUsageByMinute

Tab	Panel	Description	Data source

Column	Description
Product	Resource name, for example 1E Client
Executable	Resource executable, for example 1e.client.exe
Instance Count	Number of currently running instances.
Cpu Percent	Percentage of CPU currently being consumed.
Memory Virtual Mb	Virtual memory consumed in Mb.
Memory Physical Mb	Physical memory consumed in Mb.
Io Read Kb Per Second	Number of associated read input/output operations per second.
Io Write Kb Per Second	Number of associated write input/output operations per second.
Handle Count	The number of object handles.

Downloads	**Summary**	Download activity and status for the device. Whenever you click on an FQDN on any of the Nomad pages then the **Device View** will be displayed with the **Downloads** tab selected.	Data from Nomad.

Tab	Panel	Description	Data source
Content	Content Titles on the selected device, the default view is from **All Sources**, **All Types** and **All Status**. **Note** You may see a difference in the number of items in a device's Nomad cache versus that displayed in the Nomad app Device View. This is because if downloaded content has been deleted from Configuration Manager, the content titles cannot be resolved in the Nomad app and are not displayed. This is under consideration for re-design and may be revised in future versions of Nomad.	Data from Nomad.	
Nomad Configuration	**1E Nomad Branch Settings .**	1E-Nomad-NomadBranchSettings	
Experience	**Metrics**	Metrics are the data points that are collected by the 1E Client and sent to the Tachyon server. They are collected at different intervals depending on the type of data that is being collected.	Data from Experience metrics
Trends	The Trends tab shows the changes in the scores over time. Hovering over any of the bars shows the details for that time and event. If the user viewing the device details also has the ability to at least ask a question in Explorer the Explore button will be visible.	Data from Experience metrics	
Logs	The Event Logs tab gives you a listing of the Windows Event log entries for that device.	Data from Experience metrics	

<table>
<tr><th>Tab</th><th>Panel</th><th>Description</th><th>Data source</th></tr>
<tr><td></td><td>This brings that data to this view and is very useful when determining the root cause of an issue that has been reported on the device.</td><td></td><td></td></tr>
<tr><td>Application Interactions</td><td>Shows user interaction times and ratios across applications measured over the last 30 days</td><td>1E-Experience-ApplicationInteraction</td><td></td></tr>
<tr><td>User interactions</td><td>Shows user interactive sessions with activity over last 30 days.</td><td>1E-Experience-UserInteractionHistory</td><td></td></tr>
<tr><td>Hardware</td><td>Disk drives</td><td>Shows disk drives, including hardware and usage information.

Column — Description

Drive — Drive letter.

Volume Name — Volume name, if set.

Drive Type — Drive type, for example:
• Removable Disk
• Local Disk
• Compact Disk.</td><td>1E-TachyonPlatform-Hardware-DiskDrives</td></tr>
</table>

Tab	Panel	Description		Data source
		Size Gb	Total disk size in Gb.	
		Free Space Gb	Current free space in Gb.	
		Usage Percent	Percentage used of total drive space.	
		File System	File system, for example NTFS.	
		Manufacturer	Standard or SSD drive.	
		Model	Drive manufacturer.	
		Serial Number	Unique disk serial number.	
		Partition	Drive and partition of the specific drive.	
		Firmware Revision	Drive firmware version.	
		Device ID	Device ID of the specified disk.	
Peripherals	Shows the list of plug and play hardware devices (Windows only).			1E-TachyonPlatform-Hardware-Devices

Tab	Panel	Description	Data source

Column	Description
Device Type	Hardware device, including for example things like: • Battery • Monitor • Keyboard • Mouse • Ports • SoftwareDevice.
Name	Device name.
Instance Count	Number of instances of a peripheral device.
Service	Associated Windows service, for example atapi, serial, PCI, ACPI.

Network	**Throughput**	Shows network throughput on all adapters for the last hour, represented by the following tiles: • **Average throughput** - including Timestamp, Bytes Received per Second, Bytes Sent Per Second • **Bytes received per second** • **Bytes sent per second**.	1E-TachyonPlatform-Network-AverageThroughput

<table>
<tr><th>Tab</th><th>Panel</th><th>Description</th><th>Data source</th></tr>
<tr><td>Interface configuration</td><td>Returns the output from the native network interface configuration command (e.g. ipconfig or ifconfig).</td><td>1E-TachyonPlatform-Network-InterfaceConfiguration</td><td></td></tr>
<tr><td>DNS</td><td>Shows the Cache and Host file tiles:
DNS Cache Contents - with the entries from local DNS cache, Host Name and Address.
HOSTS file - shows the content of the drivers/etc/hosts file.</td><td>1E-TachyonPlatform-Network-DnsCache
1E-TachyonPlatform-Network-HostFileContent</td><td></td></tr>
<tr><td>TCP connections</td><td>Returns a list of established TCP connections.<table><tr><th>Column</th><th>Description</th></tr><tr><td>Process Name</td><td>Local process name.</td></tr><tr><td>Process Id</td><td>Uniquely identifies an active process.</td></tr><tr><td>Class</td><td>Class of Internet networking protocol.</td></tr><tr><td>Local Address</td><td>Local network address.</td></tr><tr><td>Local Port</td><td>Network port used by a specific process.</td></tr><tr><td>Remote Address</td><td>Source IP address from which the traffic came from.</td></tr><tr><td>Remote Port</td><td>Remote port used by a specific process.</td></tr></table></td><td>1E-TachyonPlatform-Network-TcpConnections</td><td></td></tr>
</table>

Tab	Panel	Description	Data source
	Latency Ms The time taken in milliseconds for data or a request to go from a source to a destination.		
Listening ports	Returns a list of processes which are listening for network connections. Column: Description **Process Name**: Local process name. **Process Id**: Uniquely identifies an active process. **Class**: Class of Internet networking protocol. **Local Address**: Local network address. **Local Port**: Network port used by a specific process. **Product**: Related product, for example host process for Windows Services, Local Security Authority Process, SCNotification.	1E-TachyonPlatform-Network-ListeningPorts	
ARP Cache	Returns a list of processes which are listening for network connections and also shows routing tables.	1E-TachyonPlatform-Network-ArpCache 1E-TachyonPlatform-Network-RoutingTable	
WIFI	Shows a list of visible wifi networks, including basic network properties.	1E-TachyonPlatform-Network-WiFiNetworks	

Tab	Panel	Description	Data source

Column	Description
SSID	WiFi network name.
Is Connected	Shows as either true or false, dependent on whether the corresponding adapter is connected to the network.
Is Hidden	Shows as true if the WiFi network is not broadcasting a public SSID.
Is Secure	Shows as either true or false: • true - if the WiFi network is secure • false - if the network is open.
Signal	Shows WiFi signal quality; from 0 (worst) to 100 (best).
Authentication	The default authentication mechanism supported by the network.
BSSI IDs	The Service Set Identifier (SSID) of the network, it will be empty if the network is hidden.
Encryption	Shows the default encryption mechanism

Tab	Panel	Description	Data source
		supported by the network.	
	Adapter	Shows the WiFi network adapter name to which this network is visible.	
Policies	**Rules Compliance**	Column: **Rule Name** — Name of rules applied to the current device. The viewable list relates to the selected Tachyon policy from the policy dropdown on the page. **State** — If the device state is Compliant, Noncompliant or Not Applicable. **Type** — Rule type: • Check - allows you to verify that a device has a particular state, such as a registry	Data from Guaranteed State

Tab	Panel	Description		Data source
			key having a specific value • Fix - allows you to define a desired state for the device and then enforce that state.	
		Effectiveness	Policy rule effectiveness is the usefulness of policy rules and is represented as either: • Disabled - the rule has not yet been enabled from the Guaranteed State Rule Administration page, so it is not	

Tab	Panel	Description	Data source
		currently active • Unassigned - the rule is enabled, but has not been deployed to any devices • Ineffective - the rule has been deployed, but no devices have changed their compliance position for this rule in the last thirty days • Effective - the rule has been deployed and at least	

Tab	Panel	Description	Data source
		one device has changed its compliance position for this rule in the last thirty days. **History** Rule history.	
Software	**Installations**	Shows (per-device) installed software. **Product** Software product name. **Publisher** Software publisher. **Version** Product version number. **Architecture** Instruction set architecture (ISA) version. **Install Date** Software installation date.	1E-TachyonPlatform-Software-Installations

<table>
<tr><th>Tab</th><th>Panel</th><th>Description</th><th>Data source</th></tr>
<tr><td>Windows services</td><td>Shows list of installed Windows services and their current state.

<table><tr><th>Column</th><th>Description</th></tr><tr><td>Name</td><td>Windows service name.</td></tr><tr><td>State</td><td>Windows service state, Running or Stopped.</td></tr><tr><td>Startup Type</td><td>Windows service startup type, for example Automatic, Automatic (Delayed Start), Manual, Disabled.</td></tr><tr><td>Process Id</td><td>Uniquely identifies an active process.</td></tr><tr><td>Description</td><td>Windows service description.</td></tr><tr><td>Logon Account</td><td>Windows service logon account context.</td></tr><tr><td>Type</td><td>Windows services type, for example file system driver, kernel driver, shared process.</td></tr></table></td><td>1E-TachyonPlatform-Software-Services</td><td></td></tr>
<tr><td>Env. Variables</td><td>Shows operating system environment variables.</td><td>1E-TachyonPlatform-Software-EnvironmentVariables</td><td></td></tr>
<tr><td>Processes</td><td>Shows detailed information about all running processes.</td><td>1E-TachyonPlatform-Software-Processes</td><td></td></tr>
</table>

Tab	Panel	Description	Data source

Column	Description
Product	Software product name.
Executable	Executable name.
Version	Product version number.
Devices count	How many devices are reporting.
Crashes	Number of times this software crashed during the last 24-hour reporting period.
Hangs	Number of times this software crashed during the last 24-hour reporting period. **Note** Software crash and hang information is obtained from Windows event data. For background information on Windows events and the event viewer refer to https://support.microsoft.com/en-gb/help/302542/how-to-diagnose-system-problems-with-event-viewer-in-microsoft-windows
Performanc	Number of performance anomalies detected in this

Tab	Panel	Description	Data source
	e anomalies	software during the last 24-hour reporting period.	
	I/O write KB/s	Average disk I/O read rate per second during the last 24-hour reporting period.	
	I/O write KB/s	Average disk I/O write rate per second during the last 24-hour reporting period. **Note** For background information on analyzing disk storage performance refer to https://docs.microsoft.com/en-gb/archive/blogs/cotw/analyzing-storage-performance	
	Virtual Memory Usage KB	Average Virtual Memory Usage KB during the last 24-hour reporting period. **Note** For an explanation of Windows Virtual Memory organization refer to https://answers.microsoft.com/en-us/windows/forum/windows_10-performance/physical-and-virtual-memory-in-windows-10/e36fb5bc-9ac8-49af-951c-e7d39b979938 and https://support.microsoft.com/en-	

Tab	Panel	Description	Data source
		us/help/2160852/ram-virtual-memory-pagefile-and-memory-management-in-windows	
	Processor Time Seconds	Each instance of the executable will burn processor time. This column gives the average of the total time consumed by each process instance per second. Each instance uses the sum of all time used by each core in parallel. Therefore, it is possible to see more seconds here than in a day (usually 60 x 60 x 24 = 86400) for the whole column, if your system is working extremely hard 24x7. The theoretical maximum would be somewhere near ***number of cores*** x ***seconds per day*** . Hence, 'Processor Time' rather than 'Human Time'	
	Processor Time %	This is an easier notion than Processor Time Seconds. This is the average of the processor consumption of each instance. Each instance of this process will have caused different percentages of compute resource in all the processors and cores to be used over time (unless they have specifically requested certain core affinity). For each minute each process is running, a profile of the usage is built for the whole day. This value is the average of all of those samples. There is no way to work	

Tab	Panel	Description	Data source
		out, for any one of the process instances involved, how long any particular instance was running for. This could indicate a process that is going wild with resources, but it would take more investigation on the device to discover for how long this is happening. It is perfectly possible to see all the values in this column adding up to more than 100% as the processes were not necessarily running at the same time. **Note** For further information on Processor time refer to https://social.technet.microsoft.com/wiki/contents/articles/12984.understanding-processor-processor-time-and-process-processor-time.aspx	
	Responsiveness Impact %	An indicator of how reactive a process is to activity by other processes on the device. Typically, anti-virus products watch and respond to potentially suspicious activity such as increased network traffic. Anti-virus products will differ in their impact on the overall performance of a device. **Note** Responsiveness Impact % is used to indicate how sensitive a process appears to be to the use of system resources by other	

Tab	Panel	Description	Data source
		processes on a device. For example, Security Protection software present on a device may reveal a spike in its activity whenever a new process is started on that device. This would typically be because the Security Protection software may wish to ensure that the new process starting on the device is present in a security white list. Other software may also react to activity by other processes and by reacting they impact system resource uses, thereby adversely affecting the user's experience. So it is useful to be able to identify software with the highest Responsiveness Impact on a device and potentially investigate further. **Note** Responsiveness Impact % represents the proportion of the increased CPU activity detected by the 1E Client as a result of performing a set of operating system-level operations that can be	

Tab	Panel		Description	Data source
		attributed to a given running process. Examples of these would be Windows registry and resource creation operations. It is reported as a percentage to normalize results across devices that offer a range of computing power. For example, if *software.exe* on a device is attributed a Responsiveness Impact of 53% this means that more than half of the spike in CPU usage caused by software monitoring activity on that device can be attributed to *software.*		
	Handle Count	Average number of Windows handles used by this software during the last 24-hour reporting period. **Note** For further information on Windows handles refer to https://docs.microsoft.com/en-us/windows/win32/sysinfo/handles-and-objects For tips on examining open handles for any Windows process refer to https://docs.microsoft.com		

Tab	Panel	Description	Data source
		/en-us/sysinternals/downloads/handle and https://techcommunity.microsoft.com/t5/windows-blog-archive/pushing-the-limits-of-windows-handles/ba-p/723848	
	Physical Memory Usage KB	Average Physical Memory Usage KB during the last 24-hour reporting period. **Note** Please refer to https://docs.microsoft.com/en-us/sysinternals/downloads/rammap for a useful tool to examine physical memory allocation on a device.	
1E Client	**Binaries**	Shows a list of the binary files in the executable folder of the 1E Client. Column: Description **File Name**: Associated 1E Client file name. **File Version**: Software version. **File Size**: File size in bytes. **Description**: File description	1E-TachyonPlatform-Client-Binaries

Tab	Panel	Description		Data source
		Date Created	The date the file was written to disk.	
		Date Modified	The date the file was last saved.	
Configuration file	Shows the full content of the 1E Client configuration file, including: • Logging settings • Communication settings • Agent settings • Module settings.			1E-TachyonPlatform-Client-ConfigFileContent
Extensibility	Shows extensibility objects (modules and providers) loaded by the 1E Client.			1E-TachyonPlatform-Client-Extensibility
	Column	Description		
	Type	Module or Provider component.		
	Binary Name	Associated 1E Client binary name, for example 1E.Client.Module.Interaction.dll		
	Name	Name, for example Interaction.		
	Version	1E Client version, for example 5.2.5.251		
Local Storage	Shows **Data Files** and **Client Inventory Database Use** tiles that display the list of:			1E-TachyonPlatform-Client-DataFiles 1E-TachyonPlatform-Client-InventoryDatabaseUse

Tab	Panel	Description	Data source
		• Data files (logs, databases, etc) created by the 1E Client • Tables in the1E Client Inventory database, along with a row count per table.	

1.11.4.6 Product Pack references

The Device View page requires the following feature-related Product Packs that contain instructions used by the page.

Product Pack name	Instruction name	Device View panel	Readable Payload
1E-Experience	**1E-Experience-LogonSessions**	n/a	Current user logon sessions
1E-Experience	**1E-Experience-UserInteractionHistory**	Experience\User Interaction	Get user interaction history over last 30 days
1E-Nomad	**1E-Nomad-NomadBranchSettings**	Downloads\Nomad Configuration	Nomad Branch service settings
1E-Tachyon-Platform	**1E-TachyonPlatform-Client-Binaries**	1E Client\Binaries	List deployed 1E Client binary files
1E-Tachyon-Platform	**1E-TachyonPlatform-Client-ConfigFileContent**	1E Client\Configuration File	Show 1E Client configuration file content
1E-Tachyon-Platform	**1E-TachyonPlatform-Client-DataFiles**	1E Client\Local Storage	List 1E Client data files
1E-Tachyon-Platform	**1E-TachyonPlatform-Client-Extensibility**	1E Client\Extensibility	Show 1E Client extensibility (modules and providers)

Product Pack name	Instruction name	Device View panel	Readable Payload
1E-Tachyon-Platform	**1E-TachyonPlatform-Client-InventoryDatabaseUse**	1E Client\Local Storage	List of inventory database tables
1E-Tachyon-Platform	**1E-TachyonPlatform-Hardware-Devices**	Hardware\Peripherals	List of hardware devices
1E-Tachyon-Platform	**1E-TachyonPlatform-Hardware-DiskDrives**	Hardware\Disk Drives	List disk drives
1E-Tachyon-Platform	**1E-TachyonPlatform-Hardware-ResourceUsage**	Overview\Resource Usage	Hardware resource usage over time
1E-Tachyon-Platform	**1E-TachyonPlatform-Hardware-ResourceUsageByMinute**	Overview\Resource Usage	Resource usage by executable for %minute%
1E-Tachyon-Platform	**1E-TachyonPlatform-Network-ArpCache**	Network\ARP and Routing	List entries in ARP cache
1E-Tachyon-Platform	**1E-TachyonPlatform-Network-AverageThroughput**	Network\Throughput	Network throughput for last 60 minutes
1E-Tachyon-Platform	**1E-TachyonPlatform-Network-DnsCache**	Network\DNS	DNS cache entries
1E-Tachyon-Platform	**1E-TachyonPlatform-Network-HostFileContent**	Network\DNS	Host file content (for DNS overrides)
1E-Tachyon-Platform	**1E-TachyonPlatform-Network-InterfaceConfiguration**	Network\Interface configuration	Network interface configuration
1E-Tachyon-Platform	**1E-TachyonPlatform-Network-ListeningPorts**	Network\Listening ports	Processes listening on TCP and UDP ports
1E-Tachyon-Platform	**1E-TachyonPlatform-Network-RoutingTable**	Network\ARP and Routing	Routing table information

Product Pack name	Instruction name	Device View panel	Readable Payload
1E-Tachyon-Platform	**1E-TachyonPlatform-Network-TcpConnections**	Network\TCP connections	Established TCP connections
1E-Tachyon-Platform	**1E-TachyonPlatform-Network-WiFiNetworks**	Network\WiFi	List visible WiFi networks
1E-Tachyon-Platform	**1E-TachyonPlatform-Software-EnvironmentVariables**	Software\Env. Vars	List environment variables
1E-Tachyon-Platform	**1E-TachyonPlatform-Software-Installations**	Software\Installations	List software installations
1E-Tachyon-Platform	**1E-TachyonPlatform-Software-Processes**	Software\Processes	List running process details
1E-Tachyon-Platform	**1E-TachyonPlatform-Software-Services**	Software\Windows Services	List Windows Services

1.11.5 Log files

Names and locations of log files created by Tachyon Server, 1E Client, and Tachyon tools.

1.11.5.1 Tachyon Setup logs

Setup creates a Setup log file for itself and an Install log for each of the components (if used) in the same folder as itself:

- *BIInstall.log*
- *CatalogInstall.log*
- *ContentDistribution.log*
- *SLAInstall.log*
- *Tachyon.Setup.log*
- *TachyonInstall.log*

1.11.5.2 Tachyon Server logs

The default location for all logs is the folder *%ALLUSERSPROFILE%\1E*

Subsystem	Component		
Tachyon Master	Tachyon portal UI and applications (Tachyon)	1E\Tachyon\	*Tachyon.Portal.log*
Consumer API	1E\Tachyon\	*Tachyon.ConsumerAPI.log*	
Coordinator service	1E\Tachyon\	*Tachyon.Coordinator.log* *Tachyon.Instrumentation.log*	
Experience web application	1E\Tachyon\	*Tachyon.Experience.log*	
1E Catalog	Catalog UI (CatalogWeb - Admin sync)	1E\Catalog\	*Catalog.Integration.UI.log*
Catalog API			
Catalog Update Service	1E\Catalog\	*Catalog.UpdateService.log*	
Nomad	Nomad web application	1E\ContentDistribution	*ContentDistribution.log*
SLA	SLA/Platform APIs (Admin, Core External)	1E\Tachyon\	*Tachyon.AdminAPI.log*
SLA Platform UI (Platform)	1E\SLA Platform\	*Web.log*	

Subsystem	Component		
SLA Engine	1E\SLA Platform\	*Engine.log*	
SLA Integrate Services (Connector Manager)	1E\SLA Platform\	*1E.SLAPlatformIntegrateAgent.log* *1E.SLAPlatformIntegrateManager.log* *1E.SLAConnector.<type>_sync.log*	
SLA Inventory	n/a	*n/a*	
SLA Operations Provider (not currently used)	1E\Platform Consumer\	*n/a*	
SLA databases (Data, Integrate, Shared)	n/a	*n/a*	
BI	MDX API	SQL database	*[SLA-BI].[BI].[Event Log]*
Tachyon Response	Core	1E\Tachyon\	*Tachyon.CoreAPI.log*
Background Channel (Background)	1E\Tachyon\	*Tachyon.BackgroundAPI.log*	
Switch(es) (also includes a single Switch Host service)	1E\Tachyon\	*Tachyon.Switch.4000.SW1.log* *Tachyon.Switch.Host.log*	

Please refer to Services and NTFS Security if changing the location of log files.

In this version of Tachyon Server, some installers do not support the LOGPATH property and the logs folder is not configurable during installation.

Each component has a configuration file in the Tachyon Server installation folder structure, which contains log configuration details. Defaults are:

- Filepath *%ALLUSERSPROFILE%\1E\<product>* where the product is Tachyon, SLA Platform, and 1E Catalog.
- Filename as shown in the table above.
- Maximum size 10MB (2MB for Switch logs).
- 2 rollover files numbered 1 to 2 with the rollover number included as n.log (5 rollover files for Switch logs).
- Date and timestamps are UTC to help troubleshooters synchronize logs on systems in different time zones.

Switch logs have the following names:

- The first Switch installed will typically have a log filename **Tachyon.Switch.4000.SW1.log** (where 4000 is the port it is listening on and SW1 is the **config name** in the SwitchConfiguration table in the TachyonMaster database).
- Other Switches on the same server will have different config names appended.
- The log filename will be unique on a server, but there may be the same named log on a different server.
- A Switch will continue to use the same log unless the SwitchConfiguration table is modified so that a different ID is used.
- If you see a Tachyon.Switch.log without a config name appended, this is a special case where a Switch cannot find its correct configuration and has fallen back to using the template * row which has ID=1. In which case you will need to troubleshoot how that happened.
- Rollover logs have numbers appended, for example, Tachyon.Switch_A.1.log, up to a default maximum of 5.

Tachyon server components use the **log4net RollingFileAppender** class. Details can be found in http://logging.apache.org/log4net.

1.11.5.2.1 Tachyon Server log files

For any issue, please provide a zip containing log files from the following locations:

- %ALLUSERSPROFILE%\1E\Catalog*.log
- %ALLUSERSPROFILE%\1E\ContentDistribution*.log
- %ALLUSERSPROFILE%\1E\Platform Consumers*.log
- %ALLUSERSPROFILE%\1E\SLA Platform*.log
- %ALLUSERSPROFILE%\1E\Tachyon*.log

If you are having licensing issues, please include:

- %ALLUSERSPROFILE%\1E\Licensing*

Please refer to the Log files page for more details.

1.11.5.2.2 Logging Levels

The table below describes the logging levels which are configurable for server components.

Value	Description
Error	Only outputs errors. An error is a serious problem, typically requiring operator intervention of some sort to restore full functionality.
Warn	Outputs errors and warnings. A warning indicates a potential problem, where the system can nonetheless function without intervention.
Info	Outputs general information in addition to errors and warnings. This is the default.
Debug	Outputs debugging information in addition to all the previous levels.

Warning

Logging levels should only be changed from **info** only if requested by 1E Support and reset to **info** after investigation is complete.

Tip

The method of configuring logging levels uses the above text values, where -log=0 is the default to mean the same as *-log=info*.

1.11.5.3 1E Client logs

1E Client logs on Windows

%ALLUSERSPROFILE%\1E\Client\1E.Client.log (used by 1E Client and Tachyon features, and Shopping client)

%ALLUSERSPROFILE%\1E\Client\NomadBranchUninstall-YYYY_MM_HHTMM_HH_SS_000Z.log

1E Client logs on macOS

/Library/Logs/1E.Client.Daemon.log (shows any service start errors)

/Library/Logs/1E.Client.log (shows the current operation of the 1E Client)

1E Client logs on other non-Windows platforms

/var/log/1E/Client/1E.Client.log

Nomad client log

%ALLUSERSPROFILE%\1E\NomadBranch\LogFiles\NomadBranch.log

PXE Everywhere Agent log

%ALLUSERSPROFILE%\1E\PXEEverywhere\PXEEverywhere.log

Shopping WSA client log

%ALLUSERSPROFILE%\1E\Client\WSA.log

WakeUp client log

%ALLUSERSPROFILE%\1E\Agent\WakeUpAgt.log

Note

By default, Windows resolves %ALLUSERSPROFILE% as C:\ProgramData\

1.11.5.4 Software Reclaimer logs

Every time the Reclaimer runs it will create a local log file of the process it is doing. The location and name of the log file depends on what task the reclaimer is doing.

Task	Logpath	Notes
Optout	**C:\Users\{USER}\AppData\Local\Temp\ AppClarity.SoftwareReclaimer.log**	Optout mode is normally run under user context so that the user can interact with the dialog. This means the log file will be in the users Temp folder within the

Task	Logpath	Notes
		user profile.
Mandatory	**C:\windows\Temp\AppClarity.SoftwareReclaimer.log**	Mandatory mode is normally set to run under system context, in order to process reclaim uninstall commands. Therefore, the log file will be under the system temp directory.
Reclaim	**C:\windows\Temp\AppClarity.SoftwareReclaimer.MSI.log**	For a mandatory reclaim, if a reclaim occurs using an MSI then an MSI log file is also created.

1.11.5.5 Configuration Manager Console Extensions log

%ALLUSERSPROFILE%\1E\Tachyon\Tachyon.CmConsole.log

%ALLUSERSPROFILE%\1E\Tachyon\Tachyon.RunInstructionUI.log

1.11.5.6 The Instruction Management Studio (TIMS) log

%ALLUSERSPROFILE%\1E\Tachyon\Tachyon.InstructionManagementStudio.log

1.11.5.7 Tachyon Product Pack Deployment Tool log

Tachyon.ProductPackDeploymentTool.log

In the same location as the tool.

1.11.6 Scripts

All scripts are referenced on other pages within the documentation.

1.11.6.1 Scripts for installation and upgrades

1.11.6.1.1 Install Windows Server roles and features

The following PowerShell script is used on Windows Server roles and features. Tachyon Setup can do all of this except for **Basic Authentication** (required by 1E Core) and **HTTP redirect** (required if Nomad is supporting down-level clients after replacing ActiveEfficiency).

```
Import-Module ServerManager

Get-WindowsFeature | Out-file $PSScriptRoot\ServerManager-1.txt -Append
Install-WindowsFeature Web-Server,
Web-Http-Redirect,
Web-Dyn-Compression,
Web-Basic-Auth,
Web-IP-Security,
Web-Windows-Auth,
Web-Asp-Net45,
Web-Mgmt-Console,
Net-Framework-45-Core,
Net-Framework-45-ASPNET

Uninstall-WindowsFeature Web-DAV-Publishing

Get-WindowsFeature | Out-file $PSScriptRoot\ServerManager-2.txt -Append
```

1.11.6.1.2 Changing the configuration of Network Adapters

The following extract is used here: Changing the configuration of Network Adapters.

If the configuration of any network adapters is changed, then the Tachyon website configuration for **IP Address and Domain Restrictions** may need to be updated with the server's new IPv4 and IPv6 addresses. Failure to update the configuration after a network change will cause issues between the Switch and the Core and prevent the Tachyon Server from functioning.

Use the PowerShell cmdlet **Gevt-NetIPAddress** to determine the current IP Addresses, and if necessary update the configuration of the Core web application.

The following **AddIpSec.ps1** script can be used to refresh local IP Addresses. It does *not* remove old, unwanted, or remote IP Addresses. Nor does it add addresses for remote Switches, which would need to be added manually.

```
# Adds local IPv4, v6 and loopback addresses to the IP Address and Domain Restr
ictions of the specified web applications. It does not delete any addresses
# Remote addresses must be manually configured.
# It only adds addresses if the specified web application exists.

Import-Module "WebAdministration"

Function AddIpSec() {
    param(
        [Parameter(Mandatory=$true)][string]$SiteName,
        [Parameter(Mandatory=$true)][string]$AppName
    )

    Write-Output "Adding IP restrictions to $AppName"

    $fullAppPath = "IIS:\Sites\" + $SiteName + "\" + $AppName

    if (Test-Path -Path $fullAppPath) {
        $appPath = $SiteName + "/" + $AppName
        $ipAddreses = Get-NetIPAddress | sort IpAddress | foreach { $_.IPAddres
s }
        Set-WebConfigurationProperty /system.webserver/security/ipsecurity -Nam
e allowUnlisted -Value "false" -Location $appPath -PSPath IIS:\
        foreach ($ipAddress in $ipAddreses)
        {
            $existingRestriction = Get-WebConfiguration system.webServer/Securi
ty/ipSecurity/add -Location $appPath -PSPath IIS:\ | where { $_.ipAddress -eq $
ipAddress }
            if (-not ($existingRestriction)) {
                Add-WebConfiguration system.webServer/security/ipSecurity -Loca
tion $appPath -Value @{ipAddress="$ipAddress";allowed="true"} -PSPath IIS:\
                Write-Output "Allowed restriction on IP $ipAddress added to $Ap
pName"
            }
            else {
                Write-Output "Restriction on IP $ipAddress already exists in $A
ppName. So skipping."
            }
        }
    }
    else {
        Write-Output "$AppName web application does not exist"
    }
}

$siteName = "Tachyon"
```

```
AddIpSec -SiteName $siteName -AppName "Core"
AddIpSec -SiteName $siteName -AppName "WelcomeCore"
```

1.11.6.1.3 Change Shopping 6.0 Sync from ActiveEfficiency to direct Configuration Manager

The following SQL script is used on In-place upgrade of ActiveEfficiency Server for Nomad.

```
-- Disclaimer:
-- Your use of this script is at your sole risk. This script is provided "as-is
", without any warranty,
-- whether express or implied, of accuracy, completeness, fitness for a particu
lar purpose, title or
-- non-infringement, and is not supported or guaranteed by 1E. 1E shall not be
liable for any damages
-- you may sustain by using this script, whether direct, indirect, special, inc
idental or consequential,
-- even if it has been advised of the possibility of such damages.

UPDATE dbo.tb_Preference
SET
Description = 'Sets the interval for synchronizing the members in Computer Cate
gory groups held in the Shopping database with Active
Directory. Also used for the ConfigMgr, Intune Machine sync and the ConfigMgr,
Intune user sync. The value for the interval uses the units defined in the
Active Directory Sync Units parameter.'
WHERE
preferencename = 'Users and Machines, AD Sync Interval'
GO

UPDATE dbo.tb_Preference
SET
Description = 'The unit is used by the AD, ConfigMgr, Intune Machine and User S
ync Interval setting. This may be set to one of the
following values: Days, Hours or Minutes.'
WHERE
preferencename = 'Users and Machines, AD Sync Units'
GO

UPDATE dbo.tb_Preference
SET
PreferenceValue = 'False'
WHERE
preferencename = 'Sync Machines and Users From Active
Efficiency'
GO

UPDATE dbo.tb_Preference
SET
Hidden = 1
WHERE
preferencename = 'Sync Machines From Old Sccm'
```

```
GO

UPDATE dbo.tb_Preference
SET
Hidden = 1
WHERE
preferencename = 'ActiveEfficiency ServerName'
GO
```

1.11.6.1.4 Manually migrate Nomad data from ActiveEfficiency to Content Distribution

The following PowerShell and SQL scripts are used on Side-by-side upgrade of ActiveEfficiency Server for Nomad. Click to download - AE-CD Data Migration Scripts.zip

Note

1. **ExportData.ps1** - run on any computer that has read access to the ActiveEfficiency database
2. **CreateTables.sql** - run on the SQL Server instance that hosts the ContentDistribution database created by Tachyon Setup
3. **ImportData.ps1** - run on any computer that has write access to the ContentDistribution database.

1.11.6.1.5 Granting Network Service access to Configuration Manager

The following SQL script is used on System Center Configuration Manager connector configuration.

```
-- Connect to the SQL instance using an account that has sysadmin rights.
-- Execute this SQL script on the Configuration Manager database.
-- The script creates a SQL Login on the instance for [hostname\ConfigMgr_DView
Access]
-- and grants it the following rights on the Configuration Manager database:
-- [db_datareader]
-- EXECUTE on [dbo].[fn_GetAppState]
-- EXECUTE on [dbo].[fnGetSiteNumber]

DECLARE @SqlLogin nvarchar(2000)
DECLARE @SqlString nvarchar(max)

SET @SqlLogin = CAST(host_name() AS varchar(512)) + '\ConfigMgr_DViewAccess'
PRINT 'Granting permissions for ''' + @SqlLogin + ''' on database ' + DB_NAME()
+ ' ...'

SET @SqlString = '
IF NOT EXISTS ( SELECT schema_name FROM information_schema.schemata WHERE schem
a_name = '''+@SqlLogin +''' )
EXEC (''CREATE SCHEMA [' + @SqlLogin + ']'')
'
EXEC sp_executesql @SqlString
```

```
SET @SqlString = '
IF NOT EXISTS (SELECT * FROM sys.server_principals WHERE name = '''+ @SqlLogin
+''')
CREATE LOGIN [' + @SqlLogin + '] FROM WINDOWS WITH DEFAULT_DATABASE=[master]
'
EXEC sp_executesql @SqlString

SET @SqlString = '
IF NOT EXISTS (SELECT * FROM sys.database_principals WHERE name = '''+ @SqlLogi
n +''')
CREATE USER [' + @SqlLogin + '] FOR LOGIN [' + @SqlLogin + '] WITH DEFAULT_SCHE
MA=[' + @SqlLogin + ']
'
EXEC sp_executesql @SqlString
PRINT 'SQL Login created.'

SET @SqlString = '
ALTER ROLE [db_datareader] ADD MEMBER [' + @SqlLogin + ']
GRANT EXECUTE ON [dbo].[fn_GetAppState] TO [' + @SqlLogin + '] AS [dbo]
GRANT EXECUTE ON [dbo].[fnGetSiteNumber] TO [' + @SqlLogin + '] AS [dbo]
'
EXEC sp_executesql @SqlString
PRINT 'Permissions granted.'
```

1.11.6.1.6 Estimating the RAM requirements for AI Powered Auto-curation

The following scripts are used on AI Powered Auto-curation to calculate the amount of additional RAM that is required before you enable this feature.

The following script is run on the Configuration Manager database before Tachyon is installed.

```
/*SCCM database query to get number of distinct software titles from SCCM datab
ase*/
USE [YourSCCMDBName]
GO
SELECT COUNT(*) AS 'Distinct Software Titles'
FROM (
        SELECT DISTINCT DisplayName0 AS Title FROM [v_ADD_REMOVE_PROGRAMS] WITH
(NOLOCK)
        UNION
        SELECT DISTINCT [Caption0] AS Title FROM [v_GS_OPERATING_SYSTEM] WITH (
NOLOCK)
) AS Titles
```

The following script is run on SLA-Data database after Tachyon is installed and has already populated the inventory repository.

```
/*SLA query to get number of distinct software titles from SLA-Data database*/
USE [SLA-Data]
CREATE TABLE #Software
       (
              [SoftwareID]                    INT IDENTITY(1,1) PRIMARY KEY,
```

```
            [DataSource]                        NVARCHAR(255) COLLATE DATABASE_
DEFAULT,
            [SoftwareIdent]                     NVARCHAR(MAX) COLLATE DATABASE_
DEFAULT,
            [SoftwareIdent_Hash]                        VARBINARY(128),
            [Vendor]                            NVARCHAR(MAX) COLLATE DATABASE_
DEFAULT,
            [Vendor_Hash]                                   VARBINARY(128),
            [Title]                             NVARCHAR(MAX) COLLATE DATABASE_
DEFAULT,
            [Title_Hash]                        VARBINARY(128),
            [Version]                           NVARCHAR(MAX) COLLATE DATABASE_
DEFAULT,
            [Version_Hash]                      VARBINARY(128),
            [ColloquialVersion]                 NVARCHAR(MAX) COLLATE DATABASE_
DEFAULT,
            [ColloquialVersion_Hash]            VARBINARY(128),
            [Edition]                           NVARCHAR(MAX) COLLATE DATABASE_
DEFAULT,
            [Edition_Hash]                      VARBINARY(128),
            [NormalizedProductID]               INT
      );
SELECT * FROM #Software
EXEC [usp_ReportDataEx_se] 1, N'Software', N'#Software';

SELECT count(*) AS 'Distinct Software Titles'
FROM
(
SELECT DISTINCT [Title] FROM #Software
) a

DROP TABLE #Software
```

1.11.6.1.7 Modifying 1E Catalog AI Powered Auto-curation file download post-installation

The following script can be used to modify the **EnableAIPackageSync** setting in the **Settings** table of the **1ECatalog** database, and is used on the Configuring 1E Catalog connection to 1E Cloud page. Click below to view the SQL script to configure the this setting.

```
/* Script to change 1ECatalog setting */
USE [1ECatalog]
GO
DECLARE @setting nvarchar(max), @oldvalue nvarchar(max), @newvalue nvarchar(max
);;
SET @setting = 'EnableAIPackageSync'
SET @newvalue = 'True'

SET @oldvalue = (SELECT [Value] FROM [dbo].[Settings] WHERE [Key]= @setting)

UPDATE [dbo].[Settings] SET [Value]=@newvalue WHERE [Key]=@setting
```

```
SELECT @setting AS 'Setting', @oldvalue AS 'Before', [Value] AS 'After' FROM [d
bo].[Settings]
WHERE [Key]=@setting
GO
```

1.11.6.1.8 Modifying the AI Package Deployment Path

The *Script to change SLA Deployment Path for AI Package* script can be used to modify the **AIModelDeploymentPath** setting in the **Settings** tables of the **SLA-Shared** and **SLA-Data** databases and is used on the AI Powered Auto-curation page. It is not possible to modify the download path use by the 1E Catalog Update service. Click below to view the SQL script to configure this setting.

```
/* Script to change SLA Deployment Path for AI Package */
/* The value is copied from SLA-Shared to instance in SLA-Data when a new inven
tory repository is created */
/* Updating SLA-Shared means script is not required for each new repository */
/* Updating all values in SLA-Data means all repositories use the same value */

DECLARE @setting nvarchar(max), @oldvalue nvarchar(max), @newvalue nvarchar(max
)
SELECT @newvalue = 'C:\ProgramData\1E\SLA Platform\AI'
SELECT @setting = 'AIModelDeploymentPath'

USE [SLA-Shared]
SELECT @oldvalue = [VALUE] FROM [dbo].[ProjectSetting]
WHERE [Group] = 'ProcessAIEngine' AND [Name] = @setting

UPDATE [dbo].[ProjectSetting] SET [Value]=@newvalue WHERE [Name]=@setting

SELECT DB_NAME() + '.dbo.ProjectSetting' AS 'Table', @setting AS 'Setting', @ol
dvalue AS 'Before', [Value] AS 'After' FROM [dbo].[ProjectSetting]
WHERE [Name]=@setting

USE [SLA-Data]
SELECT @oldvalue = [VALUE] FROM [dbo].InstanceSetting
WHERE [Group] = 'ProcessAIEngine' AND [Name] = @setting AND [InstanceID] = 1

UPDATE [dbo].[InstanceSetting] SET [Value]=@newvalue WHERE [Name]=@setting

SELECT DISTINCT DB_NAME() + '.dbo.InstanceSetting' AS 'Table', @setting AS 'Set
ting', @oldvalue AS 'Before', [Value] AS 'After' FROM [dbo].[InstanceSetting]
WHERE [Name]=@setting
GO
```

1.11.6.1.9 Modifying 1E Client Cloud synchronization behavior post-installation

The *Script to change 1ECatalog setting* script is used to configure the 1E Catalog **SubscriptionType** setting and is used on the Configuring 1E Catalog connection to 1E Cloud page. Click below to view the SQL script to configure this setting.

```
/* Script to change 1ECatalog setting */
USE [1ECatalog]
GO
DECLARE @setting nvarchar(max), @oldvalue nvarchar(max), @newvalue nvarchar(max
);;
SET @setting = 'SubscriptionType'
SET @newvalue = '2'

SET @oldvalue = (SELECT [Value] FROM [dbo].[Settings] WHERE [Key]= @setting)

UPDATE [dbo].[Settings] SET [Value]=@newvalue WHERE [Key]=@setting

SELECT @setting AS 'Setting', @oldvalue AS 'Before', [Value] AS 'After' FROM [d
bo].[Settings]
WHERE [Key]=@setting
GO
```

1.11.6.2 Operational scripts

1.11.6.2.1 Create Direct-based management groups from a file

The following PowerShell script is used on Management Groups page.

> **Note**
>
> This script has changed to support an API change in Platform 8.1

Click here to download - Create-DirectManagementGroupUsingFile.ps1

Click **Read more...** to view **Create-DirectManagementGroupUsingFile.ps1**.

```
<#
.SYNOPSIS
1E Tachyon – Create Direct Management Group
Copyright © 1e Ltd 2022 - all rights reserved
http://www.1e.com

Version 2.0

Disclaimer
Your use of this software is at your sole risk. All software is provided "as-is
", without any warranty, whether express or implied, of accuracy, completeness,
fitness for a particular purpose, title or non-infringement, and none of the so
ftware is supported or guaranteed by 1E. 1E shall not be liable for any damages
you may sustain by using this software, whether direct, indirect, special, inci
dental or consequential, even if it has been advised of the possibility of such
damages.

If you have an issue using this software, please ensure you are using an unmodi
fied version before contacting 1E Support.
```

```
.DESCRIPTION
This script reads the Device FQDN list in files and creates Direct Membership M
anagement Groups through SLA/Tachyon APIs. If the group does not exist
it is created and devices are added. If the group exists, the existing devices
are deleted and new devices are added.


.PARAMETER TachyonApiBaseUrl
Mandatory parameter.  The header name used to access the Tachyon web service.
Should match the header listed in the IIS bindings on the Tachyon server.

.PARAMETER FolderPath
Mandatory parameter.  The name of the input folder which contains the files to
be used in creating Direct Membership Management Groups. These files contain
the list of devices to be used in creating Management Groups.  The File name sh
ould be same as the name of Name of Management Group. Also, the first line
of the file should contain the description of Management Group to be created, f
rom next line onwards every line contains the Device FQDN.

.PARAMETER UseCustomCredentials
Optional switch.  If UseCustomCredentials is used, User will be prompted to ent
er the credentials, otherwise the script will use default credentials.


.EXAMPLE
.\Create-DirectManagementGroupUsingFile.ps1 -TachyonApiBaseUrl https://tachyon.
lab.local -FolderPath C:\Temp\MgFolder

Scenario:
A Tachyon server is accessed using URL https://tachyon.lab.local/Tachyon using
default credentials.  The files containing the Device FQDN list
is in the directory C:\Temp\MyFolder.

.EXAMPLE
..\Create-DirectManagementGroupUsingFile.ps1 -TachyonApiBaseUrl https://tachyon
.lab.local -FolderPath C:\Temp\MgFolder -UseCustomCredentials

Scenario:
A Tachyon server is accessed using URL https://tachyon.lab.local/Tachyon using
different credentials other than current default credentials.
The files containing the Device FQDN list is in the directory C:\Temp\MyFolder.

#>

param(
    [Parameter(Mandatory=$true, HelpMessage="Enter Tachyon API Base URL e.g. :
https://tachyon.testlab.com")]
    [ValidateNotNullOrEmpty()]
    [string] $TachyonApiBaseUrl,
```

```
    [Parameter(Mandatory=$true, HelpMessage="Enter Folder Path which contains f
iles containing Device FQDN list")]
    [ValidateNotNullOrEmpty()]
    [string] $FolderPath,

    [Parameter(Mandatory=$false, HelpMessage="To use Custom Credentials other t
han windows default credentials")]
    [Switch] $UseCustomCredentials
)

$ScriptVersion = "2.0" # Update the script version here

function Write-Log {

    [CmdletBinding()]
    Param(
          [parameter(Mandatory=$true)]
          [String]$Path,

          [parameter(Mandatory=$true)]
          [String]$Message,

          [parameter(Mandatory=$true)]
          [String]$Component,

          [Parameter(Mandatory=$true)]
          [ValidateSet("Debug", "Info", "Message", "Warning", "Error")]
          [String]$Type
    )

    switch ($Type) {
        "Info" { [int]$Type = 1 }
        "Warning" { [int]$Type = 2 }
        "Error" { [int]$Type = 3 }
        "Debug" { [int]$Type = 4 }
        "Message" { [int]$Type = 5 }
    }

    # Create a log entry
    $Content = "<![LOG[$Message]LOG]!>" +`
        "<time=`"$(Get-Date -Format "HH:mm:ss.ffffff")`" " +`
        "date=`"$(Get-Date -Format "M-d-yyyy")`" " +`
        "component=`"$Component`" " +`
        "context=`"$([System.Security.Principal.WindowsIdentity]::GetCurrent().
Name)`" " +`
        "type=`"$Type`" " +`
        "thread=`"$([Threading.Thread]::CurrentThread.ManagedThreadId)`" " +`
        "file=`"`">"

    try {
```

```
        # Write the line to the log file
        Add-Content -Path $Path -Value $Content
    }
    catch {
        Write-Host "User does not have access to write log at path $Path"
        Write-Host $Message
    }

    if ($Type -eq 1) {
        Write-Host $Message -ForegroundColor Yellow
    }

    if ($Type -eq 3) {
        Write-Host $Message -ForegroundColor Red
    }

    if ($Type -eq 5) {
        Write-Host $Message
    }
}

function Invoke-DirectMgApi{
    [CmdletBinding()]
    Param(
          [parameter(Mandatory=$true)]
          [String]$uri,

          [parameter(Mandatory=$true)]
          [String]$payload,

          [parameter(Mandatory=$false)]
          [System.Management.Automation.PSCredential]$credential
    )

    $hdrs = @{
        "Accept" = "application/json"
        "Content-type" = "application/json"
        "X-Tachyon-Consumer" = "Platform"
    }

    try {
        $stopwatchApi =  [system.diagnostics.stopwatch]::StartNew()

        $Content = "Invoking API"
        Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation
.MyCommand.Name -Type Message

        [Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType
]::Tls -bor [Net.SecurityProtocolType]::Tls11 -bor [Net.SecurityProtocolType]::
Tls12
```

```
        if($credential){
            $response = Invoke-RestMethod -Method POST -Uri $uri -Body $payload
-Credential $credential -Headers $hdrs
            $Content = "Response from API : $response"
            Write-Log -Path $LogFilePath -Message $Content -Component $MyInvoca
tion.MyCommand.Name -Type Message
        }
        else {
            $response = Invoke-RestMethod -Method POST -Uri $uri -Body $payload
-UseDefaultCredentials -Headers $hdrs
            $Content = "Response from API : $response"
            Write-Log -Path $LogFilePath -Message $Content -Component $MyInvoca
tion.MyCommand.Name -Type Message
        }

        $stopwatchApi.Stop()

        $Content = "Time taken by API : $($stopwatchApi.Elapsed.TotalSeconds) s
econds"
        Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation
.MyCommand.Name -Type Message
    }
    catch {
        $err = $_

        $Content = "An error occured : $($err.Exception)"
        Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation
.MyCommand.Name -Type Error

        $Content = "Error Details : $($err)"
        Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation
.MyCommand.Name -Type Debug
    }
}

# Get the Current Directory
$CurrentDirectory = $PSScriptRoot

if ($UseCustomCredentials -eq $true) {
    $cred = Get-Credential
}

$LogFilePath = Join-Path $PSScriptRoot "$($MyInvocation.MyCommand.Name)_$(Get-D
ate -Format ddMMyyyyHHmmss).log"

$Content = "***********************************************"
Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation.MyComma
nd.Name -Type Debug
```

```
$Content = "Starting script"
Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation.MyComma
nd.Name -Type Debug

$Content = "*********************************************"
Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation.MyComma
nd.Name -Type Debug

$Content = "Running Script Version: " + $ScriptVersion
Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation.MyComma
nd.Name -Type Debug

# Get the Current Directory

$Content = "Current Directory is " + $CurrentDirectory
Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation.MyComma
nd.Name -Type Debug

$Content = "Tachyon API Base URL: " + $TachyonApiBaseUrl
Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation.MyComma
nd.Name -Type Message

$Content = "Folder Path containing Device list files: " + $FolderPath
Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation.MyComma
nd.Name -Type Message

$Content = "Verifying Folder Path : $FolderPath"
Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation.MyComma
nd.Name -Type Debug

if (!(Test-Path $FolderPath)) {
    $Content = "Folder path does not exist : $FolderPath"
    Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation.MyC
ommand.Name -Type Error

    exit
}

$Content = "Fetching all supported files from folder"
Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation.MyComma
nd.Name -Type Debug
$files = Get-ChildItem -Path $FolderPath -Filter *.txt

$Content = "Total Files in folder $FolderPath : $($files.Count)"
Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation.MyComma
nd.Name -Type Debug

foreach($file in $files)
{
    $fileFullPath = $file.FullName
```

```
    $Content = "Reading File : $fileFullPath"
    Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation.MyC
ommand.Name -Type Message

    $stopwatchFileRead =  [system.diagnostics.stopwatch]::StartNew()

    $fqdnList = New-Object System.Collections.Generic.List[System.Object]

    foreach($line in [System.IO.File]::ReadLines($fileFullPath))
    {
        if($line -ne ""){
            $fqdnList.Add($line.Trim())
        }
    }

    if($fqdnList.Count -lt 2){
        $Content = "No device present in file"
        Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation
.MyCommand.Name -Type Error

        Continue
    }

    #File name is Management Group Name
    $MGName = $file.BaseName

    #First line of the file is the Management Group Description
    $MgDescription = $fqdnList[0]

    #Removing the first line from collection as it's MG description
    $fqdnList.RemoveAt(0)

    $uploadModelObject = [PSCustomObject]@{
        Name     = $MGName
        Description = $MgDescription
        Devices    = $fqdnList
    }

    $payload = ConvertTo-Json $uploadModelObject

    $stopwatchFileRead.Stop()

    $Content = "Time taken in reading file : $($stopwatchFileRead.Elapsed.Total
Seconds) seconds"
    Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation.MyC
ommand.Name -Type Debug

    $Content = "Creating Management Group -"
    Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation.MyC
```

```
ommand.Name -Type Info

    $Content = "  Name : $MGName"
    Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation.MyC
ommand.Name -Type Message

    $Content = "  Description : $MgDescription"
    Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation.MyC
ommand.Name -Type Message

    $Content = "  Total Devices in file : $($fqdnList.Count)"
    Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation.MyC
ommand.Name -Type Message

    #trimming any white space if any in the begining or end in url
    $TachyonApiBaseUrl = $TachyonApiBaseUrl.Trim()

    $uri = "$TachyonApiBaseUrl/admin/managementgroups/upload"

    $Content = "URI : $uri"
    Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation.MyC
ommand.Name -Type Debug

    Invoke-DirectMgApi -uri $uri -payload $payload -Credential $cred

}

$Content = "Complete"
Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation.MyComma
nd.Name -Type Message
```

1.11.6.2.2 Create Direct-based management groups from a Configuration Manager collection

The following PowerShell script is used on Management Groups page.

Note

This script has changed to support an API change in Platform 8.1

Click here to download - Create-DirectManagementGroupUsingCmCollection.ps1

Click **Read more...** to view **Create-DirectManagementGroupUsingCmCollection.ps1**.

```
<#
.SYNOPSIS
1E Tachyon – Create Direct Management Group
Copyright © 1e Ltd 2022 - all rights reserved
http://www.1e.com

Version 2.0

Disclaimer
```

Your use of this software is at your sole risk. All software is provided "as-is ", without any warranty, whether express or implied, of accuracy, completeness, fitness for a particular purpose, title or non-infringement, and none of the so ftware is supported or guaranteed by 1E. 1E shall not be liable for any damages you may sustain by using this software, whether direct, indirect, special, inci dental or consequential, even if it has been advised of the possibility of such damages.

If you have an issue using this software, please ensure you are using an unmodi fied version before contacting 1E Support.

.DESCRIPTION
This script reads the memberships of ConfigMgr Collections (Both Direct and Que ry based membership) and creates Direct Membership Management
Groups through SLA/Tachyon APIs. If the group does not exist it is created, and devices are added. If the group exists, the existing devices
are deleted and new devices are added. The script is designed to run from the C onfigMgr server It queries WMI and gets the information
necessary to connect to the ConfigMgr's site namespace.

.PARAMETER TachyonApiBaseUrl
Mandatory parameter. The header name used to access the Tachyon web service. Should match the header listed in the IIS bindings on the Tachyon server.

.PARAMETER FilePath
Mandatory parameter. The name of the input file which contains the list of col lections to be used in creating Direct Membership Management Groups. Each line in file
contains Collection Name, Management Group Name, and Management Group Descripti on; all three values separated by a comma.
e.g.
Collection 1,Management Group 1, Management Group 1 Description
Collection 2,Management Group 2, Management Group 2 Description

.PARAMETER UseCustomCredentials
Optional switch. If UseCustomCredentials is used, User will be prompted to ent er the credentials, otherwise the script will use default credentials.

.EXAMPLE
.\Create-DirectManagementGroupUsingCmCollection.ps1 -TachyonApiBaseUrl https:// tachyon.lab.local -FilePath C:\Temp\Collection.txt

Scenario:
A Tachyon server is accessed using URL https://tachyon.lab.local/Tachyon using default credentials. The file containing the list of collections to process is in the location C:\Temp\Collection.txt.

.EXAMPLE

```
..\Create-DirectManagementGroupUsingCmCollection.ps1 -TachyonApiBaseUrl https:/
/tachyon.lab.local -FilePath C:\Temp\Collection.txt -UseCustomCredentials

Scenario:
A Tachyon server is accessed using URL https://tachyon.lab.local/Tachyon using
different credentials other than current default credentials.
The file containing the list of collections to process is in the location C:\Te
mp\Collection.txt.

#>


param(
    [Parameter(Mandatory=$true, HelpMessage="Enter Tachyon API Base URL e.g. :
https://tachyon.testlab.com")]
    [ValidateNotNullOrEmpty()]
    [string] $TachyonApiBaseUrl,

    [Parameter(Mandatory=$true, HelpMessage="Enter File Path which contains col
lection details in csv format. The file should contain Collection Name, Managem
ent Group Name, and Management Group Description")]
    [ValidateNotNullOrEmpty()]
    [string] $FilePath,

    [Parameter(Mandatory=$false, HelpMessage="To use Custom Credentials other t
han windows default credentials")]
    [Switch] $UseCustomCredentials
)

$ScriptVersion = "2.0" # Update the script version here

function Write-log {

    [CmdletBinding()]
    Param(
          [parameter(Mandatory=$true)]
          [String]$Path,

          [parameter(Mandatory=$true)]
          [String]$Message,

          [parameter(Mandatory=$true)]
          [String]$Component,

          [Parameter(Mandatory=$true)]
          [ValidateSet("Debug", "Info", "Message", "Warning", "Error")]
          [String]$Type
    )

    switch ($Type) {
```

```
        "Info" { [int]$Type = 1 }
        "Warning" { [int]$Type = 2 }
        "Error" { [int]$Type = 3 }
        "Debug" { [int]$Type = 4 }
        "Message" { [int]$Type = 5 }
    }

    # Create a log entry
    $Content = "<![LOG[$Message]LOG]!>" +`
        "<time=`"$(Get-Date -Format "HH:mm:ss.ffffff")`" " +`
        "date=`"$(Get-Date -Format "M-d-yyyy")`" " +`
        "component=`"$Component`" " +`
        "context=`"$([System.Security.Principal.WindowsIdentity]::GetCurrent().
Name)`" " +`
        "type=`"$Type`" " +`
        "thread=`"$([Threading.Thread]::CurrentThread.ManagedThreadId)`" " +`
        "file=`"`">"

    try {
        # Write the line to the log file
        Add-Content -Path $Path -Value $Content
    }
    catch {
        Write-Host "User does not have access to write log at path $Path" -Fore
groundColor Yellow
        Write-Host $Message
    }

    if ($Type -eq 1) {
        Write-Host $Message -ForegroundColor Yellow
    }

    if ($Type -eq 3) {
        Write-Host $Message -ForegroundColor Red
    }

    if ($Type -eq 5) {
        Write-Host $Message
    }
}

function Invoke-DirectMgApi{
    [CmdletBinding()]
    Param(
          [parameter(Mandatory=$true)]
          [String]$uri,

          [parameter(Mandatory=$true)]
          [String]$payload,
```

```
        [parameter(Mandatory=$false)]
        [System.Management.Automation.PSCredential]$credential
    )

    $hdrs = @{
        "Accept" = "application/json"
        "Content-type" = "application/json"
        "X-Tachyon-Consumer" = "Platform"
    }

    try {
        $stopwatchApi =  [system.diagnostics.stopwatch]::StartNew()

        $Content = "Invoking API"
        Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation
.MyCommand.Name -Type Message

        [Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType
]::Tls -bor [Net.SecurityProtocolType]::Tls11 -bor [Net.SecurityProtocolType]::
Tls12

        if($credential){
            $response = Invoke-RestMethod -Method POST -Uri $uri -Body $payload
-Credential $credential -Headers $hdrs
            $Content = "Response from API : $response"
            Write-Log -Path $LogFilePath -Message $Content -Component $MyInvoca
tion.MyCommand.Name -Type Message
        }
        else {
            $response = Invoke-RestMethod -Method POST -Uri $uri -Body $payload
-UseDefaultCredentials -Headers $hdrs
            $Content = "Response from API : $response"
            Write-Log -Path $LogFilePath -Message $Content -Component $MyInvoca
tion.MyCommand.Name -Type Message
        }

        $stopwatchApi.Stop()

        $Content = "Time taken by API : $($stopwatchApi.Elapsed.TotalSeconds) s
econds"
        Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation
.MyCommand.Name -Type Message
    }
    catch {
        $err = $_

        $Content = "An error occured : $($err.Exception)"
        Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation
.MyCommand.Name -Type Error
```

```
        $Content = "Error Details : $($err)"
        Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation
.MyCommand.Name -Type Debug
    }
}

function Connect-ConfigMgrModule{
    try {
        # Load CM PowerShell Module

        if (-Not (Test-Path "HKLM:\SOFTWARE\Wow6432Node\Microsoft\ConfigMgr10\A
dminUI")) {
            $Content = "Configuration Manager not found. Pleaes verify if the m
achine has Configuration Manager installed."
            Write-Log -Path $LogFilePath -Message $Content -Component $MyInvoca
tion.MyCommand.Name -Type Error
            exit
        }

        $CMConsolePath = (Get-ItemProperty -Path "HKLM:\SOFTWARE\Wow6432Node\Mi
crosoft\ConfigMgr10\AdminUI" | Select-Object -expandProperty AdminUILog).Replac
e("\AdminUILog\", "")
        if ($CMConsolePath) {
            Import-Module -Name "$CMConsolePath\bin\ConfigurationManager.psd1"
            $Content = "Loaded ConfigurationManager.psd1 module"
            Write-Log -Path $LogFilePath -Message $Content -Component $MyInvoca
tion.MyCommand.Name -Type Debug
        }
        else {
            $Content = "ConfigurationManager.psd1 module not found. Pleaes veri
fy if the machine has Configuration Manager installed."
            Write-Log -Path $LogFilePath -Message $Content -Component $MyInvoca
tion.MyCommand.Name -Type Error
            exit
        }

        # Get the CM Site Code
        $CMSiteCode = Get-WMIObject -Namespace root\sms -Class SMS_ProviderLoca
tion | Select-Object -expandproperty SiteCode

        if ($CMSiteCode -eq "") {
            $Content = "Sitecode could not be determined."
            Write-Log -Path $LogFilePath -Message $Content -Component $MyInvoca
tion.MyCommand.Name -Type Error
            exit
        }

        $Content = "ConfigMgr Site Code: " + $CMSiteCode
        Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation
.MyCommand.Name -Type Message
```

```
        $CMLocation = $CMSiteCode + ":"

        $Content = "Setting Location : $CMLocation"
        Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation
.MyCommand.Name -Type Debug

        Push-Location

        Set-Location -Path $CMLocation
    }
    catch {
        $err = $_

        $Content = "An error occured while loading configuration manager module
: $($err.Exception)"
        Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation
.MyCommand.Name -Type Error

        $Content = "Error Details : $($err)"
        Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation
.MyCommand.Name -Type Debug

        exit
    }


}

function Read-ConfigMgrDeviceCollection{
    [CmdletBinding()]
    Param(
          [parameter(Mandatory=$true)]
          [hashtable]$collectionList
    )

    try {
        $stopwatch =  [system.diagnostics.stopwatch]::StartNew()

        $arrCMCollList = Get-CMDeviceCollection | Select-Object -Property Colle
ctionID,Name
        ForEach ($CMCollection IN $arrCMCollList){
            $CMCollName = $CMCollection.Name

            $Content = "Retrieved Collection Name from ConfigMgr: " + $CMCollNa
me
            Write-Log -Path $LogFilePath -Message $Content -Component $MyInvoca
tion.MyCommand.Name -Type Debug

            $CMCollId = $CMCollection.CollectionID
```

```
            If ($collectionList.ContainsKey($CMCollName)){

                $arrCollectionMembership = Get-CMCollectionMember -CollectionId
$CMCollID | Select-Object -expandProperty Name
                If ($null -ne $arrCollectionMembership){
                    $Content = "Fetching Devices from Collection : " + $CMCollN
ame
                    Write-Log -Path $LogFilePath -Message $Content -Component $
MyInvocation.MyCommand.Name -Type Message

                    $MgName = $collectionList["$CMCollName"][0]
                    $MgDescription = $collectionList["$CMCollName"][1]

                    #Create File to save the device list, which later will be u
sed to create MG
                    $MGFileName = $MgName + ".txt"
                    $MGFilePath = Join-Path $FolderPath $MGFileName
                    if (!(Test-Path $MGFilePath)){
                        $Content = New-Item -itemType File -Path $FolderPath -N
ame $MGFileName
                        Write-Log -Path $LogFilePath -Message $Content -Compone
nt $MyInvocation.MyCommand.Name -Type Debug

                        $Content = "Created file $MGFilePath"
                        Write-Log -Path $LogFilePath -Message $Content -Compone
nt $MyInvocation.MyCommand.Name -Type Debug

                        Add-Content -Path "$MGFilePath" -Value "$MgDescription"

                        $Content = "Added description $MgDescription"
                        Write-Log -Path $LogFilePath -Message $Content -Compone
nt $MyInvocation.MyCommand.Name -Type Debug
                    }

                    ForEach ($CollMember IN $arrCollectionMembership){
                        $deviceDetails = Get-CMDevice -Name $CollMember -Resour
ce | Select-Object Name,FullDomainName
                        $deviceFullName = $deviceDetails.Name + "." + $deviceDe
tails.FullDomainName

                        $Content = "Adding device: " + $deviceFullName + " to M
G File: " + $MgName
                        Write-Log -Path $LogFilePath -Message $Content -Compone
nt $MyInvocation.MyCommand.Name -Type Debug

                        Add-Content -Path "$MGFilePath" -Value "$deviceFullName
"
                    }
                }
```

```
            }
        }

        $stopwatch.Stop()

        $Content = "Time taken in reading devices from Collection : $($stopwatc
h.Elapsed.TotalSeconds) seconds"
        Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation
.MyCommand.Name -Type Message

        Pop-Location

        $Content = "Update location back to local drive"
        Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation
.MyCommand.Name -Type Debug

        $Content = "**********************"
        Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation
.MyCommand.Name -Type Message
    }
    catch {
        $err = $_

        $Content = "An error occured while fetching devices : $($err.Exception)
"
        Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation
.MyCommand.Name -Type Error

        $Content = "Error Details : $($err)"
        Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation
.MyCommand.Name -Type Debug

        exit
    }


}

# Get the Current Directory
$CurrentDirectory = $PSScriptRoot

#Temp Folder to contain list of devices which will be used to create MG
$MGFolderName = "MGDeviceList"
$FolderPath = Join-Path $CurrentDirectory $MGFolderName

if ($UseCustomCredentials -eq $true) {
    $cred = Get-Credential
}
```

```
$LogFilePath = Join-Path $CurrentDirectory "$($MyInvocation.MyCommand.Name)_$(G
et-Date -Format ddMMyyyyHHmmss).log"


$Content = "***********************************************"
Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation.MyComma
nd.Name -Type Debug

$Content = "Starting Script"
Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation.MyComma
nd.Name -Type Debug

$Content = "***********************************************"
Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation.MyComma
nd.Name -Type Debug

$Content = "Running Script Version: " + $ScriptVersion
Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation.MyComma
nd.Name -Type Debug

$Content = "Current Directory is: " + $CurrentDirectory
Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation.MyComma
nd.Name -Type Debug

$Content = "Tachyon API Base URL: " + $TachyonApiBaseUrl
Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation.MyComma
nd.Name -Type Message

$Content = "File Path containing CM Collection list: " + $FilePath
Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation.MyComma
nd.Name -Type Message

$Content = "Temp Folder Path to save Device List: " + $FolderPath
Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation.MyComma
nd.Name -Type Message


$Content = "Verifying File Path : $FilePath"
Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation.MyComma
nd.Name -Type Debug

if (!(Test-Path $FilePath)) {
    $Content = "File path does not exist : $FilePath"
    Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation.MyC
ommand.Name -Type Error

    exit
}
```

```
try {
    if (!(Test-Path $FolderPath)) {
        $Content = "Creating temp folder : $FolderPath"
        Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation
.MyCommand.Name -Type Debug

        $Content = New-Item -Path "$CurrentDirectory" -Name $MGFolderName -Item
Type "directory"
        Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation
.MyCommand.Name -Type Debug
    }
    else{
        $Content = "Deleting existing MG files from $FolderPath"
        Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation
.MyCommand.Name -Type Debug

        # Delete Collection Membership List Files
        Remove-Item -Path "$FolderPath\*.*"
    }
}
catch {
    $Content = "User does not have permission to create : $FolderPath"
    Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation.MyC
ommand.Name -Type Error

    exit
}

# Read Collection Details from File
$Content = "Reading collection details from $FilePath"
Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation.MyComma
nd.Name -Type Message

$collectionList = @{}

foreach($line in [System.IO.File]::ReadLines($FilePath))
{
    if($line -ne ""){
        $collectionDetails = $line.Split(",")
        if($collectionDetails.Count -lt 3){
            $Content = "Input data not in correct format. It should contain <Co
llectionName>,<MGName>,<MGDescription>"
            Write-Log -Path $LogFilePath -Message $Content -Component $MyInvoca
tion.MyCommand.Name -Type Error
            exit
        }
        $collectionList.Add($collectionDetails[0],@($collectionDetails[1],$coll
ectionDetails[2]))
    }
}
```

```
if($collectionList.Count -lt 1){
    $Content = "No collection details present in file"
    Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation.MyC
ommand.Name -Type Error

    exit
}

#Loading Config Manager Powershell Modules
Connect-ConfigMgrModule

#Read Device Collections from Config Manager and prepare device list in temp fo
lder which will be used to create
Read-ConfigMgrDeviceCollection -collectionList $collectionList

$Content = "Verifying Folder Path : $FolderPath"
Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation.MyComma
nd.Name -Type Debug

if (!(Test-Path $FolderPath)) {
    $Content = "Folder path does not exist : $FolderPath"
    Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation.MyC
ommand.Name -Type Error

    exit
}

$Content = "Fetching all files from folder"
Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation.MyComma
nd.Name -Type Debug
$files = Get-ChildItem -Path $FolderPath -Filter *.txt


$Content = "Total Files in folder $FolderPath : $($files.Count)"
Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation.MyComma
nd.Name -Type Debug

foreach($file in $files)
{
    $fileFullPath = $file.FullName

    $Content = "Reading File : $fileFullPath"
    Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation.MyC
ommand.Name -Type Message

    $stopwatchFileRead =  [system.diagnostics.stopwatch]::StartNew()

    $fqdnList = New-Object System.Collections.Generic.List[System.Object]
```

```
    foreach($line in [System.IO.File]::ReadLines($fileFullPath))
    {
        if($line -ne ""){
            $fqdnList.Add($line)
        }
    }

    if($fqdnList.Count -lt 2){
        $Content = "No device present in file"
        Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation
.MyCommand.Name -Type Error

        Continue
    }

    #File name is Management Group Name
    $MGName = $file.BaseName

    #First line of the file is the Management Group Description
    $MgDescription = $fqdnList[0]

    #Removing the first line from collection as it's MG description
    $fqdnList.RemoveAt(0)

    $uploadModelObject = [PSCustomObject]@{
        Name     = $MGName
        Description = $MgDescription
        Devices    = $fqdnList
    }

    $payload = ConvertTo-Json $uploadModelObject

    $stopwatchFileRead.Stop()

    $Content = "Time taken in reading file : $($stopwatchFileRead.Elapsed.Total
Seconds) seconds"
    Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation.MyC
ommand.Name -Type Debug

    $Content = "Creating Management Group -"
    Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation.MyC
ommand.Name -Type Info

    $Content = "  Name : $MGName"
    Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation.MyC
ommand.Name -Type Message

    $Content = "  Description : $MgDescription"
    Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation.MyC
ommand.Name -Type Message
```

```
    $Content = "  Total Devices in file : $($fqdnList.Count)"
    Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation.MyC
ommand.Name -Type Message

    #trimming any white space if any in the begining or end in url
    $TachyonApiBaseUrl = $TachyonApiBaseUrl.Trim()

    $uri = "$TachyonApiBaseUrl/admin/managementgroups/upload"

    $Content = "URI : $uri"
    Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation.MyC
ommand.Name -Type Debug

    Invoke-DirectMgApi -uri $uri -payload $payload -Credential $cred
}

$Content = "Complete"
Write-Log -Path $LogFilePath -Message $Content -Component $MyInvocation.MyComma
nd.Name -Type Message
```

1.11.7 Server installers

Windows Installer properties for each of the Tachyon server installers.

> **Warning**
>
> Tachyon Setup is the only supported method of installing, upgrading, and patching a Tachyon server.
>
> Installation using standalone **msi** or **msp** files is not supported unless advised by 1E, which may be necessary for complex installations, using non-interactive (quiet/silent) command lines, and may require further post-install configuration steps.

1.11.7.1 Tachyon Setup installation order

When installing all components on a single server, Tachyon Setup installs them in the following order:

1. Tachyon Server - **TachyonServer.msi**
2. 1E Catalog - **1ECatalog.msi**
3. SLA Platform - **SLA.Platform.Installer.msi**
4. SLA Business Intelligence - **SLA.BI.Installer.msi** (optional but required for Patch Success)
5. Nomad - **ContentDistribution.msi** (optional but required for Nomad)
6. AppClarity - **AppClarity.msi**
7. Application Migration - **ApplicationMigration.msi**

The installer properties for these MSI are provided in the following pages, including some notes on how the setup uses the properties.

- Tachyon Server installer properties
- Content Distribution installer properties
- 1E Catalog installer properties
- SLA Platform installer properties
- SLA Business Intelligence installer properties
- Application Migration installer properties
- AppClarity installer properties.

1.11.7.2 Tachyon platform zip file

The **Tachyon Platform** file can be downloaded from 1E Support Portal https://support.1e.com/. Extracting the zip will create a folder structure containing the following, where the files highlighted in bold are required by setup.

- Licenses.txt
- Tachyon Release Information.html
- **Tachyon.Setup.exe**

Please refer to:

- Tachyon Setup, for detailed information about each screen in setup
- Quick Start if you want a brief overview of installing Tachyon.

Warning

Tachyon Setup is the only supported method of installing, upgrading, and patching a Tachyon server.

Installation using standalone **msi** or **msp** files is not supported unless advised by 1E, which may be necessary in complex installations, using non-interactive (quiet/silent) command-lines, and may require further post-install configuration steps.

- Installers**1ECatalog.msi**
- Installers**AppClarity.msi**
- Installers**ApplicationMigration.msi**

This folder contains **msi installer files** for components and applications that will be installed by setup if their prerequisites are met.

- Installers**ContentDistribution.msi**
- Installers**SLA.BI.Installer.msi**
- Installers**SLA.Platform.Installer.msi**
- Installers**TachyonServer.msi**
- Installers\TachyonToolkit.msi
- Installers\Apps\Experience**Experience.zip**
- Installers\Apps\Experience**metadata.json**
- Installers\Apps\Explorer**Explorer.zip**
- Installers\Apps\Explorer**metadata.json**
- Installers\Apps\GuaranteedState**GuaranteedState.zip**
- Installers\Apps\GuaranteedState**metadata.json**
- Installers\Apps\Inventory**Inventory.zip**
- Installers\Apps\Inventory**metadata.json**
- Installers\Apps\Nomad**metadata.json**
- Installers\Apps\Nomad**Nomad.zip**
- Installers\Apps\PatchSuccess**metadata.json**
- Installers\Apps\PatchSuccess**PatchSuccess.zip**
- Installers\Apps\Settings**metadata.json**
- Installers\Apps\Settings**Platform.zip**
- ProductPacks\Newtonsoft.Json.dll

This folder contains **apps folders** for consumer applications that will be installed by setup if their prerequisites are met.

If you do not want to install a consumer application, then delete the folder before running setup.

Later, if you need to install the consumer application, then you can reinstate the folder and install the app using setup as described in Tachyon Setup.

Note

Some consumer applications are installed using their msi instead of an apps folder, for example AppClarity and Application Migration.

These Product Packs are required to support various features, for more detail please refer to

- ProductPacks\Tachyon.ProductPackDeploymentTool.exe
- ProductPacks\Tachyon.ProductPackDeploymentTool.exe.config
- ProductPacks\Tachyon.SDK.Consumer.dll
- ProductPacks\Classic\1E-ConfigMgrConsoleExtensions.zip
- ProductPacks\Classic\1E-Experience.zip
- ProductPacks\Classic\1E-Explorer-TachyonAgent.zip
- ProductPacks\Classic\1E-Explorer-TachyonCore.zip
- ProductPacks\Classic\1E-Inventory.zip
- ProductPacks\Classic\1E-Nomad.zip
- ProductPacks\Classic\1E-Patch-Success.zip
- ProductPacks\Classic\1E-Tachyon-Platform.zip
- ProductPacks\Integrated\MEMCMClientHealth.zip
- ProductPacks\Integrated\NomadClientHealth.zip
- ProductPacks\Integrated\TachyonCore.zip
- ProductPacks\Integrated\WindowsClientHealth.zip

Tachyon Product Packs reference. If your license permits, you can use additional Product Packs available from 1E Exchange to meet specific use cases.

Classic Product Packs	Contain instructions, for use in Explorer and other applications. They can be uploaded using the **Tachyon Product Pack Deployment Tool**, or using **Settings→Instructions→Instruction sets** page in the Tachyon portal.
Integrated Product Packs	Contain policies, rules and fragments for use by Guaranteed State, and may also include instructions. They can only be uploaded using the **Tachyon Product Pack Deployment Tool**.

Tip

The **Tachyon Product Pack Deployment Tool** can be started independently or at the end of the **Tachyon Setup** process via the Post-installation checks screen, where the screen contains a link that launches the tool. The **Tachyon Setup** method of starting the tool is recommended because Tachyon Setup ensures you have the correct permissions to upload the Product Packs.

1.11.7.3 Tachyon Server installer properties

A table of the Windows Installer properties for the Tachyon Server installer.

Warning

Tachyon Setup is the only supported method of installing, upgrading, and patching a Tachyon server.

Installation using standalone **msi** or **msp** files is not supported unless advised by 1E, which may be necessary in complex installations, using non-interactive (quiet/silent) command-lines, and may require further post-install configuration steps.

Note

Mandatory properties must be provided when installing using a command-line.

The installer file is: **TachyonServer.msi**

The fields in the table below are:

ACTIVE_DIRECTORY_SERVER | ADDLOCAL | DEVICECOUNT | DROPOLDDB_EXPERIENCE | DROPOLDDB_MASTER | DROPOLDDB_RESPONSES | EXTERNALIISHOSTHEADER | HTTPSIISPORT | IISIPADDRESS | IISPORT | INSTALLDIR | INTERNALIISHOSTHEADER | LICENSEFILEPATH | LOGPATH | MAILFROM | SERVERCERTIFICATETHUMBPRINT | SMTPENABLED | SMTPPORT | SMTPSERVER | SQLSERVER_EXPERIENCE | SQLSERVER_MASTER | SQLSERVER_RESPONSES | SSASDROPDB_EXPERIENCE | SSASSERVER_EXPERIENCE | STARTCOORDINATOR | STARTSWITCH | TWOFACTORAUTHENABLED | WORKFLOWWEBPORT

Property	Default	Mandatory	Description
ACTIVE_DIRECTORY_SERVER	GC://	Yes	A list of Active Directory URLs. Tachyon services locate users and computers and membership of security groups by querying a semi-colon delimited list of Active Directory GC and/or LDAP URLs. GC URL: This is the quickest and simplest method of resolving users and group membership. A single GC URL will normally resolve all users and groups within a single **forest**. Supports only Universal security groups. LDAP URL: A single LDAP URL will normally resolve all users and groups within a single **domain**. Supports Universal and Global security groups. Required if a Global Catalog (GC) server does not exist in a trusted forest, or if Global security groups must be used.

Property	Default	Mandatory	Description
			Any domain which contains Tachyon servers, users or groups must: • be resolvable from the Tachyon Server using DNS - that is, the server must be able to resolve domain names using DNS • have a two-way trust with the domain in which the Tachyon (Master Stack) Server exists - so that users trust the server, and the server trusts users • allow the Tachyon Server to read computer, user and security group objects in each domain The default **GC://** is sufficient for a Tachyon Server in a simple Active Directory environment of one forest which has a Global Catalog. You can include, but it is not required, the name of the server's local domain or root domain, for example: **GC://acme.local** To add support for a remote forest which has its own GC, you would for example have **GC://acme.local;GC://nadir.local** and so forth adding the root domain of any other forests to the list of GC URLs. If you prefer to use LDAP, or there are difficulties with trusts between forest domains, then you would create a list of LDAP URLs including *all* domains that have Tachyon users and groups, as well as domains in which a Tachyon server resides. For example: **LDAP://acme.local;LDAP://pop.acme.local;LDAP://rock.acme.local;LDAP://country.acme.local;LDAP://nadir.local;LDAP://disco.nadir.local** You can mix GC and LDAP URLs, but you should avoid mixing LDAP URLs that are also resolved by a GC URL. For example: **GC://;LDAP://nadir.local;LDAP://disco.nadir.local** The Coordinator Workflow module queries AD for email details of Tachyon users, and the Consumer API queries AD

Property	Default	Mandatory	Description

			for security details of Tachyon users to support Role-Based Access Control.
			
			Tachyon Setup will verify the details you have supplied. However you can run the following command on your server to confirm it can resolve the name of the local domain in DNS and locate Domain Controllers with the Global Catalog role.
			
			`nslookup gc._msdcs`
			
			Use the following command to resolve **<domain>** and its GC DCs.
			
			`nslookup gc._msdcs.<domain>`

ADDLOCAL	ALL	No	Default is **ALL** when installing all components on a single-server. The following components (MSI features) are selected when installing a Master Stack, Response Stack and Custom configuration. Names are delimited by a comma and are case-sensitive. Master Stack: • ConfigurationViewer • Coordinator • Consumer • Database_EXPERIENCE • Database_MASTER • Experience • Portal • SSASDatabase_EXPERIENCE Response Stack: • Background • Core • CoreInternal • Database_RESPONSES • Switch Specifying Portal or Experience does not install Tachyon applications, but are required in order for relevant

Property	Default	Mandatory	Description
			applications to work. Tachyon applications are installed separately by Tachyon Setup.
DEVICECOUNT	1000	No	This is the number of devices supported by the Tachyon server which is being installed. The number of devices supported by a Tachyon Server determines the number of Switches configured on the server. The range is 1 to 250,000; default is 1,000. A single server with suitable resources can support up to five Switches and up to 250,000 devices, with each Switch supporting up to 50,000 devices. Additional servers or configuration may be required according to the design of the Tachyon system. The total number of devices supported across the Tachyonsystem must not exceed the license file allocation.
DROPOLDDB_EXPERIENCE	0	No	If set to 1 then the installer will drop the TachyonExperience database and attempt to create a new database. To create the database requires the server installation account has sysadmin rights on the SQL Server instance SQLSERVER_MASTER. If set to 0 (default) then the installer will keep the existing TachyonResponses database. This requires the installation account has db_owner rights on the database. This setting is used in the following scenarios. • For a new installation and an empty database has been pre-created. • When the database has been restored and Tachyon is being re-installed either during a recovery, or because the database has been moved to a new SQL Server instance. • Upgrading.

Property	Default	Mandatory	Description
DROPOLDDB_MASTER	0	No	If set to 1 then the installer will drop the TachyonMaster database and attempt to create a new database. To create the database requires the server installation account has sysadmin rights on the SQL Server instance SQLSERVER_MASTER. If set to 0 (default) then the installer will keep the existing TachyonResponses database. This requires the installation account has db_owner rights on the database. This setting is used in the following scenarios. • For a new installation and an empty database has been pre-created. • When the database has been restored and Tachyon is being re-installed either during a recovery, or because the database has been moved to a new SQL Server instance. • Upgrading.
DROPOLDDB_RESPONSES	0	No	If set to 1 then the installer will drop the TachyonResponses database and attempt to create a new database. To create the database requires the server installation account has sysadmin rights on the SQL Server instance SQLSERVER_RESPONSES. If set to 0 (default) then the installer will keep the existing TachyonResponses database. This requires the installation account has db_owner rights on the database. This setting is used in the following scenarios. • For a new installation and an empty database has been pre-created. • When the database has been restored and Tachyon is being re-installed either during a recovery, or because the database has been moved to a new SQL Server instance. • Upgrading.

Property	Default	Mandatory	Description
EXTERNALIISHOSTHEADER	TACHYON.<DomainFQDN>	Yes	Sets the host header used by the HTTPS binding of the Tachyon Website. This must be the same as the DNS Alias FQDN. EXTERNALIISHOSTHEADER and HTTPSIISPORT configure the HTTPS binding that uniquely identifies the Tachyon Website used by the following: • Browsers connection to the Explorer (Explorer and Admin) • Tachyon clients retrieving content from the Background Channel • Internal Tachyonservices
HTTPSIISPORT **HTTPSIISPORT**	443	Yes	Sets the port used by the HTTPS binding of the Tachyon Website. EXTERNALIISHOSTHEADER and HTTPSIISPORT configure the HTTPS binding that uniquely identifies the Tachyon Website used by the following: • Browsers connection to the Explorer (Explorer and Admin) • Tachyon clients retrieving content from the Background Channel • Internal Tachyon services
IISIPADDRESS	*	Yes	Sets the IP Address used by the HTTP and HTTPS bindings of the Tachyon Website. The default value of * sets IIS to listen on all IP addresses. On multihomed servers with multiple IP addresses you may optionally set this value, but in general we recommend leaving this as * to bind to all IP addresses. If this value is set it must correspond to one of the IP addresses configured for the DNS Alias FQDN.

Property	Default	Mandatory	Description
			INTERNALIISHOSTHEADER, IISIPADDRESS and IISPORT configure the HTTP binding that can be used to access IIS web applications that are *not* configured to **Require SSL**, for example ContentDistribution, CoreExternal and CatalogWeb. Please refer to Verify IIS Configuration for configuration details of IIS web applications.
IISPORT	80	Yes	Sets the port used by the HTTP binding of the Tachyon Website. INTERNALIISHOSTHEADER, IISIPADDRESS and IISPORT configure the HTTP binding that can be used to access IIS web applications that are *not* configured to **Require SSL**, for example ContentDistribution, CoreExternal and CatalogWeb. Please refer to Verify IIS Configuration for configuration details of IIS web applications.
INSTALLDIR	%ProgramFiles%\1E\Tachyon\	No	Sets the installation folder for all the Tachyon components. For a non-default installation please refer to Services and NTFS Security.
INTERNALIISHOSTHEADER	<computername>.<DomainFQDN>	Yes	Sets the host header used by the HTTP binding of the Tachyon Website. This should be the computername FQDN of the Tachyon Server. INTERNALIISHOSTHEADER, IISIPADDRESS and IISPORT configure the HTTP binding that can be used to access IIS web applications that are *not* configured to **Require SSL**, for example ContentDistribution, CoreExternal and CatalogWeb. Please refer to Verify IIS Configuration for configuration details of IIS web applications.
LICENSEFILEPATH		Yes (UI) No (comm	The full path, including the file name, must be provided for a valid Tachyon license file. 1E will provide you with a **Tachyon.lic** license file that defines the applications, tools, and features your Tachyon System is able to use, for how long, and how many

Property	Default	Mandatory	Description
		and-line)	devices it supports, this may be an evaluation or subscription license. • The license must be activated. Once activated, it may be used only by the Tachyon System that activated it. • Licenses can be renewed or updated, but if allowed to expire, then the affected products or features will not be usable. • For a new installation, the Tachyon Setup program will let you select the license file from any folder on disk. • For an existing installation, the license file is copied into the folder: %PROGRAMDATA%\1E\Licensing on your Tachyon Server.
LOGPATH	%AllUsersProfile%\1E\Tachyon\	No	Sets the path to the Tachyon server log files. It does not set the filename of each log. See Log files for more details. For a non-default installation please refer to Services and NTFS Security. **Warning** Not supported by Tachyon Setup. If you need to change the default location, please contact 1E.
MAILFROM		Yes	Sets the mail-from email address used by the Tachyon Server when it sends emails. For guidance about the Mail-From address see Email and 2FA requirements.
SERVERCERTIFICATETHUMBPRINT		No	Used by Tachyon Setup to uniquely identify which certificate was selected by the user for use by Tachyon components. Tachyon Setup uses the selected certificate

Property	Default	Mandatory	Description
			to assign to the main binding for the Tachyon website, the coordinator web service, and Switches. `SERVERCERTIFICATETHUMBPRINT=3d699d8f28c2d7e0514cb0e047a1fd2f9db9bf4f` If you are using the installer instead of Tachyon Setup, and do not specify a thumbprint property in the command-line, the installer will automatically select the first suitable certificate it finds in the server's Personal certificate store. In which case you must ensure there is only one suitable certificate, otherwise you may find Switches, and the bindings for the website and coordinator using different certificates. You can review the bindings using Tachyon Setup→ Maintenance→ Server certificate... as decribed in Verify the Tachyon Server certificate bindings. See Certificate requirements for requirements.
SMTPENABLED	1	No	Determines whether Tachyon email features are available. It uses email for • notifications • two-factor authentication • sending Telemetry data to 1E. For guidance about using non-default SMTP settings, see Email and 2FA requirements. If email notifications need to be disabled after installation, then see Changing the SMTP Host configuration. To configure Telemetry after installation, please refer to Enabling or disabling Telemetry features. If set to 1 then email is enabled. If set to 0 then the following are disabled: • Email notifications

Property	Default	Mandatory	Description
			• Two-factor authentication - see TWOFACTORAUTHENABLED • Sending Telemetry data to 1E
SMTPPORT	25	No	Sets the port used to connect to the SMTP relay/gateway Default is 25. If the port needs to be changed after installation, then see Changing the SMTP Host configuration.
SMTPSERVER		Yes	Sets the FQDN of the SMTP relay/gateway. If the FQDN needs to be changed after installation, then see Changing the SMTP Host configuration.

SQLSERVER_EXPERIENCE	(local)	Yes	Sets the name for the SQL Server instance that hosts the TachyonExperience database.
			This can be set in one of the following formats depending on the setup of the instance.
			`(local)`
			`ServerName`
			`ServerName,PortNumber`
			`ServerName\InstanceName`
			`ServerName\InstanceName,PortNumber`

SQLSERVER_MASTER	(local)	Yes	Sets the name for the SQL Server instance that hosts the TachyonMaster database.
			This can be set in one of the following formats depending on the setup of the instance.
			`(local)`
			`ServerName`
			`ServerName,PortNumber`
			`ServerName\InstanceName`
			`ServerName\InstanceName,PortNumber`

SQLSERVER_RESPONSES	(local)	Yes	Sets the name for the SQL Server instance that hosts the TachyonResponses database.

Property	Default	Mandatory	Description

			This can be set in one of the following formats depending on the setup of the instance.
			
			`(local)`
			`ServerName`
			`ServerName,PortNumber`
			`ServerName\InstanceName`
			`ServerName\InstanceName,PortNumber`

SSASDROPDB_EXPERIENCE	0	No	If set to 1 then the installer will drop the TachyonExperience cube and attempt to create a new cube. To create the cube requires the server installation account has sysadmin rights on the SQL Server Analysis Service instance SSASSERVER_EXPERIENCE. If set to 0 (default) then the installer will keep the existing TachyonExperience cube.

SSASSERVER_EXPERIENCE	(local)	Yes	Sets the name for the SQL Server Analysis Service instance that hosts the TachyonExperience cube.
			
			This can be set in one of the following formats depending on the setup of the instance.
			
			`(local)`
			`ServerName`
			`ServerName,PortNumber`
			`ServerName\InstanceName`
			`ServerName\InstanceName,PortNumber`

STARTCOORDINATOR	1	No	Flag indicating if the Coordinator service should be started after installation.
STARTSWITCH	1	No	Flag indicating if the Switch Host service should be started after installation.
TWOFACTORAUTHENABLED	1	No	Determines whether Tachyon uses two-factor authentication. If email is disabled then so is two-factor authentication which relies on email.

Property	Default	Mandatory	Description
			See Email and 2FA requirements. Default is same as SMTPENABLED.
WORKFLOWWEBPORT	8080	No	Sets the port used by HTTPS binding of the Coordinator Workflow module. This is separate from the Tachyon Website. **Tachyon Setup** suggests **8081** by default, and should not need to be changed. **Note** **TachyonServer.msi** installer defaults to **8080** if the WORKFLOWWEBPORT parameter is not provided. Tachyon Setup uses **8081** to avoid conflict with HTTP port 8080 which is the default used by SLA Platform 3.3 and earlier versions.

1.11.7.4 Content Distribution installer properties

A table of the Windows installer properties for the Content Distribution installer.

Warning

Tachyon Setup is the only supported method of installing, upgrading, and patching a Tachyon server.

Installation using standalone **msi** or **msp** files is not supported unless advised by 1E, which may be necessary in complex installations, using non-interactive (quiet/silent) command-lines, and may require further post-install configuration steps.

Note

Mandatory properties must be provided when installing using a command-line.

The installer file is: **ContentDistribution.msi**

CMSERVER | DATABASE_MODE | DBNAME | DBSERVER | DROPOLDDB | IDLETIMEOUTMINS | INSTALLDIR | NOMADSYNCINTERVAL | PLATFORMURL | RECYLEMINS | SITENUMBER | WAKEUPURL

Property	Default	Mandatory	Description
CMSERVER		Yes	Name of the Configuration Manager Site server. ContentDistribution will fetch CM database details for synchronization. The Content Distribution installer connects and reads the root\sms WMI namespace on ConfigMgr site server to get the associated SMS Providers and their details. Query - SELECT SiteCode, Machine, NamespacePath FROM SMS_Providerlocation WHERE ProviderForLocalSite=TRUE. The connection could be locally or remotely depending on where the SiteServer is. Then connects to each SMS Provider WMI Namespace \\providerfqdn\root\sms\site_XXX one by one and uses the one it is able to connect to get the details like SMS DB Name and ServerName etc. The WMI Access could be local or remote depending on where the SMS Provider is. Query - SELECT * FROM SMS_SCI_SiteDefinition WHERE ItemName = "Site Definition" AND SiteCode = "XXX". You can also provide a SMS provider server name as value of CMSERVER property but in that case only that provider will be tried and if installer fails to connect to it, no other sms provider associated with the site will be tried.
DATABASE_MODE	*SingleUser*		Database usage mode. It may be set to one of the following values: • *SingleUser* - Sets the upgrade scripts to run in single user mode • *MultiUser* - Sets the upgrade scripts to run in multi-user mode The default value sets the upgrade scripts to run in single-user mode to avoid multiple connections during upgrade (Only for SQL 2005).

Property	Default	Mandatory	Description
			Enabling *MultiUser* mode, by setting the following property on the installer command-line, may be necessary for larger databases to help to smooth the upgrade process: *DATABASE_MODE= "MultiUser"* **Note** Please Note: MultUser and SingleUser are case sensitive
DBNAME	ContentDistribution		Name for the ContentDistribution database.
DBSERVER	localhost	Yes	Name of the SQL Server instance where the ContentDistribution database is installed.
DROPOLDDB	0		If set to 1 on the command-line, it drops the current ContentDistribution database during installation. The default behavior for this property is to not drop the old database. **Note** Exercise caution when using this option, as any existing data will be deleted. Do not use this option if you want to preserve your existing data.
IDLETIMEOUTMINS	0		Specify the amount of time (in minutes) for which a worker process (of CD app pool) should remain idle before it's shutdown.
INSTALLDIR	C:\Program Files\1E\Content Distribution		The installation directory in the Destination Folder screen.
NOMADSYNCINTERVAL	30		The interval (in minutes) before the next data synchronization takes place between Nomad and Configuration Manager. The valid range for this interval is between 5 and 1440 (1 day) minutes. If you set the interval below the lower limit, it

Property	Default	Mandatory	Description
			defaults to the minimum (5 minutes). Similarly, if you set the interval above the upper limit, it defaults to 1440 minutes. If a synchronization fails, it restarts after 15 minutes. Used in the Nomad screen.
PLATFORMURL		Yes	Platform base URL of the Tachyon website.
RECYLEMINS	0		Specify the amount of time (in minutes) after which ContentDistribution application pool should be recycled.
SITENUMBER			Exposed to Tachyon Setup only. Tachyon Setup sets its value to Tachyon website Site ID. Installer installs the Content Distribution application under the Web site whose site number matches the specified one.
WAKEUPURL			To support Nomad integration with WakeUp. Specify either an HTTP or HTTPS URL to match the binding used on the NightWatchman web server. The port does not need to be included if using a standard HTTP/S port 80 or 443. • http://<NightWatchmanServer>:8080/nwmc/MachineSearchService • https://<NightWatchmanServer>:8443/nwmc/MachineSearchService This adds a **Url** setting to the **AppSettings** section of %Program Files%1E\ContentDistribution\Web\WebService\appsettings.json file.

1.11.7.5 1E Catalog installer properties

A table of the Windows installer properties for the 1E Catalog installer.

Warning

Tachyon Setup is the only supported method of installing, upgrading, and patching a Tachyon server.

Installation using standalone **msi** or **msp** files is not supported unless advised by 1E, which may be necessary in complex installations, using non-interactive (quiet/silent) command-lines, and may require further post-install configuration steps.

Note

Mandatory properties must be provided when installing using a command-line.

The installer file is: **1ECatalog.msi**

DATABASENAME | DROPOLDDB | IISHOSTHEADER | IISIPADDRESS | IISPORT | INSTALLDIR | LOGPATH | SQLSERVER | SVCPASSWORD | SVCUSER

Property	Default	Mandatory	Description
DATABASENAME	1ECatalog	No	Name for the 1E Catalog database.
DROPOLDDB	0	No	If set to 1 on the command-line, it drops the 1ECatalog database during installation if it exists on the specified SQL Server instance. The default behavior for this property is to not drop the existing database. **Note** Exercise caution when using this option as any existing data will be deleted. Do not use this option if you want to preserve your existing data.
IISHOSTHEADER		No	Host header used for the HTTP binding of the website hosting the CatalogWeb web application. If used, this should be a DNS FQDN of the web server, recommended to be a CNAME, for example: *catalog.acme.local* **Note**

Property	Default	Mandatory	Description
			See HTTP binding note below. **Note** When installed by Tachyon Setup the HTTP host header is not specified, causing the CatalogWeb application to be installed under the Default website or its own CatalogWeb website.
IISIPADDRESS	*	No	IP address used for the HTTP binding of the website hosting the CatalogWeb web application. If you want to be non-specific about the IP address, use the default *. **Note** See HTTP binding note below. **Note** When installed by Tachyon Setup the HTTP IP Address is not specified, causing the CatalogWeb application to be installed under the Default website or its own CatalogWeb website.
IISPORT	80	No	Port used for the HTTP binding of the website hosting the CatalogWeb web application. **Note** See HTTP binding note below. **Note** When installed by Tachyon Setup the HTTP port is not specified, causing the CatalogWeb application to be installed under the

Property	Default	Mandatory	Description
			Default website or its own CatalogWeb website.
INSTALLDIR	C:\Program Files\1E\Catalog\	No	The installation directory in the Destination Folder screen. **Note** When installed by Tachyon Setup the installation folder for Catalog has the same parent folder as the Tachyon installation.
LOGPATH	C:\ProgramData\1E\Catalog\	No	The folder where the Catalog.UpdateService.log file is found.
SQLSERVER	(local)	Yes	Name of the SQL Server instance where the 1E Catalog database is installed.
SVCPASSWORD		No	Password for SVCUSER.
SVCUSER	NT AUTHORITY\Network Service	No	User name for the **1E Catalog Update Service** service account and website **application pool**. **Note** Do not use the SVCUSER property if you want to use the default. **Note** Tachyon Setup uses **NT AUTHORITY\Network Service**.

HTTP binding

If an existing website uses the same HTTP binding (combination of HTTP port and IP address, and also Host Header if used) then the Catalog web application will be created under that website. For example, the Catalog web application is normally created under

Default Web Site because it uses port 80 and * by default. If an existing web site does not have a matching HTTP binding then the installer will create a new website called CatalogWeb with the specified HTTP binding.

HTTPS is not supported. Please contact 1E if this is required.

1.11.7.6 SLA Platform installer properties

A table of the Windows installer properties for the SLA Platform installer.

Warning

Tachyon Setup is the only supported method of installing, upgrading, and patching a Tachyon server.

Installation using standalone **msi** or **msp** files is not supported unless advised by 1E, which may be necessary in complex installations, using non-interactive (quiet/silent) command-lines, and may require further post-install configuration steps.

Note

Mandatory properties must be provided when installing using a command-line. The table shows which default values are managed by Tachyon Setup

The installer file is: **SLA.Platform.Installer.msi**

CATALOG_DATABASE_NAME | CATALOG_DATABASE_SERVER | CATALOG_DATABASE_USEINTEGRATEDSECURITY | COMMON_DATABASE_SERVER | COMMON_DATABASE_USEINTEGRATEDSECURITY | CUSTOMER_USERNAME | IIS_HOST_HEADER | IIS_HTTP_PORT | IIS_HTTPS_PORT | IIS_IP_ADDRESS | IIS_SITE_NAME | IIS_SSL_CERTIFICATE_SERIAL | IIS_SSL_CERTIFICATE_STORE_NAME | IIS_SSL_CERTIFICATE_STORE_LOCATION | IIS_SSL_CERTIFICATE_THUMBPRINT | INSTALLFOLDER | INTEGRATE_REST_PORT | LOG_FOLDER | SLA_ENABLE_HTTPS | SLA_PLATFORM_FQDN | SVC_USEACCOUNT | SVC_USEACCOUNT_PASSWORD | SVC_USEACCOUNT_USERNAME | TARGETDIR

Property	Default	Mandatory	Description
CATALOG_DATABASE_NAME	1ECatalog	No	The name of the 1E Catalog database.
CATALOG_DATABASE_SERVER		Yes	The SQL Server instance name which hosts the 1E Catalog database. **Note** Tachyon Setup prompts for the SQL Server database instance.

Property	Default	Mandatory	Description
CATALOG_DATABASE_USEINTEGRATEDSECURITY	1	No	Determines which method the SLA Platform services and application pools will acess the 1E Catalog database • 1 - Windows authentication uses the specified SVC_USEACCOUNT service account • 0 - SQL authentication uses the specified SQL Login The SLA Platform uses a Linked Server on the SQL Server instance that hosts the SLA Platform databases, to access the 1E Catalog database. The SLA Platform also connects to the Catalog API, which it finds by reading the CatalogSettings table in the 1E Catalog database. **Note** Tachyon Setup uses 1: Windows authentication.
COMMON_DATABASE_SERVER		Yes	The SQL Server instance name which will host the four SLA Platform databases. **Warning** Do not specify (local) even if the SQL Server instance is local. This avoids issues with Linked

Property	Default	Mandatory	Description
			servers used by SLA Platform and companion products. **Note** DROPOLDDB is not supported. If you want to create new databases then manually drop the old ones first, after backing them up. **Note** Tachyon Setup prompts for the name of the SQL Server instance.
COMMON_DATABASE_USEINTEGRATEDSECURITY	1	No	Determines which method the SLA Platform services and application pools will acess the SLA Platform databases • 1 - Windows authentication uses the specified SVC_USEACCOUNT service account • 0 - SQL authentication uses the specified SQL Login **Note** Tachyon Setup uses 1: Windows authentication.
CUSTOMER_USERNAME	The installer account	No	The **default web user**.

Property	Default	Mandatory	Description
			• Must be a domain user account • Normally the same as the Installer account • Specified in the **Customization Settings** panel in the SLA Platform installer (not available in Tachyon Setup) • This is the only account that can be used when first logging into the SLA Platform website, until the account is used to create additional users **Warning** The **Domain** part of the username will restrict access to SLA Platform to just users from that domain. See Server installation account **Note** Tachyon Setup uses the default: the installer account.
IIS_HOST_HEADER			Host header used for the HTTP binding of the SLA Platform website. **Note**

Property	Default	Mandatory	Description
			See HTTP binding note below. **Note** Tachyon Setup uses the same HTTP host header as the Tachyon website, which defaults to the servername FQDN.
IIS_HTTP_PORT	8080	No	Port used for the HTTP binding of the SLA Platform Website. **Note** See HTTP binding note below. **Note** Tachyon Setup uses the same HTTP port as the Tachyon website, which defaults to **80**. This causes the SLA Platform web applications to be installed under the Tachyon website.
IIS_HTTPS_PORT	8443	No	Port used for the HTTPS binding of the SLA Platform website. Used only if SLA_ENABLE_HTTPS=1. **Note** See HTTPS binding note below. **Note** Tachyon Setup uses the same HTTPS port

Property	Default	Mandatory	Description
			as the Tachyon website, which defaults to **443**. This causes the SLA Platform web applications to be installed under the Tachyon website.
IIS_IP_ADDRESS	*	No	IP address used for the HTTP binding of the SLA Platform website. If you want to be non-specific about the IP address, use the default *. **Note** See HTTP binding note below. **Note** Tachyon Setup uses the same HTTP IP Address binding as the HTTP binding IP Address of the Tachyon website, which defaults to *** (all)**. This causes the SLA Platform web applications to be installed under the Tachyon website.
IIS_SITE_NAME	SLA Platform Web Site	No	Website name. Not configurable in the installer UI. **Note** Tachyon Setup does not use this as it

Property	Default	Mandatory	Description
			expects the SLA Platform will be installed under the Tachyon website.
IIS_SSL_CERTIFICATE_SERIAL		Yes, if HTTPS is enabled	The **serial number** of the specified SSL certificate. Used only if SLA_ENABLE_HTTPS=1. **Note** See HTTPS binding note below. **Note** Tachyon Setup uses the same web server certificate as the Tachyon website.
IIS_SSL_CERTIFICATE_STORE_NAME	My	No	The **certificate store** in which to search for the specified SSL certificate. **My** is the Personal store. Used only if SLA_ENABLE_HTTPS=1. **Note** Tachyon Setup uses the default: My.
IIS_SSL_CERTIFICATE_STORE_LOCATION	LocalMachine	No	The **account type** for the specified certificate store. **LocalMachine** is the Computer account. Used only if SLA_ENABLE_HTTPS=1. **Note** Tachyon Setup uses the default: LocalMachine.

Property	Default	Mandatory	Description
IIS_SSL_CERTIFICATE_THUMBPRINT		Yes, if HTTPS is enabled	The **thumbprint** of the specified SSL certificate. Used only if SLA_ENABLE_HTTPS=1. **Note** See HTTPS binding note below. **Note** Tachyon Setup uses the same web server certificate as the Tachyon website.
INSTALLFOLDER	C:\Program Files\1E\SLAPlatform\	No	The installation directory in the **Custom Setup** screen. **Note** If you change the install location please ensure the service account has the necessary NTFS security permissions, as described in Services and NTFS Security. **Note** Tachyon Setup uses the same parent folder as the Tachyon installation. **Warning** The SLA Platform installer does not support INSTALLDIR.
INTEGRATE_REST_PORT	6002	No	Port used by SLA Integrate services. The Integrate

Property	Default	Mandatory	Description
			Manager listens on this port for the Integrate Agent. **Note** Tachyon Setup uses the default 6002.
LOG_FOLDER	C:\ProgramData	No	The folder where the SLA Platform log files are found, as well as other resource files, including inventory product packs. • 1E.SLAConnector.sccm_sync.log • 1E.SLAPlatformIntegrateAgent.log • 1E.SLAPlatformIntegrateManager.log An additional logs folder is found in C:\ProgramData\1E\Platform Consumer **Note** If you change the logs folder location please ensure the service account has the necessary NTFS security permissions, as described in Services and NTFS Security **Warning** The SLA Platform installer does not support LOGPATH

Property	Default	Mandatory	Description
			Note Not used by Tachyon Setup.
SLA_ENABLE_HTTPS	1	No	Determines whether an HTTPS binding is created in addition to the HTTP binding. **Note** Tachyon Setup uses **1**: enable HTTPS.
SLA_PLATFORM_FQDN	The FQDN of the server	No	The FQDN of the SLA Platform server.
SVC_USEACCOUNT	1	Yes	Specifies whether the service account is a domain account (1) or Network Service (0). **Note** Tachyon Setup uses **0**: Network Service. The service account is used for the following: • 1E SLA Platform Engine service • 1E SLA Platform Integrate Agent service • 1E SLA Platform Integrate Manager service • SLAPlatform web application pools (3)
SVC_USEACCOUNT_PASSWORD		Yes	Password for SVC_USEACCOUNT_USERNAME.

Property	Default	Mandatory	Description
			Note Not used by Tachyon Setup.
SVC_USEACCOUNT_USERNAME		No	The service account if SVC_USEACCOUNT=1. Must be specified as **domain\username**. **Note** Not used by Tachyon Setup.
TARGETDIR	C:\	No	*TARGETDIR*is used only for administrative installation, it is not used for normal installations. You need to use the *TARGETDIR* property for an administrative installation of SLA Platform, for example if you want to unpack the MSI to find a specific file. `msiexec /a SLA.Platform.Installer.msi TARGETDIR="C:\Source\SLAPlatform"` **Note** Not used by Tachyon Setup.

HTTP binding

If an existing website uses the same HTTP binding (combination of HTTP port, host header and IP address) then the SLA Platform web applications will be created under that website instead of under a dedicated website called SLA Platform Web Site.

HTTPS binding

When doing a non-interactive install, an HTTPS binding is created only if all of the following are specified:

- SLA_ENABLE_HTTPS=1

- IIS_SSL_CERTIFICATE_SERIAL
- IIS_SSL_CERTIFICATE_THUMBPRINT

1.11.7.7 SLA Business Intelligence installer properties

A table of the Windows installer properties for the SLA Business Intelligence installer. Business Intelligence is only required by the Patch Success application.

> **Warning**
>
> Tachyon Setup is the only supported method of installing, upgrading, and patching a Tachyon server.
>
> Installation using standalone **msi** or **msp** files is not supported unless advised by 1E, which may be necessary in complex installations, using non-interactive (quiet/silent) command-lines, and may require further post-install configuration steps.
>
> **Note**
>
> Mandatory properties must be provided when installing using a command-line.

The installer file is: **SLA.BI.Installer.msi**

BI_DATABASE_DROPDB | BI_DATABASE_NAME | BI_DATABASE_PASSWORD | BI_DATABASE_SERVER | BI_DATABASE_USEINTEGRATEDSECURITY | BI_DATABASE_USERNAME | COMMON_DATABASE_NAME | SSAS_DATABASE_DROPDB | SSAS_DATABASE_NAME | SSAS_DATABASE_PASSWORD | SSAS_DATABASE_SERVER | SSAS_DATABASE_USERNAME

Property	Default	Mandatory	Description
BI_DATABASE_DROPDB	0		If set to 1 on the command-line, it drops the SLA-BI database during installation if it exists on the specified SQL Server instance. The default behavior for this property is to not drop the existing database. **Note** Exercise caution when using this option as any existing data will be deleted. Do not use this option if you want to preserve your existing data.

Property	Default	Mandatory	Description
BI_DATABASE_NAME	SLA-BI		The name of the SLA-BI database.
BI_DATABASE_PASSWORD		Depends	If not using integrated security, this property specifies the password for the SQL authentication username specified in BI_DATABASE_USERNAME.
BI_DATABASE_SERVER		Yes	Name of a SQL Server database instance to host the SLA-BI database. **Note** Tachyon Setup prompts for the SQL Server database instance.
BI_DATABASE_USEINTEGRATEDSECURITY	1		Specifies if integrated security is to be used to access BI database. Values are: • 0 – false • 1– true If integrated security is used, then BI will use the SLA Platform service account (specifically the **1E SLA Platform Engine** service account). **Note** Tachyon Setup uses integrated security, which means BI uses **Network Service** assuming SLA was installed by Tachyon Setup.

Property	Default	Mandatory	Description
BI_DATABASE_USERNAME		Depends	If not using integrated security, this property specifies the SQL Login of the **BI SQL user**: • a SQL login must be pre-created in the SQL instance hosting the BI database • an identical SQL login must be pre-created in the SQL database instance hosting the SLA Platform databases, if the BI database is hosted on a separate instance
COMMON_DATABASE_NAME	SLA-Shared		The name of the SLA Platform database used by BI.
SSAS_DATABASE_DROPDB	0		If set to 1 on the command-line, it drops the SLA-BI cube during installation if it exists on the specified SQL Server instance. The default behavior for this property is to not drop the existing cube. **Note** Exercise caution when using this option as any existing data will be deleted. Do not use this option if you want to preserve your existing data.
SSAS_DATABASE_NAME	SLA-BI		The name of the SLA-BI cube.
SSAS_DATABASE_PASSWORD		Yes	Password for the Windows account used by the BI API to query the cube.

Property	Default	Mandatory	Description
			Note Tachyon Setup prompts for the password of the SSAS_DATABASE_USERNAME user account.
SSAS_DATABASE_SERVER		Yes	Name of a SSAS database instance to host the SLA-BI cube. **Note** Tachyon Setup prompts for the SSAS instance.
SSAS_DATABASE_USERNAME		Yes	Username for the **BI SSAS user** domain account. This is used by the BI Multidimensional Expressions (MDX) API on the Master Stack to query the SLA-BI cube. **Note** Tachyon Setup prompts for a domain user account.

1.11.7.8 Application Migration installer properties

A table of the Windows installer properties for the Application Migration installer.

> **Warning**
>
> Tachyon Setup is the only supported method of installing, upgrading, and patching a Tachyon server.
>
> Installation using standalone **msi** or **msp** files is not supported unless advised by 1E, which may be necessary in complex installations, using non-interactive (quiet/silent) command-lines, and may require further post-install configuration steps.
>
> **Note**
>
> Mandatory properties must be provided when installing using a command-line.

The installer file is: **ApplicationMigration.msi**

Property	Default	Mandatory	Description
PLATFORMBASEURL	n/a	Yes	The URL used to access the Tachyon Portal website. You can connect either using HTTP or HTTPS. In either case, the URL will be based on the settings made on the **Website Configuration** screen of the Tachyon Setup program. Please refer to Website configuration for more details. For example, if your Tachyon server FQDN is **ACME-TCN01.ACME.LOCAL** and your Tachyon DNS alias is **TACHYON.ACME.LOCAL**, and these have been configured as the host headers on the **Website Configuration** screen of the Tachyon Setup program, then either of the following URLs can be used: • http://ACME-TCN01.ACME.LOCAL • https://TACHYON.ACME.LOCAL If you have specified a custom port on the **Website Configuration** screen of the Tachyon Setup program, then this should also be added to the URLs. For example: • http://ACME-TCN01.ACME.LOCAL:8080 • https://TACHYON.ACME.LOCAL:8443

Ensure all steps on the Requirements page have been completed before installation.

See Installation for more details about installations.

1.11.7.9 AppClarity installer properties

A table of the Windows installer properties for the AppClarity installer.

Warning

Tachyon Setup is the only supported method of installing, upgrading, and patching a Tachyon server.

Installation using standalone **msi** or **msp** files is not supported unless advised by 1E, which may be necessary in complex installations, using non-interactive (quiet/silent) command-lines, and may require further post-install configuration steps.

Note

Mandatory properties must be provided when installing using a command-line.

The installer file is: **AppClarity.msi**

Property	Default	Mandatory	Description
SLAPLATFORMURL		Yes	You can connect either using HTTP or HTTPS. In either case, the URL will be based on the settings made on the **Website Configuration** screen of the Tachyon Setup program. Please refer to Website configuration for more details. For example, if your Tachyon server FQDN is **ACME-TCN01.ACME.LOCAL** and your Tachyon DNS alias is **TACHYON.ACME.LOCAL**, and these have been configured as the host headers on the **Website Configuration** screen of the Tachyon Setup program, then either of the following URLs can be used: • http://ACME-TCN01.ACME.LOCAL • https://TACHYON.ACME.LOCAL If you have specified a custom port on the **Website Configuration** screen of the Tachyon Setup program, then this should also be added to the URLs. For example: • http://ACME-TCN01.ACME.LOCAL:8080 • https://TACHYON.ACME.LOCAL:8443 The URL used to access the Tachyon Portal. This must be set to a valid URL for Tachyon "https://Tachyon.acme.local" (https://<alias>.<domain>)

Ensure all steps on the Preparation page have been completed before installation.

See Installing and upgrading for more details about installations.

1.11.8 Tachyon Server reference

Reference information specific to Tachyon Server components of the platform.

1.11.8.1 Switch Command Lines

Details of command line parameters used by the **SwitchCommandLine** entry in the Tachyon Switch Host 's **Tachyon.Switch.Host.exe.config** file.

> **Warning**
>
> This page is for information only. Do not make configuration changes unless instructed to do so by 1E.

1.11.8.1.1 Switch Command Lines

The Tachyon Switch Host has a **Tachyon.Switch.Host.exe.config** file, which has one or more **SwitchCommandLine** keys. If there is more than one Switch then each key is uniquely numbered: **key="SwitchCommandLine.n"**

The following is an example default key.

```
<add key="SwitchCommandLine" value="-cfgName=ACME-TCNMST-SW1 -config=https://tachyon.acme.local:443/Core -NoStdOut -NoSumm -NoSw2Sw -Log=INFO" />
```

The configuration file has a single command-line for each Switch, which should not need to be updated after installation. However, there are some complex scenarios where 1E may instruct you to make some changes.

Parameters	Comment	Notes
-cfgname=<name>	Specifies which row to use in the TachyonMaster database **SwitchConfiguration** table by matching the **<name>** using the following rules: 1. If **-cfgName=<name>** is specified, then the Switch expects to find a matching name in the **SwitchConfiguration** table. The convention for **<name>=<hostname>-<switchnumber>** where Switch number is unique and starts with SW1 2. If **-cfgName=<name>** is not specified, then the Switch will use the configuration where **<name>** is the	For a Switch on a DMZ Server this will be -cfgName=ACME-TCNDMZ-SW1 if ACME-TCNDMZ is the hostname of the DMZ server.

Parameters	Comment	Notes
	hostname of the server on which the Switch is running 3. If the **SwitchConfiguration** table does not have a row matching the server's name or hostname, then the Switch will use the default * row. If there is no match then the Switch will log an error and will not start. Example -cfgName=ACME-TCNMST-SW1	
-config=<fqdn>	The fully qualified domain name (fqdn) used by the Switch to connect to the Core. For example -config=https://tachyon.acme.local:443/Core	Included in template config.
-dmz	Allows the use of the Switch on a DMZ Server that is not domain-joined and is using SAML. Not required for domain-joined DMZ Server.	
-fips	Add this parameter to force client-Switch communications to use only FIPS-compliant algorithms. Windows and .NET Framework support a range of cryptographic algorithms, collectively known as cipher suites. There are various ways you can configure operating systems to permit use of specific cipher suites and security policies, which can include or enforce the use of FIPS-compliant algorithms.	

Parameters	Comment	Notes
	Tachyon components, including Switches, use whichever algorithms you have permitted without additional configuration. To enforce use of FIPS-compliant algorithms therefore requires you to correctly configure the OS of servers and devices. Switches are an exception because they do not rely on Windows, and will negotiate the strongest algorithm an client is permitted to use, which may not be FIPS-compliant, but will always negotiate the strongest FIPS-compliant algorithm if the **-fips** parameter is used.	
-ignoreClientCerts	The Switch does not require clients to present certificates. Requires **SecurityLevel** to be set to 4 (default is 5). Instructs the Switch to ignore any client certificate presented. Tachyon clients are allowed to connect if they provide no client certificate, an invalid client certificate, or a valid client certificate.	Added by TachyonSetup if **Switches require client certificates to be presented by 1E Client** is unchecked in Client certificates screen. For a new installation, Tachyon Setup also changes the **SecurityLevel** from default 5 to 4 in the **SwitchConfiguration** table of the **TachyonMaster** database.
-log.<log area>=<logging level>	Specifies the logging level for a logging area. The default value is -log=0 (same as -log=info) which provides logging of all Switch areas at info level. The following table shows permitted logging levels.	Included in template config as -log=0

Parameters	Comment	Notes

Value	Description
Error	Only outputs errors. An error is a serious problem, typically requiring operator intervention of some sort to restore full functionality.
Warn	Outputs errors and warnings. A warning indicates a potential problem, where the system can nonetheless function without intervention.
Info	Outputs general information in addition to the errors and warnings. This is the default.
Debug	Outputs debugging information in addition to all the previous levels.
Trace	Outputs the maximum information available. Used only in exceptional circumstances as it will generate huge amounts of logging output.

Warning

Logging levels should only be changed from

Parameters	Comment	Notes
	info only if requested by 1E Support and reset to **info** after investigation is complete. 1E Support may ask you to increase or reduce specific areas of logging. The example below increases the level of logging for http, decreases metrics, and leaves other areas as normal. `-log=info -log.http=debug -log.metrics=warn`	
-NoStdOut	Prevent the Switch echo logging to stdout in addition to the Switch log file. Remove only for testing.	
-NoSumm	Prevent the Switch logging warnings about not being able to connect to the Summarizer component. If this parameter is omitted, the Switch will attempt to report to a Summarizer using the URL specified in the **SummaryUrl** value in the **SwitchConfiguration** table, and log errors if it cannot connect. The Summarizer component monitors performance and is a separately installed component, only if required.	Included in template config.
-NoSw2Sw	Disable switch-to-switch communications.	Included in template config.
-skipCrlChecks	The Switch does not attempt to retrieve certificate revocation lists. Requires **SecurityLevel** to be set to 4 (default is 5).	

Parameters	Comment	Notes
	This affects the Switch and clients, that is, the Switch does not check the CRL of its own certificate, nor those of clients. This does not impact browsers connecting to Explorer, or the internal functions of the server.	

Warning

SecurityLevel is configurable in the **SwitchConfiguration** table of the **TachyonMaster** database. Typically, each Switch will have its own row in this table, and therefore has its own configuration.

By default, **SecurityLevel** is 5, and is only changed to allow Switches to use lower security options.

Do NOT change the **SecurityLevel** unless required. ONLY change this to the value required to support the necessary Switch configuration.

1.11.8.2 Device Deduplication

Several scenarios can lead to the same device being reported more than once within Tachyon, which can find their way into Experience and other applications. The main issue is duplicates having different TachyonGuid's. TachyonGuid is the primary distinct identifier of a device, meaning that when calculating the total number of devices within the system it can easily show a count that is higher than the real world number. It also means that data associated with a device (for example, Experience performance data) will eventually be split among multiple TachyonGuids, affecting access to the device's data as well as affecting aggregations.

In most cases, deduplicating using the device FQDN should suffice, in that it is reasonable to assume that multiple devices with the same FQDN are the same device. However, this is not true in all cases - for various reasons some organizations do not use FQDN to identify a device, they may uniquely identify devices based on Make, Model and Serial Number. For this reason, the deduplication feature can be configured with one or more device attributes to uniquely identify a distinct device.

Note

The Coordinator runs a device grooming task that deletes devices from the TachyonMaster database. This deletes devices that have not connected to the platform in a set number of days (99 by default). When devices are groomed a deleted event will be sent. The *tachyonGuid* specifies the device being deleted, for delete events payload will be null.

1.11.8.2.1 Configuration

Tachyon stores its Device Deduplication configuration in:
<INSTALLDIR>\Tachyon\Coordinator\Tachyon.Server.Coordinator.exe.config

> **Note**
>
> After any changes reboot the server or restart the **1E Tachyon Coordinator** service.

The time and frequency of when the Device Deduplication process runs is changed by adding and editing the **DeviceDeduplication** setting:

```
<module assemblyName="Tachyon.Server.Coordinator" providerName="Tachyon.Server.
Coordinator.Scheduling.SchedulingModule">
  <settings>
    <add key="Crontab1" value="50 23 * * * LogDevicesSeenInTheLast7Days" />
    <add key="Crontab2" value="15 * * * * MaintainPolicyRulePartitioning" />
    <add key="Telemetry" value="40 23 * * 5 SendTelemetryStats" />
    <add key="DeviceDeduplication" value="0 1 * * 0 DeviceDeduplication {Delete
Devices:'false',UpdateDeviceData:'false',DeleteOrphanedDeviceData:'false',Devic
eIdentifier:['FQDN']}" />
  </settings>
</module>
```

The numbers that you see after **value** is a crontab schedule expression. The schedule **0 1 * * 0** means "at 01:00 hours, any day of the month, any month of the year, on weekday 0 (Sunday)". In other words, this configuration runs the Device Deduplication process at 1AM UTC every Sunday night.

You can use an online tool such as https://crontab.guru/ to verify your crontab schedule expression.

> **Warning**
>
> Please ensure there are no spaces in the **arguments** text {within the brackets}.
>
> Do not change the other crontab keys unless advised by 1E.

1.11.8.2.1.1 Modifying when Device Deduplication runs

By default, **Device Deduplication** runs at 1AM UTC every Sunday night. Another process called **Experience Synchronization** runs at 2AM UTC daily. It is very important that Experience Synchronization is not running when Device Deduplication starts, therefore if you change the time when either of these processes start, then you must ensure **Experience Synchronization** process starts **after** the **Device Deduplication** process start, and ideally there should be at least a 1 hour gap to avoid overlap. You may need a longer gap for very large systems.

1.11.8.2.2 Arguments

Running with all "Update..." and "Delete..." arguments set to false will make no database changes and is considered a diagnostic/practice run. Following a run such as this the DeviceDeduplication and DeviceDeduplicationLog tables could then be analyzed to figure out how many duplicates are in the environment based on the **DeviceIdentifier** input. This would provide a projected impact for

a subsequent run with one or more of these arguments set to true. Alternatively, the user could then also choose to modify the **DeviceIdentifier** value to include more/less/different columns that would provide a more fine tuned target of what the user expects a truly unique device to be.

Argument	Default	Usage
Instance	Instance number of last run +1	This can optionally be added to the list of parameters in the app setting. By default, the orchestration will handle this automatically. If specifying, previous instance numbers can be found in the DeviceDeduplicationLog table. A use case for specifying this is retroactive execution, see **Instance** below section for more details.
DeleteDevices	False	Delete duplicate devices from both databases, and any management group associations for those devices.
UpdateDeviceData	False	Relink TachyonExperience performance data from duplicate devices (that will be deleted) to the singular active device that will be kept.
DeleteOrphanedDeviceData	False	Remove TachyonExperience performance data that is associated with a device that no longer exists.
DeviceIdentifier	['FQDN']	This is an array of one or more **passes**, with each **pass** made up of one or more **device attributes** (column names) from the **Device** table in the **TachyonMaster** database. Please refer to Device Deduplication below for more details about using multiple passes. You can use any column from the**Device**table that is a**device attribute**, however, you should only use attributes that uniquely identify a device. Device attributes that are commonly used to uniquely identify a device are: **Fqdn**,**SMBiosGuid**, **MAC**, **SerialNumber**,**Manufacturer**, **Model**, **Domain**, **Name**,**User**, and**Location**. Some of these attributes can be used on their own, whilst others must be used in combination. You should avoid using TachyonGuid, or any of the date columns. Each pass must be wrapped in **single quotes**. Any attributes specified within a pass are create a single hash per device. When

Argument	Default	Usage
		using multiple passes, or multiple attributes within a pass, they must each be separated by a**comma**. For example: DeviceIdentifier:['SerialNumber,SMBiosGuid**',**'Manufacturer,Model,Location**',**'FQDN',] **Note** Any devices that contain identical values across all the specified attributes will be assigned the same hash. Of these devices, the one that has the most recent **LastConnUtc** value will be marked as **ToBeDeleted**=0 whilst the others will be marked as **ToBeDeleted**=1. This is how we identify duplicates as well as the single active device that we want to keep. The **CreatedUtc**that is retained for the kept device is not necessarily the earliest or the latest of all its duplicates. **Note** If the column schema of the **Device** table changes between runs, then the **DeviceDeduplication** table will have to be backed up and deleted before the next run. This will generate a new version of the table in the next run with up-to-date device columns, which also means new columns can now be specified within the **DeviceIdentifier** value.

The following table describes the system behavior for every permutation of boolean arguments passed to DeviceDeduplication:

DeleteDevices	UpdateDeviceData	DeleteOrphanedDeviceData	Device Deduplication process behavior
F	F	F	This is the default configuration (3 x False). Before you change these settings, you should run a diagnostic/practice run where no changes will be made to the devices or their data. Check

DeleteDevices	UpdateDeviceData	DeleteOrphanedDeviceData	Device Deduplication process behavior
			DeviceDeduplication and **DeviceDeduplicationLog** table for results analysis.
T	F	F	Delete devices identified as duplicates, do not update or merge any existing performance data.
F	T	F	Do not delete devices identified as duplicates, reassign duplicate devices performance data to the single device that has been identified as the most recent instance of the device. ***1***
F	F	T	Do not delete devices identified as duplicates, do not update or merge any existing performance data. Delete any performance data that is associated with a TachyonGuid that no longer exists in the TachyonMaster Device table. This might be useful as a database cleanup exercise to remove "unparented data". ***1 2***
T	T	F	Delete devices identified as duplicates and merge any existing performance data that was associated with duplicates.
F	T	T	Do not delete devices identified as duplicates, reassign duplicate devices performance data to the

DeleteDevices	UpdateDeviceData	DeleteOrphanedDeviceData	Device Deduplication process behavior
			single device that has been identified as the most recent instance of the device. Finally, after relinking the data, delete any performance data that is associated with a TachyonGuid that no longer exists in the TachyonMaster Device table. ***1***
T	F	T	Delete devices identified as duplicates, do not update or merge any existing performance data. Delete any performance data that is associated with a TachyonGuid that no longer exists in the TachyonMaster Device table. ***2***
T	T	T	Delete devices identified as duplicates, reassign duplicate devices performance data to the single device that has been identified as the most recent instance of the device. Finally, after relinking the data, delete any performance data that is associated with a TachyonGuid that no longer exists in the TachyonMaster device table.

1 *- This could lead to continued inflated device counts in the system*

2 *- Be careful as this data will be deleted and cannot be recovered or merged at a later date even if the Tachyo nGuid that reported it comes online again.*

1.11.8.2.2.1 Instance

Each run of Device Deduplication will result in entries in the **DeviceDeduplicationLog** table. All rows for the run will be assigned an instance number. The Instance number is also used to be able to share context between the TachyonMaster and TachyonExperience parts of the process.

Retroactive execution: An old instance can also be passed to the process via the app setting. When an old instance is provided duplicates will not be recalculated, instead the list of devices from that previous run will be used (from the **DeviceDeduplication** table). This will also be logged in the **DeviceDeduplicationLog** table, an entry that reads "This is a rerun of a previous instance. Previous history from the DeviceDeduplication table will be used for this instance". In an execution such as this any new value for **DeviceIdentifier** will be ignored however all other new arguments will be applied.

1.11.8.2.2.2 Multiple Passes of Deduplication

The DeviceIdentifier argument is a comma separated list of passes, each pass itself being a comma separated list of device attributes. The order of specified passes is adhered to for Device Deduplication. Each pass further refines duplicate devices against the **results of the previous pass**. There is no limit to the number of passes specified.

For example, the passes listed in the table below would be run if the DeviceIdentifier is set to *`DeviceIdentifier:['SerialNumber,SMBiosGuid','Manufacturer,Model,Location','FQDN',]:`*

Pass number	Device attributes used	Identify duplicates based on...
1	SerialNumber SmBiosGuid	Devices in the TachyonMaster Device table that have the same SerialNumber AND SMBiosGuid.
2	Manufacturer Model Location	Devices identified as duplicates in pass 1 that also have the same Manufacturer, Model and Location.
3	FQDN	Devices identified as duplicates in pass 2 that also have the same FQDN.

The results of pass 3 alone are then used for the rest of the process and considered duplicates going forward.

1.11.8.2.3 Experience Synchronization

If any of the Boolean arguments are set to true, Device Deduplication may affect existing data in the system, whether through relinking to a new TachyonGuid or removing as orphaned data. For this reason, when the Device Deduplication process completes (with any settings set to true), it triggers a **full** Experience Synchronization. By default, the regular Experience Synchronization process is **incremental**, and runs at 2AM UTC daily.

The **full** Experience Synchronization includes a **full process** of the TachyonExperience aggregated data, which is initiated regardless of the current ProcessMode option specified (GlobalSetting table in the TachyonExperience database). A **full process** is required because data which typically Tachyon handles as additive can have historical data modified by the DeviceDeduplication process, which could otherwise lead to inaccurate counts and aggregations.

For large environments the **full process** of the aggregable data is likely to be a long running background process, it will not impact data displayed in the UI until it has completed. If it conflicts with an ongoing Experience Synchronization process it will be skipped. Server resource demand is likely to increase during an aggregation process. Be aware that depending on the resources available, this could affect the query response time of the UI.

The latest Accumulated Hotfix for Tachyon Platform Server allows you to add the **ExperienceSync** setting to the Coordinator configuration file. You do not need to add or modify this unless advised by 1E.

```
<module assemblyName="Tachyon.Server.Coordinator" providerName="Tachyon.Server.
Coordinator.Scheduling.SchedulingModule">
  <settings>
    <add key="Crontab1" value="50 23 * * * LogDevicesSeenInTheLast7Days" />
    <add key="Crontab2" value="15 * * * * MaintainPolicyRulePartitioning" />
    <add key="Telemetry" value="40 23 * * 5 SendTelemetryStats" />
    <add key="DeviceDeduplication" value="0 1 * * 0 DeviceDeduplication {Delete
Devices:'false',UpdateDeviceData:'false',DeleteOrphanedDeviceData:'false',Devic
eIdentifier:['FQDN']}" />
    <add key="ExperienceSync" value="0 2 * * * ExperienceSynchronization" />
  </settings>
</module>
```

The numbers that you see after **value** is a crontab schedule expression. The schedule **0 2 * * *** means "at 02:00 hours, any day of the month, any month of the year, any day". In other words, this configuration runs the Experience Synchronization process at 2AM UTC daily.

You can use an online tool such as https://crontab.guru/ to verify your crontab schedule expression.

1.11.8.2.4 Logging and analysing results

The Device Deduplication process creates logs in the **Tachyon.Coordinator.log** file.

The **DeviceDeduplicationLog** table - in the TachyonMaster database - logs more granular detail including the arguments used for the instance, details of each pass if more than one is specified, numbers of duplicates found, as well as rows affected in specific tables by various actions.

The **DeviceDeduplication** table - in the TachyonMaster database - stores a list of devices to be kept and their duplicates for the instance. The **ToBeDeleted** column is either 0 (false) for a device to be kept, and 1 (true) for a duplicate to be deleted. Kept and duplicate devices are associated by the **Hash** column.

With all arguments set to **false** you can review whether the specified **DeviceIdentifier** is able to uniquely identify devices and genuine duplicates. Once you are sure the **DeviceIdentifer** is suitable, you can then change other arguments from **false** to **true** according to your needs.

When the **DeleteDevices** argument is set to true, the **Device** table is updated for each device where older duplicates of it have been identified. Each device will have a timestamp set for **LastDeduplicationUtc** column, as well as an Experience event logged. The timestamp is updated when one or more new duplicates are found. There is also a **DeduplicationCount** column which represents the number of complete Device Deduplication

processes where a device has been found to have duplicates. These values will only be set on the device identified as being the most recent device that will be kept, not it s duplicates.

Devices with a **LastDeduplicationUtc** value can be found using the below SQL query.

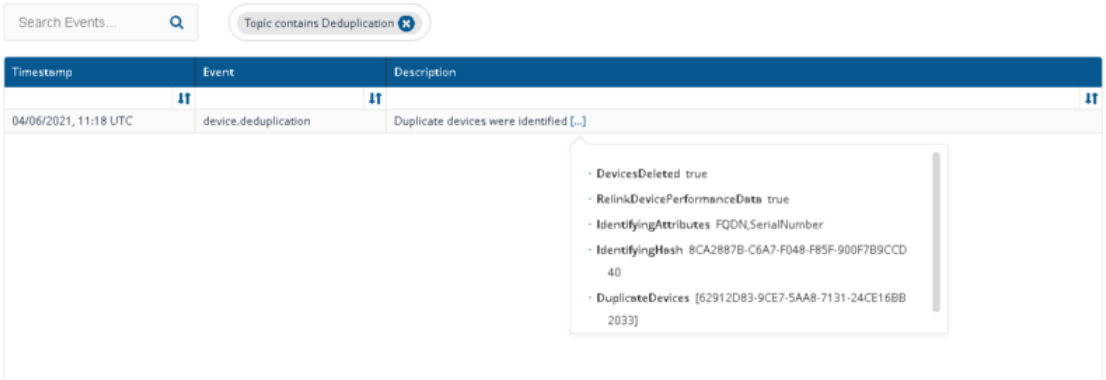
Genuine devices that have had duplicates identified

```
SELECT * FROM [TachyonMaster].[dbo].[Device] WHERE LastDeduplicationUtc IS NOT NULL and DeduplicationCount IS NOT NULL
```

The Experience event can be viewed within Experience (Devices → {Select a device} → Logs).

The details of the log will show what attributes were used when it was identified as having duplicates, if multiple passes were specified they will be delimited with a '#' in the order of execution. The **IdentifyingHash** value can be used to query the **DeviceDeduplication** table **Hash** column, in the TachyonMaster database.

This will provide all device details of the device itself as well as all of it's duplicate devices.



1.11.8.3 Roles and Securables

1.11.8.3.1 System roles

On the Roles page, a system role is indicated by an icon with a padlock

System roles are built-in and are not configurable, however, they can be assigned to users the same as any other role. The following table lists the built-in system roles.

Tachyon system role	Permissions	Allows delegation	Description	Notes
All Instructions Actioner	• InstructionSet (Actioner) for **All Instruction Sets**	Yes	Use Tachyon Explorer, execute any Instruction (Action and Question), and view	Renamed in 8.0 - was **Global Actioners**.

Tachyon system role	Permissions	Allows delegation	Description	Notes
			any Instruction response	
All Instructions Approver	• InstructionSet (Approver) for **All Instruction Sets**	Yes	Use Tachyon Explorer, approve any Instruction for anyone other than self	Renamed in 8.0 - was **Global Approvers**. If email is enabled, this role will receive an approval request email for each requested action instruction.
All Instructions Questioner	• InstructionSet (Questioner) for **All Instruction Sets**	Yes	Use Tachyon Explorer, ask any Question and view any Instruction response	Renamed in 8.0 - was **Global Questioners**.
All Instructions Viewer	• InstructionSet (Viewer) for **All Instruction Sets**	Yes	Use Tachyon Explorer, view any Instruction response	Renamed in 8.0 - was **Global Viewers**.
Full Administrator	• All	No	Has all the permissions available in the Platform and its Applications	Renamed in 8.0 - was **Global Administrators**.

Tachyon system role	Permissions	Allows delegation	Description	Notes
Group Administrator	• CustomProperty (Read) • ManagementGroup (Read, Write, Synchronize, Delete) • Security (Read, Write, Delete) • Repository.Inventory (Read, EvaluateManagementGroup)	Yes	Add Users and Management Groups, and manage their roles and assignments, below this Group Administrator's assigned Management Group(s)	**New role in 8.0** This role is similar to previous **Management Group Administrators** role, with permissions extended to support using Management Groups for RBAC, however the role is only allowed to manage Management Groups below the Management Groups they have been assigned to.
Guaranteed State Administrator	• GuaranteedState (Read,Write,Delete) • PolicyAssignment (Assign) • PolicyDeployment (Execute)	No	Use Guaranteed State, manage Rules and Polices, and assign and deploy Policies	Renamed in 8.0 - was **Guaranteed State Administrators**.
Guaranteed State Policy Assigner	• PolicyAssignment (Assign)	Yes	Assign Policies to Management Groups (does not allow use of Guaranteed State)	**New role in 8.0**

Tachyon system role	Permissions	Allows delegation	Description	Notes
Guaranteed State User	• GuaranteedState (Read)	No	Use Guaranteed State, view dashboards	Renamed in 8.0 - was **Guaranteed State Viewers**.
Installer	• Application (Write, Delete) • Consumer (Read, Write) • CustomProperty (Read) • EventSubscription (Read, Write, Delete) • Infrastructure (Read) • InfrastructureLog (Read) • InstructionSetManagement (Delete, Add, Read) • ManagementGroup (Read) • Security (Read, Write, Delete)	No	Install and upgrade the Platform and Applications, register Consumers, upload Product Packs, manage Instruction Sets, and configure Roles and Permissions	**New role in 8.0**
Inventory Administrator	• Component (Read, Write) • Connector (Read, Write, Delete, Execute) • CustomProperty (Read, Write)	No	Manage Inventory repositories - populate and archive them - export data - manage Inventory	Renamed in 8.0 - was **Inventory Administrators**.

Tachyon system role	Permissions	Allows delegation	Description	Notes
	• Inventory (Read, Export) • Inventory.Association (Read, Write, Delete, Export) • ManagementGroup (Read, Write, Synchronize, Delete) • ProcessLog (Read) • ProviderOperationLog (Read) • Repository.Inventory (Archive, Delete, EvaluateManagementGroups, Populate, Read, Write) • Schedule (Read, Delete, Write) • SynchronizationLog (Read)		associations	
Inventory User	• Inventory (Read, Export) • Inventory.Association (Read) • Repository.Inventory (Read)	No	View Inventory repositories, data and Inventory associations	Renamed in 8.0 - was **Inventory Viewers**.
Tachyon System	• Component (Read) • Connector (Execute) • Consumer (Read)	No	For service and equivalent accounts to perform Tachyon	**New role in 8.0**

Tachyon system role	Permissions	Allows delegation	Description	Notes
	• EngagementAssignment (Assign) • Engagements (Read, Write, Delete, Execute) • InstructionSetManagement (Read) • ManagementGroup (Read, Synchronize) • OffloadingData (Offload) • PolicyDeployment (Execute) • ProcessLog (Read) • ProviderOperationLog (Read) • Repository.Inventory (Read, EvaluateManagementGroups) • Security (Read)		system operations	

Questions, responses, actions are examples of securables. Other Consumers may create their own system roles and securables.

Note

When upgrading from Tachyon Platform 5.2 or earlier, roles names are automatically renamed as listed above. Other roles are deleted during the upgrade, unless they have members.

Click here to expand and see details of changes made by upgrading to this latest version of Tachyon Platfrom...

The upgrade process makes the following changes:

1. New roles are created, if they do not exist already:

New system roles

- Group Administrator
- Guaranteed State Policy Assigner
- Installer
- Tachyon System

New Custom roles

- Experience Administrator
- Experience Engagement Assigner
- Patch Success Administrator

2. The Tachyon user doing the upgrade is automatically assigned to the **Installer** role. The user is also *unassigned* from the following roles, if assigned before the upgrade:

   - Applications Administrators
   - Consumer Administrators
   - Event Subscription Administrators
   - Instruction Set Administrators
   - Permissions Administrators

3. Tachyon users associated with the NT AUTHORITY/NETWORK SERVICE and machine accounts, are assigned to the **Tachyon System** role. These users will also be *unassigned* from the following roles, if assigned before the upgrade:

   - Applications Administrators
   - Consumer Viewers
   - Engagement Administrator
   - Management Group Sync Initiators
   - Offloaders
   - Permissions Viewers
   - Survey Administrators

4. Several old roles are renamed
   a. Some are renamed from plural to singular, for example if the **Nomad Administrators**role exists it is renamed to**Nomad Administrator**
   b. An exception is in the unlikely event that the **Nomad Admins** role exists, it is renamed to **Nomad Administrator** unless that role already exists, in which case it is renamed to **Nomad Administrators** instead

c. **Global Questioner**, **Global Actioner**, **Global Viewer**, and **Global Approver** roles have been renamed with **Global...** replaced by **All instructions...**

d. **Inventory Viewers**, **Experience Viewers**, **Patch Success Viewers**, have been renamed with **...Viewers** changed to **...User**

System roles renamed from

- Global Actioners
- Global Administrators
- Global Approvers
- Global Questioners
- Global Viewers
- Guaranteed State Administrators
- Guaranteed State Viewers
- Inventory Administrators
- Inventory Viewers
- Survey Administrators
- Survey Viewers

System roles renamed to

- All Instructions Actioner
- Full Administrator
- All Instructions Approver
- All Instructions Questioner
- All Instructions Viewer
- Guaranteed State Administrator
- Guaranteed State User
- Inventory Administrator
- Inventory User
- Experience Engagement Administrator *
- Experience Engagement Viewer *

Note

* These roles are retired, and will only be kept if a user or group is assigned to it.

Custom roles renamed from

- AppClarity Administrators
- Application Migration Administrators

Custom roles renamed to

- AppClarity Administrator
- Application Migration Administrator
- Compliance Administrator

- Compliance Administrators
- Compliance Viewers
- Entitlement Administrators
- Experience Viewers
- Nomad Administrators
- Patch Success Viewers
- Reclaim Administrators
- Reclaim Viewers
- Compliance Viewer
- Entitlement Administrator
- Experience Viewer
- Nomad Administrator
- Patch Success User
- Reclaim Administrator
- Reclaim Viewer

5. Other system and custom roles are deleted. A role is kept only if it is **(a)** on the list of roles to be kept, or **(b)** the role has a user or group assigned to it

System roles that are kept

- All Instructions Actioner
- All Instructions Approver
- All Instructions Questioner
- All Instructions Viewer
- Full Administrator
- Group Administrator
- Guaranteed State Administrator
- Guaranteed State Policy Assigner
- Guaranteed State User
- Installer

System roles that have been retired

- 1E Client Deployment Administrators
- 1E Client Installer Administrators
- Applications Administrators
- Component Administrators
- Connector Administrators
- Consumer Administrators
- Consumer Viewers
- Custom Properties Administrators
- Event Subscription Administrators
- Event Subscription Viewers
- Infrastructure Administrators
- Instruction Set Administrators
- Log Viewers

- Inventory Administrator
- Inventory User
- Tachyon System

Custom roles that are kept

- 1E ITSM Connect Actioner
- AppClarity Administrator
- Application Migration Administrator
- Compliance Administrator
- Compliance Viewer
- Entitlement Administrator
- Experience Administrator
- Experience Engagement Assigner
- Experience User
- Nomad Administrator
- Patch Success Administrator
- Patch Success User
- Reclaim Administrator
- Reclaim Viewer
- Management Group Administrators
- Management Group Sync Initiators
- Offloaders
- Permissions Administrators
- Permissions Viewers
- Policy Administrators
- Provider Configuration Administrators
- Schedule Administrators
- Survey Administrators (Experience Engagement Administrator)
- Survey Viewers (Experience Engagement Viewer)
- VDI Administrators

Custom roles that have been retired

- Any custom role created by Tachyon administrators

Tip

A retired role is kept if it has a user or group assigned to it.

The following roles are retired (deleted) during an upgrade.

Retired Tachyon system role	Permissions	Notes
1E Client Deployment	• AgentDeployment (Execute, View, Approve)	Use **Full Administrator** role instead.

Retired Tachyon system role	Permissions	Notes
Administrators		
1E Client Installer Administrators	• AgentInstallerManagement (Add, Delete, Read)	Use **Full Administrator** role instead.
Applications Administrators	• Application (Write, Delete)	Use **Full Administrator** role instead.
Component Administrators	• Component (Read, Write)	Use **Inventory Administrator** role instead.
Connector Administrators	• Connector (Read, Write, Delete) • ProcessLog (Read) • ProviderOperationLog (Read)	Use **Inventory Administrator** role instead.
Consumer Administrators	• Consumer (Read, Write)	Use **Full Administrator** role instead.
Consumer Viewers	• Consumer (Read)	Create a custom role if required.
Custom Properties Administrators	• CustomProperty (Read, Write)	Use **Full Administrator** role instead.
Event Subscription Administrators	• EventSubscription (Read, Write, Delete)	Use **Full Administrator** role instead.

Retired Tachyon system role	Permissions	Notes
Event Subscription Viewers	• EventSubscription (Read)	Use **Full Administrator** role instead.
Experience Engagement Administrators	• Consumer (Read) • Engagements (Read, Write, Delete, Execute) • EventSubscription (Read, Write, Delete) • ManagementGroup (Read) • PolicyDeployment (Execute)	If this role is retained during an upgrade, it will have been renamed from **Survey Administrators**.
Experience Engagement Viewers	• Engagements (Read) • EventSubscription (Read)	If this role is retained during an upgrade, it will have been renamed from **Survey Viewers**.
Infrastructure Administrators	• Infrastructure (Read, Write, Delete)	Use **Full Administrator** role instead.
Instruction Set Administrators	• InstructionSetManagement (Delete, Add, Read)	Use **Full Administrator** role instead.
Log Viewers	• InfrastructureLog (Read) • ProcessLog (Read) • ProviderOperationLog (Read) • SynchronizationLog (Read)	Create a custom role if required.

Retired Tachyon system role	Permissions	Notes
Management Group Administrators	• ManagementGroup (Read, Write, Synchronize, Delete) • Repository.Inventory (Read, EvaluateManagement Groups)	Use **Full Administrator** or **Group Administrator** role instead.
Management Group Sync Initiators	• ManagementGroup (Read, Synchronize) • ProcessLog (Read) • ProviderOperationLog (Read) • Repository.Inventory (Read, EvaluateManagement Groups)	Not required for users. It is only needed for system accounts and replaced by the **Tachyon System** role.
Offloaders	• OffloadingData (Offload)	Not required for users. It is only needed for system accounts and replaced by the **Tachyon System** role.
Permissions Administrators	• InfrastructureLog (Read) • InstructionSetManagement (Read) • ManagementGroup (Read) • Security (Read, Write, Delete)	Use **Full Administrator** or Group Administrator role instead.
Permissions Viewers	• InstructionSetManagement (Read) • ManagementGroup (Read) • Security (Read)	Create a custom role if required.

Retired Tachyon system role	Permissions	Notes
Policy Administrators	• Consumer (Read) • PolicyDeployment (Execute)	Use **Guaranteed State Administrator** roles instead.
Provider Configuration Administrators	• ProviderConfiguration (Read, Write, Delete)	Use **Full Administrator** role instead.
Schedule Administrators	• Connector (Execute) • ProcessLog (Read) • ProviderOperationLog (Read) • Repository.* (All) • Schedule (Read, Write, Delete)	Use one or more of the following roles depending which repositories you need to use: • **Inventory Administrator** (system) • **AppClarity Administrator** (custom) • **Compliance Administrator** (custom) • **Entitlement Administrator** (custom) • **Reclaim Administrator** (custom)
VDI Administrators	• EventSubscription (Read, Write) • ManagementGroup (Read) • VDI (Read, Write)	Use the **Experience Administrator** custom role instead.

1.11.8.3.2 Custom roles

On the Roles page, a custom role is indicated by an icon with a cogwheel

The following table lists built-in custom roles used by Tachyon Applications.

Tachyon custom role	Permissions	Allows delegation	Description	Notes
1E ITSM Connect Actioner	• InstructionSet (Actioner) on the instruction sets you wish to allow ServiceNow to use	Yes	The ServiceNow proxy user is added to this role instead of All Instructions Actioner so that ServiceNow users can only use instructions belonging to instruction sets assigned to this role	The ServiceNow proxy user is added to this role instead of **All Instructions Actioner** so that ServiceNow users can only use instructions belonging to instruction sets assigned to this role.
AppClarity Administrator	• AppClarity.Compliance (Read, Write, Export, Delete, Execute) • AppClarity.Entitlement (Read, Write, Export, Delete, Execute) • AppClarity.Reclaim (Read, Write, Export, Delete, Execute) • Connector (Execute) • Inventory (Read, Export)	No	Create, update, delete and view AppClarity Compliance, Entitlement, License Demand and Reclaim - view and export Inventory - view, edit,	Renamed in 8.0 - was **AppClarity Administrators**.

Tachyon custom role	Permissions	Allows delegation	Description	Notes
	• Inventory.Association (Read, Write, Export, Delete) • ProcessLog (Read) • ProviderOperationLog (Read) • Repository.Compliance (Read, Write, Delete, Archive, Populate) • Repository.Entitlement (Read, Write, Delete, Archive, Populate) • Repository.Inventory (Read) • Schedule (Read, Write, Delete)		delete and export Associations	
Application Migration Administrator	• Connector (Execute) • Inventory (Read) • Inventory.Association (Read,Write,Delete) • ProcessLog (Read) • ProviderConfiguration (Read) • ProviderOperationLog (Read) • Repository.ApplicationMigration (Read,Write,Delete,Archive,Populate) • Repository.Inventory (Read,Write,Populate,EvaluateManagementGroups)	No	Create, update, delete and view Application Migration Rules and Role Based Application Sets to manage installations in your estate during operating system deployment	Renamed in 8.0 - was **Application Migration Administrators**.

Tachyon custom role	Permissions	Allows delegation	Description	Notes
Compliance Administrator	• AppClarity.Compliance (Read, Write, Export, Delete, Execute) • AppClarity.Entitlement (Read, Write, Export, Delete, Execute) • AppClarity.Reclaim (Read) • Connector (Execute) • Inventory (Read, Export) • Inventory.Association (Read, Write, Export, Delete) • ProcessLog (Read) • ProviderOperationLog (Read) • Repository.Compliance (Read, Write, Delete, Archive, Populate) • Repository.Entitlement (Read, Write, Delete, Archive, Populate) • Repository.Inventory (Read) • Schedule (Read, Write, Delete)	No	Create, update, delete and view AppClarity Compliance, Entitlement and License Demand - view AppClarity Reclaim - view and export Inventory - view, edit, delete and export Associations	Renamed in 8.0 - was **Compliance Administrators**.
Compliance Viewer	• AppClarity.Compliance (Read) • AppClarity.Entitlement (Read) • ProviderOperationLog (Read)	No	View AppClarity Compliance, Entitlement and License Demand	Renamed in 8.0 - was **Compliance Viewers**.

Tachyon custom role	Permissions	Allows delegation	Description	Notes
Entitlement Administrator	• AppClarity.Entitlement (Read, Write, Export, Delete, Execute) • Connector (Execute) • Inventory (Read, Export) • Inventory.Association (Read, Write, Export, Delete) • ProcessLog (Read) • ProviderOperationLog (Read) • Repository.Compliance (Read) • Repository.Entitlement (Read, Write, Delete, Archive, Populate) • Repository.Inventory (Read) • Schedule (Read, Write, Delete)	No	Create, update, delete and view AppClarity Entitlement - view and export Inventory - view, edit, delete and export Associations	Renamed in 8.0 - was **Entitlement Administrators**.
Experience Administrator	• Consumer (Read) • EngagementAssignment (Assign) - **new** • Engagements (Read, Write, Delete, Execute) • EventSubscription (Delete, Read, Write) • Experience (Read) - **new** • ManagementGroup (Read) • PolicyDeployment (Execute) • VDI (Read, Write)	No	Use Experience, manage, assign and deploy Engagements (Surveys and Announcements), and manage Metrics	**New role in 8.0** Effectively a combination of previous **Survey Administrators** and **VDI Administrators** roles.

Tachyon custom role	Permissions	Allows delegation	Description	Notes
Experience Engagement Assigner	• EngagementAssignment (Assign)	Yes	Assign Engagements to Management Groups (does not allow use of Experience)	**New role in 8.0**
Experience User	• Engagements (Read) • EventSubscription (Read) • Experience (Read)	No	Use Experience, view Survey responses, and view Metrics	Renamed in 8.0 - was **Experience Viewers**.
Nomad Administrator	• GuaranteedState (Read) • InstructionSet (Actioner) for the **1E Nomad** instruction set on **All Devices** • Nomad (Read, Write, Delete)	No	Use Content Distribution, manage Pre-cache jobs, view the results of related Instructions and Client health policies	Renamed in 8.0 - was **Nomad Administrators**. Instruction set assigned manually after installation.
Patch Success Administrator	• Consumer (Read) • InstructionSet (Actioner) for the **1E Patch Success** instruction set on **All Devices**	No	Use Patch Success, manage and populate	**New role in 8.0** Instruction set assigned manually after installation.

Tachyon custom role	Permissions	Allows delegation	Description	Notes
	• Repository.BI (Read, Populate) • Repository.Patch (Read)		its Repository, and deploy Policies, use Explorerto deploy patches	
Patch Success User	• Consumer (Read) • InstructionSet (Questioner) for the **1E Patch Success** instruction set on **All Devices** • Repository.Patch (Read)	No	Use Patch Success, and use Explorer to ask about Patch status on devices	Renamed in 8.0 - was **Patch Success Viewers**. Instruction set assigned manually after installation.
Reclaim Administrator	• AppClarity.Reclaim (Read, Write, Export, Delete, Execute) • Connector (Execute) • Inventory (Read, Export) • Inventory.Association (Read, Write, Export, Delete) • ProcessLog (Read) • ProviderOperationLog (Read) • Repository.Compliance (Read, Populate) • Repository.Inventory (Read) • Schedule (Read, Write, Delete)	No	Create, update, delete and view AppClarity Reclaim - view and export Inventory - view, edit, delete and export Associations	Renamed in 8.0 - was **Reclaim Administrators**.

Tachyon custom role	Permissions	Allows delegation	Description	Notes
Reclaim Viewer	• AppClarity.Reclaim (Read) • ProviderOperationLog (Read)	No	View AppClarity Reclaim	Renamed in 8.0 - was **Reclaim Viewers**.

1.11.8.3.3 Securables and operations

In the SDK documentation, Securables are also known as Securable Types.

A Permission is one or more Operations for a Securable. The remit for a Securable is either Localized or Global. A Role that has only Localized permissions can be delegated.

Securable	Operations	Remit	Description
AgentDeployment	Approve, Execute, View	Global	View, create, and cancel 1E Client deployment jobs
AgentInstallerManagement	Add, Delete, Read	Global	View, upload, and delete 1E Client installers
AppClarity.Compliance	Delete, Execute, Export, Read, Write	Global	View, create, edit, delete, export, and manage AppClarity Compliance and LDC
AppClarity.Entitlement	Delete, Execute, Export, Read, Write	Global	View, create, edit, delete, export, and manage AppClarity Entitlement
AppClarity.Reclaim	Delete, Execute, Export, Read, Write	Global	View, create, edit, delete, export, and manage AppClarity Reclaim
Application	Delete, Write	Global	Install and uninstall Portal applications

Securable	Operations	Remit	Description
Component	Read, Write	Global	View and configure Components
Connector	Delete, Execute, Read, Write	Global	View, create, edit, delete, and test Connectors
Consumer	Read, Write	Global	View, add, edit, and delete Consumers
CustomProperty	Read, Write	Global	View, add, edit, and delete Custom properties
EngagementAssignment	Assign	Localized	Assign Engagements (Surveys and Announcements) to Management Groups
Engagements	Delete, Execute, Read, Write	Global	View, create, edit, delete, and enable Engagements (Surveys and Announcements) - this securable has been renamed in version 8.0 from **Surveys**
EventSubscription	Delete, Read, Write	Localized	View, create, edit, and delete the configurations of event subscriptions
Experience	Read	Global	View Experience dashboards
GuaranteedState	Delete, Read, Write	Global	View, add, edit, and delete Rules, Fragments, Trigger templates, and

Securable	Operations	Remit	Description
			Policies - view Guaranteed State dashboards
Infrastructure	Delete, Read, Write	Global	View System health and System information - view, add, and edit global settings
InfrastructureLog	Read	Global	View Infrastructure log
InstructionSet	Actioner, Approver, Questioner, Viewer	Localized	Execute, schedule, cancel, and approve instructions - view responses
InstructionSetManagement	Add, Delete, Read	Global	Upload Product Pack-add, modify, and delete instruction sets - delete instruction definitions
Inventory	Export, Read	Global	View Inventory dashboards and export inventory data
Inventory.Association	Delete, Export, Read, Write	Global	View, create, edit, and delete SCCM Associations in Inventory
ManagementGroup	Delete, Read, Synchronize, Write	Localized	Create, delete, edit, and initiate synchronization of Management Groups
Nomad	Delete, Read, Write	Global	View Content Distributiondashboar

Securable	Operations	Remit	Description
			ds and SSD peer data. View, add, and delete pre-cache jobs. Pause and resume download activity of Content Distribution clients
OffloadingData	Offload	Global	Offload (forward) event data to any Web API responsible for processing that data
PolicyAssignment	Assign	Localized	AssignGuaranteed State policies to Management Groups
PolicyDeployment	Execute	Global	Deploy all types of policies (including metrics, events, and engagements) except for Reclaim policies
ProcessLog	Delete, Read, Write	Global	View and purge the Process log, Cancel all actions
Protect	Read, Write	Global	View and deploy patches at all endpoints
ProviderConfiguration	Delete, Read, Write	Global	View, create, edit, and delete Providers
ProviderOperationLog	Read	Global	Update, delete and view provider configurations
Repository.ApplicationMigration	Archive, Delete, EvaluateManagementGrou	Global	

Securable	Operations	Remit	Description
	ps, Execute, Populate, Read, Write		
Repository.BI	Populate, Read	Global	View and populate the BI respository
Repository.Compliance	Archive, Delete, Populate, Read, Write	Global	
Repository.Entitlement	Archive, Delete, Populate, Read, Write	Global	
Repository.Inventory	Archive, Delete, EvaluateManagementGroups, Populate, Read, Write	Global	View, create, edit, and delete Inventory repositories - populate and archive them
Repository.Patch	Read	Global	View Patch Success dashboards
Schedule	Delete, Read, Write	Global	View, create, edit, and delete Schedules - view Schedule history
Security	Delete, Read, Write	Localized	Add and remove Users - view all Roles - add, modify, and delete Custom roles - assign roles to users - view Audit information log
SynchronizationLog	Read	Global	View Sync log
VDI	Read, Write	Global	View, create, edit, and delete application servers

1.11.9 Client reference

Reference information for Tachyon features of the 1E Client.

Please refer to:

- Introducing 1E Client for more information about other client features and modules, and deploying the 1E Client
- /document/preview/736743#UUID-33c212b3-863e-21bc-bc5d-52e41a0492b3 for information about the SCALE and writing your own instruction using TIMS.

1.11.9.1 1E Client command-line parameters

For a full reference of Command-line interface (CLI) parameters available to the 1E Client executable, refer to 1E Client command-line parameters.

1.11.9.2 Tachyon client settings

For a full reference of installer properties and configuration file settings for the Tachyon client features of the 1E Client, refer to Tachyon client settings.

These settings are common to Windows and non-Windows platforms.

1.11.10 Settings reference

Reference information specific to the Settings application.

1.11.10.1 Naming conventions

Suggested naming conventions for connectors, repositories, schedules, and management groups.

Tachyon and its applications create a number of default objects, therefore useful names will help differentiate them. Naming conventions will make it easier for you to see what you are working on in various places in the user interface, especially in drop-down menus where you might not see descriptions.

Scope describes where data is coming from or what it's being used for. For example Demo, Test, Lab, Q2 Audit.

Object	Convention	Reason	Examples
Connector name	<connector type> <scope> <RCR>	Naming a connector with **connector type** first causes them to be grouped together in lists. This helps when creating an action or schedule and selecting a connector. In fact, when creating an action or schedule, it is **actions types** which are listed, but their names include the **connector name**. For example, if the	SCCM Demo SCCM with RCR File upload Uploads folder

Object	Convention	Reason	Examples
		connector name is **SCCM Demo** then the resulting action type is **Sync Data - SCCM Demo**. Note the drop-down list of **actions types** shows only the **connector types** relevant to the **repository type**. Including the **scope** in the name helps to identify the data source. Include **RCR** in the name if you have enabled **Run Consolidation Reports**.	
Repository name	<scope> <repository type>	Naming with **scope** first makes it easier to know which repository you are using. The name of the **repository** you are currently using is visible in a drop-down list at the top of pages in the user interface. Including the **repository type** in the name helps when creating an action or schedule.	Demo Inventory Default Inventory
Schedule name	<action type> <repository name> <schedule>	A schedule is used to sync data or generate a report, using a specified **action type** for a specified **repository** on a specified **schedule**. The names of **action types** have two parts, for example **Sync Data - SCCM Demo** and **Generate Report - Basic Inventory Consolidation**, in which case you would only use the second part in the schedule name. Naming with **action type** first causes the same types of action to be grouped together so you can more easily	SCCM Demo Inventory 11pm *(only need to say Demo once)* SCCM Demo Default Inventory 3am *(demo connector but default in ventory)* SCCM with RCR Default Inventory Friday 2am

Object	Convention	Reason	Examples
		identify if there would be any contention between them. Typically, the **scope** will be the same for your **action type** and **repository name** therefore you can omit the repeated scope name.	
Management groups	<type> <rule summary>	**Type** helps by listing similar types together, for example, role, location, business unit, region, etc. **Rule summary** is some text that summarizes the rules used to define group membership. You can be more specific in the group description.	Region EMEA workstations City Paris datacenter servers Role Exec laptops BU Finance workstations

1.11.10.2 Server telemetry data

Details of 1E product usage statistics gathered by Tachyon to help with 1E's continued product improvement initiative.

1.11.10.2.1 What data is collected?

At a high level, the following data is collected:

- Instruction usage (by Instruction Definition and by day), and statistics on the type of resources attached to Instruction Definitions
- 1E Client configuration details, versions, operating system variants, device types, age of installation, last connected time and status, and time zones
- Registered Portal applications and Consumers
- Database table sizes
- Tachyon server component information and basic configuration
- (Anonymized) Management Group information (number of devices)
- Tachyon upgrade history

Tachyon will periodically send summarized, statistical information about usage of the product to 1E. This enables 1E to improve your experience with Tachyon as it helps us understand how features are being used, focus future development, ensure we continue to support the Operating Systems you currently use, spot early warning signs of potential issues and identify instructions

that may be causing issues or could be improved. No personally identifiable data is collected. The data is compressed, encrypted and sent to 1E through email.

> **Note**
>
> By default, Tachyon collects data continuously and sends a **compressed** and **encrypted** summary by email to 1E **every Friday at 23:40 UTC**.

Configuration

For on-premises installations of Tachyon platform, customers have the option to configure the frequency this data is sent to 1E. This option is not available for customers using SaaS versions of the platform, SaaS customers should contact their 1E Account Team.

1.11.10.2.2 Metrics

The following tables list all the telemetry metrics. Numeric values are integers unless otherwise stated.

Application

Instance format	ApplicationName
Example instance	`Explorer`
Value format	Version number
Example value	*`5.1.0.20`*
Notes	Sourced from *`Application`* table in the TachyonMaster database.

ClientAgeMonths

Instance format	NumberOfMonthsAgo
Example instance	7
Value format	Count of number of devices
Example value	*42*
Notes	Sourced from *`Device`* table in the TachyonMaster database.

ClientAgeMonths

	Based on calendar months, rather than multiples of 30 days - e.g. if today is 2nd July, a device "first seen" on the 30th June will be counted as first seen as one month ago. An instance of zero means "within the last month". Can be used to determine client deployment rate.

ClientConfiguration

Instance format	"1EClientConfiguration"
Example instance	`"NM:E0505,PX:0,TAC:40AA4A,TAI:3FFE3,TUI:60080006"`
Value format	Number of clients with that configuration
Example value	`88`
Notes	Sourced from *`Device`* table in the TachyonMaster database.

ClientConnectivity

Instance format	OnlineStatus|SwitchId|ConnectivityFlags
Example instances	`Online|1|384` `Offline|0|384`
Value format	Count of number of devices for that combination
Example value	*42*
Notes	Sourced from *`Device`* table in the TachyonMaster database. Where devices are offline, their connection flags represent the values as they were at the time of their last connection.

ClientLastSeenDays

Instance format	NumberOfDays
Example instance	7
Value format	Count of number of devices
Example value	*42*
Notes	Sourced from *Device* table in the TachyonMaster database. Milestones are 1, 2, 4, 7, 30, 90 and 365 days. The numbers will be *cumulative*, because a device which has been since in the last 1 day will also be counted in 2 days, 4 days, 7 days, etc.

ClientOsVersion

Instance format	DeviceType|OsVersionText|OsArchitecture|VirtualizationPlatform

Example instances	`Desktop|CentOS Linux release 8.2.2004 (Core) |x64|Hyper-V`
	`Desktop|Red Hat Enterprise Linux release 8.1 (Ootpa)|x64|Hyper-V`
	`Desktop|Ubuntu 18.04.4 LTS|x64|Hyper-V`
	`Desktop|Windows 10 Pro N 2004|x86|Hyper-V`
	`Desktop|Windows 7 Enterprise|x86| <- absence of Virtualization platform implies physical device`
	`Server|Windows Server 2016 Standard 1607|x64|`

Value format	Count of number of devices running that OS variant
Example value	*42*
Notes	Sourced from *Device* table in the TachyonMaster database.

ClientTimeZone

Instance format	TimeZoneIdentifier

ClientTimeZone

Example instances	`Europe/London` `Asia/Calcutta`
Value format	Count of number of devices detected in that timezone
Example value	*42*
Notes	Sourced from *`Device`* table in the TachyonMaster database.

ClientVersion

Instance format	ClientVariant|ClientVersionNumber
Example instances	`Windows|5.1.0.885` `Linux|5.0.0.234`
Value format	Count of number of devices running that variant/version of the 1E Client
Example value	*182*
Notes	Sourced from *`Device`* table in the TachyonMaster database.

Component

Instance format	Component
Example instances	`BackgroundChannel` `SwitchConfiguration.2`
Value format	For components other than the Switch, a count of instances of that component For Switch components, a pipe-delimited sequence of: • X w - number of configured workers • X s - number of configured slots

Component

	• X seclvl - configured security level • X switches - number of Switches with this configuration • X cores - number of cores bound to Switches with this configuration
Example values	`2 (for non-Switch components)` `SwitchConfiguration.2,1 w|10 s|5 seclvl|1 switches|1 cores`
Notes	Sourced from *SwitchConfiguration, Switch, BackgroundChannel, CoreApiConfiguration*tables in the TachyonMaster database.

Consumer

Instance format	Consumer
Example instance	`CmConsoleExtensions`
Value format	0 = disabled, 1 = enabled
Example value	*1 (i.e. enabled)*
Notes	Sourced from *Consumer* table in the TachyonMaster database.

InstructionDefinitionUse

Instance format	Instruction Definition Name|Instruction Definition Version
Example instance	`1E-Explorer-TachyonAgent-AgentConnectionDiagnostics|17.3`
Value format	Pipe-delimited sequence of: • X use - number of times the instruction definition has been run • X targeted - total number of devices targeted

InstructionDefinitionUse

	• X sent - total number of devices to which this instruction has been sent • X no data - total number of "success, no content" responses • X error - total number of "error" responses • X not_impl - total number of "not implemented" responses • X too_large - total number of "response too large" responses • X success_rows - total number of rows of data returned in responses • X mb_sent - total number of megabytes of network traffic sent from Switch to 1E Client • X mb_recv - total number of megabytes of network traffic received by Switch from 1E Client • X mb_urecv - total number of megabytes of equivalent uncompressed network traffic received by Switch from 1E Client All the values above are based on the sum of all executions of that instruction definition.
Example value	`2 use|900 targeted|876 sent|1 no_data|3 error|7 not_impl|0 too_large|52286 success_rows|17 mb_sent|35 mb_recv|208 mb_urecv`
Notes	Sourced from *`InstructionDefinition`* and *`InstructionStatistics`* tables in the TachyonMaster database. If an instruction definition is updated, this row reflects usage only of the most recent version of that instruction definition.

InstructionResourceCount

Instance format	ResourceType
Example instance	`Perl`

InstructionResourceCount

Value format	Total number of resources of that type
Example value	*33*
Notes	Sourced from *InstructionDefinitionResource* table in the TachyonMaster database.

InstructionResourceKb

Instance format	ResourceType
Example instance	`PowerShell`
Value format	Total size in kilobytes
Example value	*69*
Notes	Sourced from *InstructionDefinitionResource* table in the TachyonMaster database.

InstructionThroughput

Instance format	Localized date/time
Example instance	`8/4/2020 12:00:00 AM +01:00`
Value format	Pipe-delimited sequence of: • X instr - number of instructions run on that day • X targeted - total number of devices targeted • X sent - total number of devices to which instructions were sent • X no data - total number of "success, no content" responses • X error - total number of "error" responses

InstructionThroughput

	• X not_impl - total number of "not implemented" responses • X too_large - total number of "response too large" responses • X success_rows - total number of rows of data returned in responses • X mb_sent - total number of megabytes of network traffic sent from Switch to 1E Client • X mb_recv - total number of megabytes of network traffic received by Switch from 1E Client • X mb_urecv - total number of megabytes of equivalent uncompressed network traffic received by Switch from 1E Client All the values above are based on the sum of all executions of instructions on that day.
Example value	`19 instr|94 targeted|94 sent|28 no_data|36 error|0 not_impl|0 too_large|2419 success_rows|0 mb_sent|0 mb_recv|1 mb_urecv`
Notes	Sourced from *`InstructionStatistics`* table in the TachyonMaster database.

ManagementGroup

Instance format	ManagementGroupId|ManagementGroupType
Example instance	76|2
Value format	Number of devices in that management group
Example value	777
Notes	Sourced from *`ManagementGroup`* table in the TachyonMaster database. Management group types are (System = 0, Internal = 1, External = 2)

Table

Instance format	TableName
Example instance	`PolicyRuleStatus`
Value format	Pipe-delimited sequence of: • X rows - number of rows in the table • X kb_resv - total size (data and index) of reserved space for this table (i.e. space consumed on disk) • X kb_data - total size of data for this table • X kb_idx - total size of index data for this table
Example value	*95 rows|144 kb_resv|16 kb_data|32 kb_idx*
Notes	Sourced from SQL table metadata; this data may not be available if the account used to perform the query does not have permissions to query sys.* tables for TachyonMaster database. The query to derive this information is based on the query used by SQL Server Management Studio to build the "Disk Usage" report.

Upgrade

Instance format	VersionNumber
Example instance	`5.1.0.607`
Value format	Localized date/time
Example value	`8/4/2020 11:10:33 PM +01:00`

Upgrade	
Notes	Sourced from *AppliedChanges2* table in the TachyonMaster database. The version number is derived from the "SourceVersion" column, which typically is the binary version of the database resource DLLs containing the database changes to apply. Hotfixes will only be registered if they perform a database change.

1.11.10.3 System health components and checks

The **System Health** page runs a comprehensive series of component checks. By default, it shows issues, but you can see a full list of green lights by toggling **Issues only**.

The System Health page is accessible from **Settings**→**Monitoring**→**System health**.

The components in the table are:

Background Channel | Consumer API | Coordinator service Agent Deployment module | Coordinator service Licensing module | Coordinator service Management Groups module | Coordinator service Policy module | Coordinator service | Core | SLA Admin | SLA Engine | SLA Integrate Agent service | SLA Integrate Manager service | SLA Platform API | Switch

Component	Check	Description
Background Channel	Folder '~/Content' write access check	Check that the Background Channel can write to the "Content" folder within the app pool user context.
Folder '~/Installers' read access check	Check that the Background Channel can read from the "Installers" folder within the app pool user context.	
Folder '~/Policy Documents' write access check	Check that the Background Channel can write to the "PolicyDocuments" folder within the app pool user context.	
Folder '~/Update	Check that the Background Channel can read from the	

Component	Check	Description
s' read access check	"Updates" folder within the app pool user context.	
Consumer API	Active Directory connection check	Check that Consumer API can connect to Active Directory. *Uses the configured GC or LDAP connection string.*
Background Channel API connection check(s)	Check that Consumer API can connect to Background Channel API. *Uses the URL(s) stored in the TachyonMaster database.*	
Coordinator API connection check	Check that Consumer API can connect to Coordinator API. *Uses the OperationalSafeGuardsUrl application setting.*	
Core API '<Core server>' connection check(s)	Check that Consumer API can connect to Core API. *Uses the URL(s) stored in the TachyonMaster database.*	
Tachyon Master database connection check	Check that Consumer API can connect to the TachyonMaster database. *Uses the configured connection string (TachyonMaster) within the app pool user context.*	
TachyonResponse database	Check that Consumer API can connect to the TachyonResponse database(s).	

Component	Check	Description
connection check(s)	*Uses the stored connection strings within the TachyonMaster database under the app pool user context.*	
Coordinator service Agent Deployment module	Background Channel API connection check	Check that Coordinator Agent Deployment module can connect to Background Channel API. *Uses the URL(s) stored in the TachyonMaster database.*
Coordinator service Licensing module	Check license service URL	Verify that license service URL is from a trusted issuer.
Check license validity	Verify license expiry date.	
Check trust with licensing component	Verify trust between coordinator and licensing component by comparing signatures between the licensing module DLL and licensing DLL.	
Coordinator service Management Groups module	Management Group API connection check	Check that Coordinator Management Groups module can connect to SLA Management Group API using the configured URL. *Uses the SLAEndpoint module setting.*
Coordinator service	Background Channel API connection check	Check that Coordinator Policy Module can connect to Background Channel API.

Component	Check	Description
Policy module		*Uses the URL(s) stored in the TachyonMaster database.*
Coordinator service	Active Directory connection check	Check that Coordinator can connect to Active Directory. *Uses the configured GC or LDAP connection string.*
Coordinator certificate check	Check that Coordinator has a valid certificate used for the SSL API communication.	
SMTP connection check	Check that Coordinator can connect to the SMTP server using the "EHLO" command. *Only shown if SMTP emails has been enabled.*	
Tachyon Master database connection check	Check that Coordinator can connect to the TachyonMaster database. *Uses the configured connection string (TachyonMaster) within the app pool user context.*	
Website application authentication check	Check that Consumer API site has Windows authentication enabled and that Anonymous authentication is disabled.	
Website certificate binding check	Check that Consumer API has a valid certificate binding.	

Component	Check	Description
Core	TachyonMaster database connection check	Check that Core can connect to TachyonMaster database. *Uses the configured connection string (TachyonMaster) within the app pool user context.*
TachyonResponse database connection check(s)	Check that Core can connect to TachyonResponse database(s). *Uses the stored connection strings within the TachyonMaster database under the app pool user context.*	
SLA Admin	Consumer API connection check	Check that SLA Admin can connect to the Consumer API. *Uses the PermissionCheckerRootUrl application setting.*
SLA Platform API connection check	Check that SLA Admin can connect to the SLA Platform API.	
SLA-Data database connection check	Check that SLA Admin can connect to the SLA-Data database. *Uses the configured connection string (DefaultCustomerConnection) within the app pool user context.*	
SLA-Shared database connection check	Check that SLA Admin can connect to the SLA-Shared database. *Uses the configured connection string (DefaultSharedConn*	

Component	Check	Description
	ection) within the app pool user context.	
SLA Engine	1ECatalog database connection check	Check that SLA Engine can connect to the 1ECatalog database. *Uses the BaseUri application setting to request the 1ECatalog connection string from the SLA Platform API. The database connection check is performed within the service user context.*
Catalog API connection check	Check that SLA Engine can connect to the Catalog API. *Uses the URL retrieved from the SLA-Data.Component table for 1ECatalog within the service user context.*	
Consumer API connection check	Check that SLA Engine can connect to the Consumer API. *Uses the TachyonConsumerRootUrl application setting.*	
SLA Platform API connection check	Check that SLA Engine can connect to the SLA Platform API. *Uses the BaseUri application setting.*	
SLA-Data database connection check	Check that SLA Engine can connect to the SLA-Data database. *Uses the configured connection string (DefaultCustomerConnection) within the service user context.*	

Component	Check	Description
SLA-Shared database connection check	Check that SLA Engine can connect to the SLA-Shared database. *Uses the configured connection string (DefaultSharedConnection) within the service user context.*	
SLA Integrate Agent service *(part of SLA Integrate services)*	Folder '<ConnectorsRoot>' write access check	Check the SLA Integrate Agent can write to the 'dir-connectors' folder within the service user context.
Folder '<InstallerRoot>' write access check	Check the SLA Integrate Agent can write to the 'dir-job-output' folder within the service user context.	
Folder '<JobOutputRoot>' write access check	Check the SLA Integrate Agent can write to the 'dir-job-output' folder within the service user context.	
SLA Integrate Manager connection check	Check that the SLA Integrate Agent can connect to the SLA Integrate Manager. *Uses the rest-api-address application setting.*	

Component	Check	Description
SLA Platform API connection check	Check that the SLA Integrate Agent can connect to the SLA Platform API. *Uses the rest-api-address application setting to request the SLA Platform API address from the SLA Integrate Manager.*	
SLA Integrate Manager service *(part of SLA Integrate services)*	Folder '<InstallerRoot>' write access check	Check the SLA Platform Integrate Manager can write to the 'dir-installers' folder within the service user context.
Folder '<JobOutputRoot>' write access check	Check the SLA Platform Integrate Manager can write to the 'dir-job-output' folder within the service user context.	
SLA Platform API connection check	Check that SLA Integrate Manager can connect to the SLA Platform API. *Uses the sla-data-address application setting.*	
SLA-Integrate database connection check	Check the SLA Integrate Manager service can connect to the SLA-Integrate database.	

Component	Check	Description
	Uses the configured connection string (default) within the service user context.	
SLA Platform Integrate Agent	Check at least one SLA Platform Integrate Agent has reporting health status.	
SLA Platform API *API includes the UI* *The following are not checked:* • *SLA Inventory* • *SLA Operations Provider API*	1ECatalog database connection check	Check that SLA Platform API can connect to the 1ECatalog database. *Uses the configured connection string (DefaultCatalogConnection) within the app pool user context.*

Component	Check	Description
Consumer API connection check	Check that SLA Platform API can connect to Consumer API. *Uses the PermissionCheckerRootUrl application setting.*	
SLA-Data database connection check	Check that SLA Platform API can connect to the SLA-Data database. *Uses the configured connection string (DefaultCustomerConnection) within the app pool user context.*	
SLA-Shared database connection check	Check that SLA Platform API can connect to the SLA-Shared database. *Uses the configured connection string (DefaultSharedConnection) within the app pool user context.*	
SLA Engine	Check the SLA Engine has reported health status.	
Switch *Switch Host is not checked*	Core Connect (Device)	Check if this Switch can connect to core Device endpoint.
Core Connect (Instructions)	Check if this Switch can connect to core Instructions endpoint.	

Component	Check	Description
Core Connect (Policy Response)	Check if this Switch can connect to core Policy Response endpoint.	
Core Connect (Policy)	Check if this Switch can connect to core Policy endpoint.	
Core Connect (Response)	Check if this Switch can connect to core Response endpoint.	
Core Connect (Switch)	Check if this Switch can connect to core Switch endpoint.	
Recent administrative events.	Check if this Switch has had any recent errors or warnings (since last instruction poke)	

1.11.11 Inventory reference

Reference information specific to the Catalog and SLA components of the Tachyon Platform.

1.11.11.1 Autocuration and Partial Matching

How inventoried products are matched with the Catalog.

In cases where we don't have an exact match, partial matching and autocuration will be used to attempt to create valid matches.

The order of precedence for attempts is:

- Exact Match
- Full Match
- Autocuration
- Partial Match

1.11.11.1.1 Exact Match

Exact match for non edition based products:

- source V & T & Version = catalog V & T & Version

Exact match for edition based products:

- source V & T & Version & Edition = catalog V & T & Version & Edition

1.11.11.1.2 Full Match

Full match for non edition based products:

- source V & T & Version = catalog match rule l.h.s. V & T & Version

Exact match for edition based products:

- source V & T & Version & Edition = catalog match rule l.h.s. V & T & Version & Edition

1.11.11.1.3 Autocuration

Source must have number of version parts>= matching catalog entry.

When exact and full match fail, we attempt auto curation. This involves add a new version to the catalog for a specific Vendor and Title where one didn't exist before. Before doing this, we need to be confident that the version we are about to create is a valid version.

Once the new versions is added, a match is returned between the source VTVCE and the new catalog VTVCE record

The following rules must be adhered to before autocurating an entry:

- The source VT matches with a catalog VT either directly (exact) or via a match rule
  - e.g. Source Vendor = 'Microsoft' and Source Title 'Microsoft Visio'
  - there should be at least one match rule that matches the source VT to catalog VT
- The source version doesn't contain **any letters or special characters** (e.g. '/' or '-')
- If there is already an entry in the catalog with the same version major.minor, then the source major.minor must have equal or greater than number of version parts than the catalog version
  - This is to have confidence that the version we are about to add to catalog is an accurate version rather than missing some version parts
- If there is no existing major.minor in the catalog, then autocuration can occur i.e. new major.minor can be created
- For edition based product
  - The match rule being used for autocuration must be on the edition rather than the version

1.11.11.1.4 Partial Match

Source version must be same major.minor as catalog match.

If autocuration hasn't taken place, then Partial Matching is attempted. For partial matching to occur, the source version should have less than the number of version parts of the major.minor of the catalog.

Note: if it has the same or greater number of version parts then it would have autocurated

So, for example, if the catalog has version 3.2.1.1 for a specific VT and the source version was 3.2 then partial matching can take place. In partial matching, the lowest version for that catalog major.minor is returned.

1.11.11.1.5 Glossary

Edition based product is defined as a product that has at least one edition for a specific major version

Number of Version parts: how many different parts of the version number there are – e.g. 1.2.3 , number of version parts is 3

Exact match is when source VTV matches exactly a catalog VTV. If its an edition based product then it's the source VTVE matches exactly catalog VTVE

Full match is when the source VTV does not match a catalog VTV directly, but matches the source VTV via a match rule. If its an edition based product that the source VTV or VTVE matches a catalog VTVE via a match rule

l.h.s: left hand side of match rule , i.e. the source VTVCE of the match rule

VTVCE - Vendor, Title, Version, Colloquial version, Edition

VT - Vendor and Title only

Partial Match - the source Vendor and Title match the Catalog Vendor and Title

Partial Version Match - the conditions are fulfilled (see below) whereby the lowest version number for a speciific major.minor is returned as a match

1.11.11.2 By Device table

The table column headings and descriptions for the **By Device** table.

1.11.11.2.1 The By Device table

The following table shows the headings in the **By Device** table, accessible from the **Inventory→By Device** node in the navigation console:

Column heading	Description
Host Name	The name for the device. This is a link that navigates to the Product Details table for the selected device.
Last Inventory Date	The date when inventory information was last returned for the device.

Computer Type	The type of the device. For example **Workstation**, **Desktop**, **Laptop**, **Server** or **Virtual Machine** etc.
Device Model	The model for the device. For example: **Virtual Machine**, **Surface Pro 3**, **Optiplex 910** etc.
OS	The Operating System installed on the device. For example **Windows 10 Pro**.
Number of Unnormalized Software Records	The number of unnormalized software records associated with the device, i.e. the number of installed software titles on the device that couldn't be automatically matched by 1E Catalog. This is formatted as a link, click to match the records to the catalog.
Number of Normalized Software Records	The number of normalized software records associated with the device, i.e. the number of software titles installed on the device that were matched by 1E Catalog.

1.11.11.3 Product Details table

The table column headings and descriptions for the Product Details table.

1.11.11.3.1 The Product Details table

The following table shows the headings in the **Product Details** table, accessible from the **Products By Vendor** screen:

Column heading	Description
Vendor	The vendor who sells the installed software title. For example **Microsoft Corporation** is the vendor for **Office 365**.
Title	The title name for the installed software title. For example the title for Microsoft Office 365 can be **Office 365**.
Colloquial Version	Any associated informal name for the version of the installed software title. For example the Colloquial Version for Microsoft Office 365 could be **2016**.
Edition	The specific edition of the installed software title. For example the Edition for Microsoft Office 365 could be **ProPlus**.
Version	The specific version for the installed software title. For example the specific version for Microsoft Office 365 could be **16.0.10228.20080**.

Host	The host where the software title is installed. For example **Acme-win1002**.
Host Computer Name	The computer name for the host where the software title is installed.
Computer Type	The type of the computer where the software title is installed. For example **Workstation**, **Server** or **Virtual Machine**.
OS	The Operating System where the software title is installed. For example **Windows 10 Pro**.

1.11.11.4 Secondary App Rules

1.11.11.4.1 Rules used to define whether an unnormalized application is defined as a 'Secondary app'

Rules are run against all unmatched applications to identify whether they should be categorized as one of the following:

- Unidentified
- Secondary Apps

The table below shows all the rules used to categorize unmatched applications as a **Secondary Apps** rather than **Unidentified**.

Rules with the same RuleID use an **AND** operator; those with a different RuleID use an **OR** operator.

RulesetName	RuleID	FieldName	Operation Name	Value	IsDeleted	Is1EVerified
RuleSetInventory	1	SOURCE_TITLE	CONTAIN	Policy	0	1
RuleSetInventory	2	SOURCE_TITLE	CONTAIN	Debugging	0	1
RuleSetInventory	3	SOURCE_TITLE	CONTAIN	Office suite service pack	0	1
RuleSetInventory	4	SOURCE_TITLE	CONTAIN	Microsoft_VC	0	1
RuleSetInventory	5	SOURCE_TITLE	CONTAIN	Language pack	0	1

RuleSetInventory	6	SOURCE_TITLE	CONTAIN	support	0	1
RuleSetInventory	7	SOURCE_TITLE	CONTAIN	Builder	0	1
RuleSetInventory	8	SOURCE_TITLE	CONTAIN	plug-in	0	1
RuleSetInventory	9	SOURCE_TITLE	CONTAIN	Utilities	0	1
RuleSetInventory	10	SOURCE_TITLE	CONTAIN	plugin	0	1
RuleSetInventory	11	SOURCE_TITLE	CONTAIN	Prerequisite	0	1
RuleSetInventory	12	SOURCE_VENDOR	CONTAIN	Microsoft	0	1
RuleSetInventory	12	SOURCE_TITLE	CONTAIN	vs_%msi	0	1
RuleSetInventory	13	SOURCE_TITLE	CONTAIN	policies	0	1
RuleSetInventory	14	SOURCE_TITLE	CONTAIN	redistributable	0	1
RuleSetInventory	15	SOURCE_VENDOR	NOT_CONTAIN	Hewlett	0	1
RuleSetInventory	15	SOURCE_VENDOR	NOT_CONTAIN	Productivity	0	1
RuleSetInventory	15	SOURCE_VENDOR	NOT_CONTAIN	NetCentrics	0	1
RuleSetInventory	15	SOURCE_VENDOR	NOT_CONTAIN	Oracle	0	1

RuleSetInventory	15	SOURCE_VENDOR	NOT_CONTAIN	WILUTIONS	0	1
RuleSetInventory	15	SOURCE_VENDOR	NOT_EQUAL	HP	0	1
RuleSetInventory	15	SOURCE_TITLE	CONTAIN	Add in	0	1
RuleSetInventory	15	SOURCE_VENDOR	NOT_CONTAIN	Mission	0	1
RuleSetInventory	15	SOURCE_TITLE	NOT_CONTAIN	Intune	0	1
RuleSetInventory	16	SOURCE_TITLE	CONTAIN	template	0	1
RuleSetInventory	17	SOURCE_TITLE	CONTAIN	.arp.	0	1
RuleSetInventory	18	SOURCE_TITLE	CONTAIN	.product.	0	1
RuleSetInventory	19	SOURCE_TITLE	CONTAIN	interpreter	0	1
RuleSetInventory	20	SOURCE_TITLE	CONTAIN	Packaging	0	1
RuleSetInventory	21	SOURCE_VENDOR	CONTAIN	SAP	0	1
RuleSetInventory	21	SOURCE_TITLE	CONTAIN	crystalreports.webreporting.	0	1
RuleSetInventory	22	SOURCE_VENDOR	NOT_CONTAIN	Hewlett	0	1
RuleSetInventory	22	SOURCE_VENDOR	NOT_CONTAIN	Productivity	0	1

RuleSetInventory	22	SOURCE_TITLE	NOT_CONTAIN	Intune	0	1
RuleSetInventory	22	SOURCE_VENDOR	NOT_CONTAIN	Mission	0	1
RuleSetInventory	22	SOURCE_VENDOR	NOT_CONTAIN	NetCentrics	0	1
RuleSetInventory	22	SOURCE_VENDOR	NOT_CONTAIN	Oracle	0	1
RuleSetInventory	22	SOURCE_VENDOR	NOT_CONTAIN	WILUTIONS	0	1
RuleSetInventory	22	SOURCE_VENDOR	NOT_EQUAL	HP	0	1
RuleSetInventory	22	SOURCE_TITLE	CONTAIN	Add-in	0	1
RuleSetInventory	23	SOURCE_VENDOR	NOT_CONTAIN	Intel	0	1
RuleSetInventory	23	SOURCE_VENDOR	NOT_CONTAIN	Abyss	0	1
RuleSetInventory	23	SOURCE_VENDOR	NOT_CONTAIN	9Rays	0	1
RuleSetInventory	23	SOURCE_VENDOR	NOT_CONTAIN	Eltima	0	1
RuleSetInventory	23	SOURCE_VENDOR	NOT_CONTAIN	MathWorks	0	1
RuleSetInventory	23	SOURCE_VENDOR	NOT_CONTAIN	Crestron	0	1
RuleSetInventory	23	SOURCE_TITLE	CONTAIN	compiler	0	1

RuleSetInventory	23	SOURCE_VENDOR	NOT_CONTAIN	SourceTec	0	1
RuleSetInventory	23	SOURCE_VENDOR	NOT_CONTAIN	Hex%Rays	0	1
RuleSetInventory	24	SOURCE_VENDOR	CONTAIN	SAP	0	1
RuleSetInventory	24	SOURCE_TITLE	CONTAIN	repoaccess.async_scheduling	0	1
RuleSetInventory	25	SOURCE_TITLE	CONTAIN	Console	0	1
RuleSetInventory	26	SOURCE_TITLE	CONTAIN	debugger	0	1
RuleSetInventory	27	SOURCE_TITLE	CONTAIN	pre-requisite	0	1
RuleSetInventory	28	SOURCE_TITLE	CONTAIN	-core-	0	1
RuleSetInventory	28	SOURCE_VENDOR	CONTAIN	SAP	0	1
RuleSetInventory	29	SOURCE_TITLE	CONTAIN	Checker	0	1
RuleSetInventory	30	SOURCE_TITLE	CONTAIN	MUI	0	1
RuleSetInventory	31	SOURCE_TITLE	CONTAIN	SDK	0	1
RuleSetInventory	32	SOURCE_TITLE	CONTAIN	setup	0	1
RuleSetInventory	33	SOURCE_TITLE	CONTAIN	installer	0	1

RuleSetInventory	33	SOURCE_VENDOR	NOT_CONTAIN	PrinterLogic	0	1
RuleSetInventory	34	SOURCE_TITLE	CONTAIN	package	0	1
RuleSetInventory	35	SOURCE_VENDOR	NOT_CONTAIN	WILUTIONS	0	1
RuleSetInventory	35	SOURCE_VENDOR	NOT_CONTAIN	Mission	0	1
RuleSetInventory	35	SOURCE_VENDOR	NOT_EQUAL	HP	0	1
RuleSetInventory	35	SOURCE_VENDOR	NOT_CONTAIN	NetCentrics	0	1
RuleSetInventory	35	SOURCE_VENDOR	NOT_CONTAIN	Hewlett	0	1
RuleSetInventory	35	SOURCE_VENDOR	NOT_CONTAIN	Productivity	0	1
RuleSetInventory	35	SOURCE_TITLE	NOT_CONTAIN	Intune	0	1
RuleSetInventory	35	SOURCE_VENDOR	NOT_CONTAIN	Oracle	0	1
RuleSetInventory	35	SOURCE_TITLE	CONTAIN	addon	0	1
RuleSetInventory	36	SOURCE_VENDOR	CONTAIN	SAP	0	1
RuleSetInventory	36	SOURCE_TITLE	CONTAIN	cvom.java	0	1
RuleSetInventory	37	SOURCE_TITLE	CONTAIN	plug in	0	1

RuleSetInventory	38	SOURCE_TITLE	CONTAIN	crystalreports.langpack	0	1
RuleSetInventory	38	SOURCE_VENDOR	CONTAIN	SAP	0	1
RuleSetInventory	39	SOURCE_TITLE	CONTAIN	Library	0	1
RuleSetInventory	40	SOURCE_VENDOR	CONTAIN	SAP	0	1
RuleSetInventory	40	SOURCE_TITLE	CONTAIN	crystalreports.dataaccess	0	1
RuleSetInventory	41	SOURCE_TITLE	CONTAIN	olap.	0	1
RuleSetInventory	42	SOURCE_TITLE	CONTAIN	documentation	0	1
RuleSetInventory	43	SOURCE_TITLE	NOT_CONTAIN	Intune	0	1
RuleSetInventory	43	SOURCE_VENDOR	NOT_EQUAL	HP	0	1
RuleSetInventory	43	SOURCE_VENDOR	NOT_CONTAIN	Oracle	0	1
RuleSetInventory	43	SOURCE_VENDOR	NOT_CONTAIN	Productivity	0	1
RuleSetInventory	43	SOURCE_TITLE	CONTAIN	add-on	0	1
RuleSetInventory	43	SOURCE_VENDOR	NOT_CONTAIN	WILUTIONS	0	1
RuleSetInventory	43	SOURCE_VENDOR	NOT_CONTAIN	Mission	0	1

RuleSetInventory	43	SOURCE_VENDOR	NOT_CONTAIN	NetCentrics	0	1
RuleSetInventory	43	SOURCE_VENDOR	NOT_CONTAIN	Hewlett	0	1
RuleSetInventory	44	SOURCE_TITLE	CONTAIN	bootstrap	0	1
RuleSetInventory	45	SOURCE_TITLE	CONTAIN	libraries	0	1
RuleSetInventory	46	SOURCE_TITLE	CONTAIN	KB[0-9][0-9][0-9]	0	1
RuleSetInventory	47	SOURCE_TITLE	CONTAIN	utility	0	1
RuleSetInventory	48	SOURCE_TITLE	CONTAIN	Sample	0	1
RuleSetInventory	49	SOURCE_VENDOR	CONTAIN	SAP	0	1
RuleSetInventory	49	SOURCE_TITLE	CONTAIN	crystalreports.cpp.	0	1
RuleSetInventory	50	SOURCE_TITLE	CONTAIN	Addin	0	1
RuleSetInventory	50	SOURCE_VENDOR	NOT_CONTAIN	Productivity	0	1
RuleSetInventory	50	SOURCE_VENDOR	NOT_CONTAIN	Oracle	0	1
RuleSetInventory	50	SOURCE_VENDOR	NOT_CONTAIN	NetCentrics	0	1
RuleSetInventory	50	SOURCE_VENDOR	NOT_CONTAIN	WILUTIONS	0	1

RuleSetInventory	50	SOURCE_VENDOR	NOT_CONTAIN	Hewlett	0	1
RuleSetInventory	50	SOURCE_TITLE	NOT_CONTAIN	Intune	0	1
RuleSetInventory	50	SOURCE_VENDOR	NOT_CONTAIN	Mission	0	1
RuleSetInventory	50	SOURCE_VENDOR	NOT_EQUAL	HP	0	1
RuleSetInventory	51	SOURCE_TITLE	CONTAIN	connectivity.connectionserver.drivers	0	1
RuleSetInventory	51	SOURCE_VENDOR	CONTAIN	SAP	0	1
RuleSetInventory	52	SOURCE_TITLE	CONTAIN	runtime	0	1
RuleSetInventory	53	SOURCE_TITLE	CONTAIN	.%.	0	1
RuleSetInventory	54	SOURCE_TITLE	CONTAIN	Lang pack	0	1
RuleSetInventory	55	SOURCE_TITLE	CONTAIN	shared.tp.	0	1
RuleSetInventory	55	SOURCE_VENDOR	CONTAIN	SAP	0	1
RuleSetInventory	56	SOURCE_TITLE	CONTAIN	Package	0	1
RuleSetInventory	57	SOURCE_VENDOR	NOT_EQUAL	HP	0	1
RuleSetInventory	57	SOURCE_TITLE	CONTAIN	add on	0	1

RuleSetInventory	57	SOURCE_VENDOR	NOT_CONTAIN	Oracle	0	1
RuleSetInventory	57	SOURCE_VENDOR	NOT_CONTAIN	NetCentrics	0	1
RuleSetInventory	57	SOURCE_VENDOR	NOT_CONTAIN	Mission	0	1
RuleSetInventory	57	SOURCE_VENDOR	NOT_CONTAIN	WILUTIONS	0	1
RuleSetInventory	57	SOURCE_VENDOR	NOT_CONTAIN	Hewlett	0	1
RuleSetInventory	57	SOURCE_TITLE	NOT_CONTAIN	Intune	0	1
RuleSetInventory	57	SOURCE_VENDOR	NOT_CONTAIN	Productivity	0	1
RuleSetInventory	58	SOURCE_TITLE	CONTAIN	Pre requisite	0	1
RuleSetInventory	59	SOURCE_TITLE	CONTAIN	Hotfix	0	1
RuleSetInventory	60	SOURCE_TITLE	CONTAIN	MSVC	0	1
RuleSetInventory	61	SOURCE_TITLE	CONTAIN	.cpp	0	1
RuleSetInventory	62	SOURCE_TITLE	CONTAIN	help	0	1
RuleSetInventory	63	SOURCE_TITLE	CONTAIN	software development kit	0	1
RuleSetInventory	64	SOURCE_TITLE	CONTAIN	tp.apache	0	1

RuleSetInventory	64	SOURCE_VENDOR	CONTAIN	SAP	0	1
RuleSetInventory	65	SOURCE_TITLE	CONTAIN	UPDATE	0	1
RuleSetInventory	66	SOURCE_TITLE	NOT_CONTAIN	[a-z,A-Z]	0	1
RuleSetInventory	67	SOURCE_TITLE	IS_NULL		0	1
RuleSetInventory	68	SOURCE_TITLE	IS_EMPTY		0	1

1.11.11.5 Usage categories

Usage data is held in inventory repositories, and is obtained using the following types of connector:

- System Center Configuration Manager connector
- Tachyon connector

Software installations can have one of the following 4 usage categories:

- Used
- Rarely Used
- Unused
- Unreported:
- Unreported - Device stopped reporting usage: Device has a usage record but it has been 30 or more days since we received inventory from the device
- Unreported - Invalid usage date: there is a usage date but it's in the future
- Unreported - Recently installed: there is no usage date, the device has usage and the software was installed less than 7 days ago
- Unreported - Invalid install date: there is no usage date, the device has usage and the software was installed at a date in the future according to the source
- Unreported - No Product Usage: the software is not showing usage across any of its installs
- Unreported - No Device usage: the device is not reporting usage (possibly due to a corrupted Tachyon client or 1E Client)

- Unreported - Device Inventory too old: the device is not reporting usage and the inventory date is older than 30 days
- Unreported - Invalid Device Inventory date: the device is not reporting usage and the inventory date is in the future
- Unreported - No Device Inventory date: the device is not reporting usage and the inventory date is not present

How a software installation is categorized depends upon its **Last Usage Date** and the **Install Date**, both of which are derived from the inventory sources used.

- **Device Inventory Date** = maximum of device inventory dates for the consolidated device
- **Last Usage Date** = maximum of product usage date for the consolidated installation
- **End of Sync Date** = maximum of device inventory dates and maximum usage dates excluding dates in the future

	Device Inventory Date (relative to End of Sync Date)	No Device Inventory Date
Device Inventory Date < 30 days	Device Inventory Date >30 days	Device Inventory Date > End of Sync
Last Usage Date (relative to End of Sync Date)	No Last Usage Date	

All Usage on Device > 30 days old since Device Inventory	Last Usage Date > End of Sync Date	<=30 days	31-89 days	>=90 days	Device usage	No Device Usage
Product Usage across estate	No Product Usage across estate					

Install Date	Null	**Unreported** - Device stopped reporting usage	**Unreported** - Invalid Usage date	**Used**	**Rarely Used**	**Unused**	**Unused**	**Unreported** - No Product Usage	**Unreported** - No Device Usage	**Unreported** - Device inventory date too old	**Unreported** - Invalid Device inventory date	**Unreported** - No Device inventory date
< 7 Days	**Unreported** - Recently installed											
>=7 Days	**Unused**											
In the future	**Unreported** - Invalid install date											

If there is no usage data found for a normalized software installation, then :

1) A check is made to see if any installation on this device is reporting usage. If not, then the **Install Date** is categorized as **Unreported - No Device Usage**

2) A check is then made to see if this software installation is reporting usage anywhere else in the inventory repository. If no, then the **Install Date** is categorized as **Unreported - No Product Usage**

3) If the device is showing usage and the product is reporting usage across the inventory repository, the **Install Date** of the software installation is used to categorize usage:

- If **Install Date** is NULL, then the software is assumed to be **Unused**
- If **Install Date** is less than 7 days, then the install is deemed to be **Unreported - Recently installed**, as the user may not have had a chance to run the application yet
- If **Install Date** is greater than or equal to 7 days, then the install is deemed to be **Unused**, as the user has had a chance to run the application and yet there is no usage record
- If **Install Date** is set in the future (as some can sometimes happen due to error in the source data), then categorize the usage as **Unreported - Invalid install date**

For bundled products, the Last Usage Date of each component is analyzed and the most recent Last Usage Date is used to determine its usage category for the bundle.

Warning

For AppClarity 7.0 onwards the 7, 30 and 90 day limits are configurable, but they must not be changed unless advised by 1E.

- InstallDateCutOffLimit - default 7
- UsedCategoryLimit - default 30
- UnusedCategoryLimit - default 90

The settings are configurable in **[SLA-Shared].[dbo].[ProjectSetting]** table, which gets copied to **[SLA-Data].[dbo].[InstanceSetting]** when a new Inventory repository is created. Each Inventory repository will have its own group of settings in the InstanceSetting table. You can edit **[SLA-Data].[dbo].[InstanceSetting]** to change the settings for an existing repository. If that repository contains reclaim policies, the new settings will take effect and update the policies after an action is run on the repository.

Use the following SQL script to view settings in both tables.

```
SELECT [Project].[Title] AS 'ProjectTitle'
      ,[ProjectSetting].[Name] AS 'ProjectName'
      ,[ProjectSetting].[Value]
  FROM [SLA-Shared].[dbo].[ProjectSetting]
  JOIN [SLA-Shared].[dbo].[Project]
  ON [Project].[ProjectID]=[ProjectSetting].[ProjectID]
  WHERE [ProjectSetting].[Group] = 'UsageCategory'

SELECT [Instance].[InstanceID]
      ,[Instance].[Name] AS 'InstanceName'
      ,[InstanceSetting].[Name] AS 'SettingName'
      ,[InstanceSetting].[Value]
  FROM [SLA-Data].[dbo].[InstanceSetting]
  JOIN [SLA-Data].[dbo].[Instance]
  ON [Instance].[InstanceID]=[InstanceSetting].[InstanceID]
```

```
AND [Instance].[ProjectID]=[InstanceSetting].[ProjectID]
WHERE [InstanceSetting].[Group] = 'UsageCategory'
```

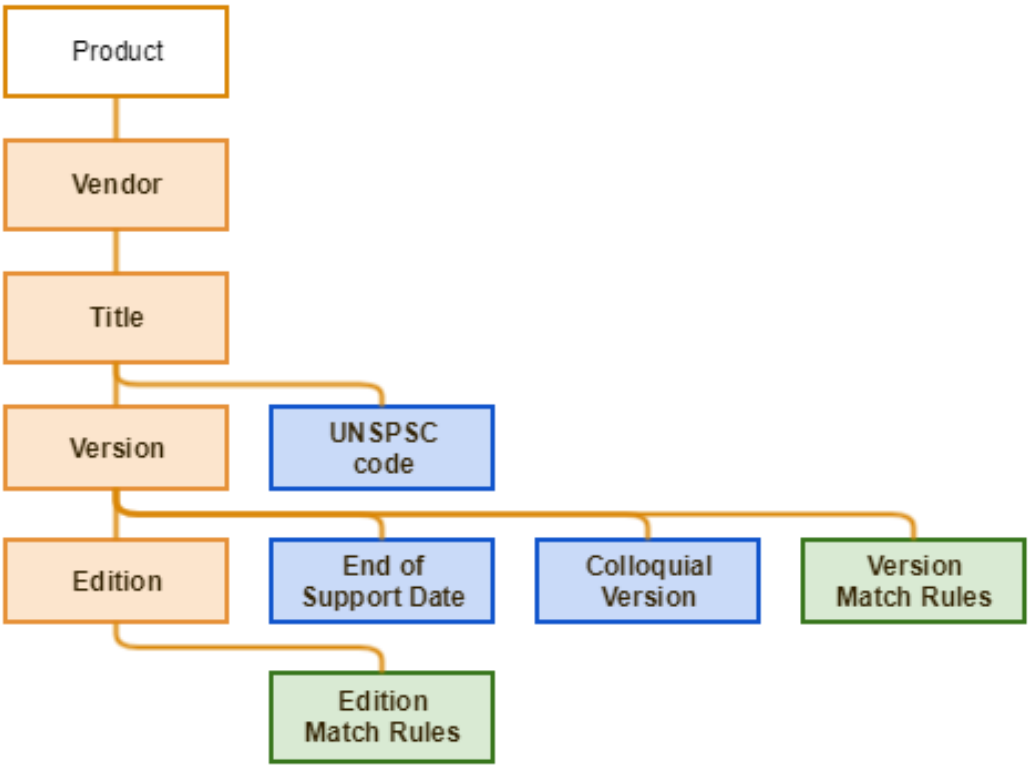
1.11.11.6 The Catalog structure

The 1E Catalog stores the canonical representation of software products, devices and processors, and the match rules used to identify them from inventory sources.

1.11.11.6.1 Products

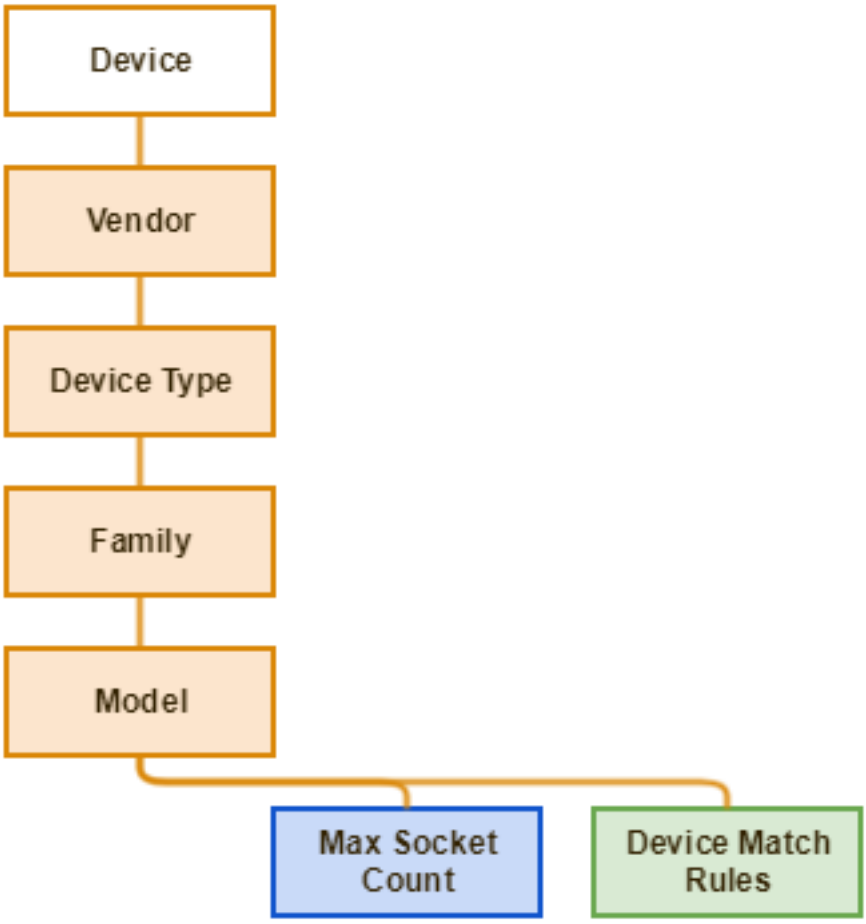
Products consist of software vendor, title, version and edition entries in the catalog that are structured as follows.

Attribute	Description
Vendor	Publisher of the software title, for example Microsoft Corporation.
Title	Name of the software product, for example Visio.
Version	Full version number of each release of the product.
Edition	If the product is an edition based product, the editions of this specific version of the product.
Edition Match rules	Rules that link one or more inventory source data entries to this specific edition, of this version, of this product.
End of support dates	Date when this version of the product is due to go end of support.
Colloquial version	If the product uses colloquial versions, then the one related to this specific version, for example 2013.
Version match rules	Rules that link one or more inventory source data entries to this specific version of this product.
UNSPSC	United Nations Standard Products and Services Code for this product, for example 43233004 for operating systems.



1.11.11.6.2 Devices

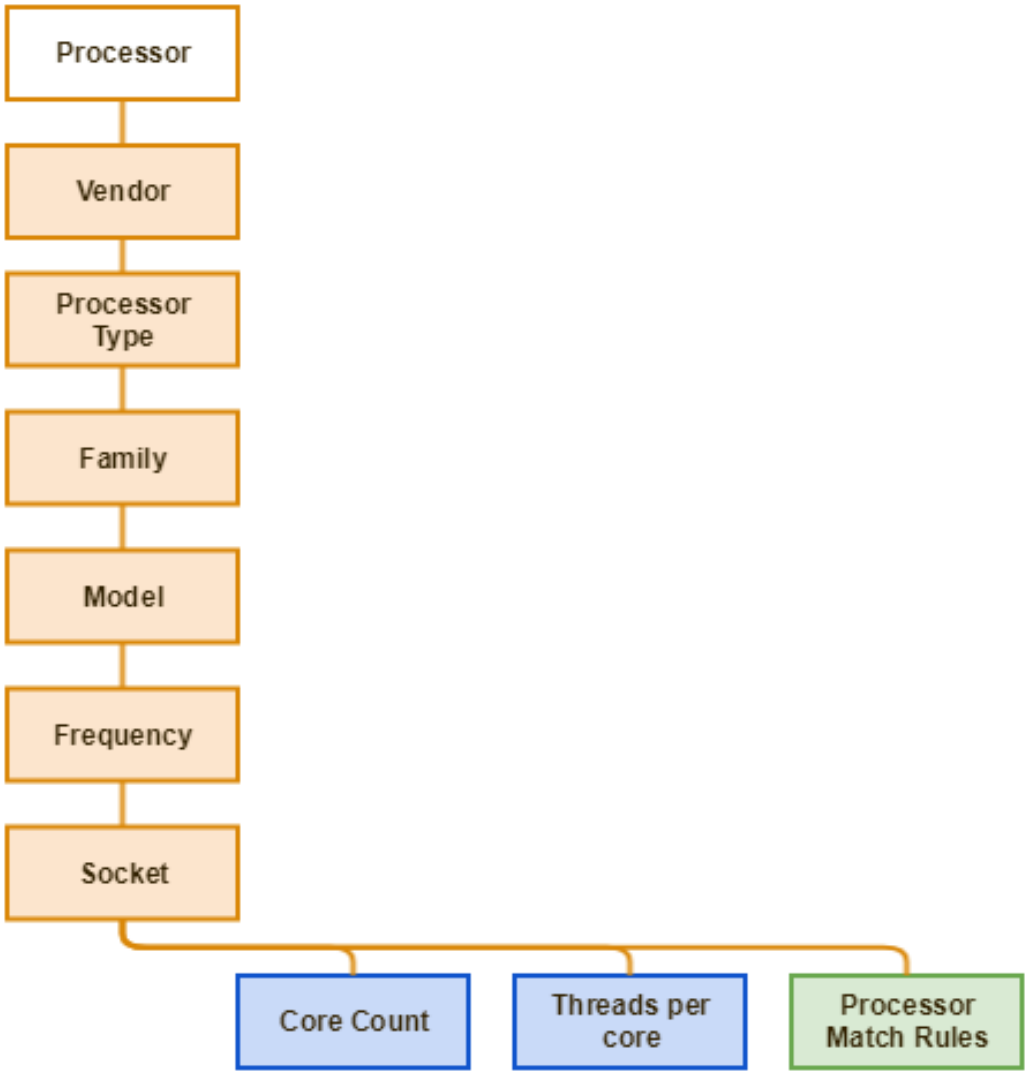
Attribute	Description
Vendor	Device vendor, for example, Dell.
Device Type	Device type, for example Desktop.
Family	Device family, for example, Inspiron.
Model	Device Model, for example, 400.
Max Socket Count	Maximum number of sockets for the device, for example, 1.
Device Match Rules	Rules that link one or more inventory source data entries to this specific device, device type, family and model.



1.11.11.6.3 Processors

Attribute	Description
Vendor	Processor vendor, for example, Advanced Micro Devices Inc.
Processor Type	Processor type, for example, Desktop.
Family	Processor family, for example, A10.
Model	Processor model, for example, 5700.
Frequency	Processor frequency, for example, 3,400.
Socket	The socket type the processor uses, for example, FMZ.
Core Count	Processor core count, for example, 4.

Attribute	Description
Threads per core	The number of threads per core for the processor, for example, 2.



1.11.11.7 Management groups rules

Rules used to create Management Groups, and which connectors that provide the data to support the rules.

For details of how to create and use Management Groups, please refer to Management Groups page.

Warning

The number of rules that a single Management Group can contain is variable because of many factors including SQL Server version, server configuration and rule type used. 1E recommends not exceeding 10,000 rules per rule-based Management Group.

Rule name	Description	SCCM	ServiceNow	Tachyon	OracleLMS	BigFix	BigFixInv	Intune	vCenter	WSUS
Device ADSite Name	AD Site the device is connected to.	✓	✓							
Device Assigned Cores	Maximum number of assigned cores for the device. Derived from	✓	✓	✓	✓	✓			✓	
Device Classification	Classification of the device. For example, **Test**, **Production** or **Development**. **Note** **Production** is the default.	✓	✓		✓					
Device Computer Name	Hostname of the computer.	✓	✓	✓	✓	✓	✓	✓	✓	✓
Device Criticality	By default, Device Criticality is set as one of the following, as described in Using Device Criticality. • Undefined • Non-critical • Low • Medium • High	✓	✓	✓	✓	✓	✓	✓	✓	✓

Rule name	Description	SCCM	ServiceNow	Tachyon	OracleLMS	BigFix	BigFixInv	Intune	vCenter	WSUS
	• Critical.									
Device Domain Name	Domain the device is installed on.	✓	✓	✓			✓			
Device Inventory date	Date that the device was last updated.	✓	✓	✓	✓			✓	✓	✓
Device Matched Device Type	Normalized device type based on chassis type. For example **Desktop**.	✓	✓	✓	✓	✓		✓	✓	✓
Device Matched Family	Normalized family of the device. For example, **Aspire**.	✓	✓	✓	✓	✓			✓	
Device Matched Model	Normalized model of the device. For example, **A30**.	✓	✓	✓	✓	✓		✓	✓	✓
Device Matched Socket count	Normalized socket count of the device. For example, **1**.	✓	✓	✓	✓	✓		✓	✓	✓
Device Matched Vendor	Normalized vendor name of the device. For example, **Acer Inc.**.	✓	✓	✓	✓	✓		✓	✓	✓

Rule name	Description	SCCM	ServiceNow	Tachyon	OracleLMS	BigFix	BigFixInv	Intune	vCenter	WSUS
Device Netbios Domain name	NetBIOS version of the device's domain name.	✓	✓	✓						
Device Netbios Name	NetBIOS version of the device name.	✓	✓	✓					✓	
Device OS	The normalized product title of the OS that is running on the device.	✓	✓	✓		✓	✓		✓	
Device Purchase date	Date that the device was purchased.	✓	✓							
Device Serial	Serial number of the computer.	✓	✓				✓	✓		
Device User Primary Username	The primary user of the device.	✓		✓						
OU Name (Deprecated)	Name of the OU that the device is in. For example **Sales**. **Note** All OUs with the same name will be used,	✓	✓							

Rule name	Description	SCCM	ServiceNow	Tachyon	OracleLMS	BigFix	BigFixInv	Intune	vCenter	WSUS
	therefore the **OU Path** rule should be used instead. The **OU Name** rule is deprecated and should be re-defined using **OU Path**. This rule is deprecated, which means it will continue to work until it is removed in a future version of Tachyon.									
OU Path	The name or path of the OU location in the AD hierarchy, using pipe | as the delimiter. For example, to get all the computers in **OU=Sales, OU=Workstations, DC=acme, DC=local** you can either specify **Sales** or - if there is more than one OU called **Sales** in the AD structure - specify the whole path **acme.local|Workstations|Sales**. Note that the DC and OU parts of a distinguished name are treated differently.	✓	✓							

Rule name	Description	SCCM	ServiceNow	Tachyon	OracleLMS	BigFix	BigFixInv	Intune	vCenter	WSUS
Processor Matched Chip Module Count	Normalized chip module count of the processor. For example, **1**.	✓	✓	✓	✓	✓				
Processor Matched Core Count	Normalized core count of the processor. For example, **2**.	✓	✓	✓	✓	✓			✓	
Processor Matched Family	Normalized family name of the processor. For example, **Athlon 64 X2**.	✓	✓	✓	✓	✓			✓	
Processor Matched Model	Normalized model name of the processor. For example, **3250e**.	✓	✓	✓	✓	✓			✓	
Processor Matched Processor Type	Normalized type of the processor. For example, **Desktop**.	✓	✓	✓	✓	✓			✓	
Processor Match	Normalized release date of the processor. For example, **31-03-2008**.	✓	✓	✓	✓	✓			✓	

Rule name	Description	SCCM	ServiceNow	Tachyon	OracleLMS	BigFix	BigFixInv	Intune	vCenter	WSUS
ed Release Date										
Processor Matched Speed MHz	Normalized speed of the processor. For example, **2.100**.	✓	✓	✓	✓	✓			✓	
Processor Matched Threads per Core	Normalized threads per core of the processor. For example, **1**.	✓	✓	✓	✓	✓			✓	
Processor Matched Vendor	Normalized vendor name of the processor. For example, **Advanced Micro Devices, Inc**.	✓	✓	✓	✓	✓			✓	
Product Catalog Colloquial Version	Software colloquial version contained in the inventory source. For example, **2012**. **Note** This will usually be blank.	✓	✓				✓	✓		
Product Catalo	Software edition contained in the inventory source. For example, **Standard**. **Note**	✓	✓	✓			✓	✓		

Rule name	Description	SCCM	ServiceNow	Tachyon	OracleLMS	BigFix	BigFixInv	Intune	vCenter	WSUS
g Edition	This will usually be blank in SCCM unless the relevant MOF extensions have been installed.									
Product Catalog Is Partial Version Matched	Flag that indicates whether the software title was partial matched or not (TRUE/**1**) or not (FALSE/**0**).	✓	✓	✓	✓	✓	✓	✓		
Product Catalog Matched Colloquial Version	Normalized software colloquial version. For example, **2016**.	✓	✓	✓	✓	✓	✓	✓		
Product Catalog Matched Edition	Normalized software edition. For example, **Standard**.	✓	✓	✓	✓	✓	✓	✓		
Product Catalog	Normalized software end of support date that of that	✓	✓	✓	✓	✓	✓	✓		

Rule name	Description	SCCM	ServiceNow	Tachyon	OracleLMS	BigFix	BigFixInv	Intune	vCenter	WSUS
Matched End of Support	version. For example, **31-10-2008**.									
Product Catalog Matched is Bundle	Flag indicating whether the normalized software is a bundle (TRUE/**1**) or not (FALSE/**0**).	✓	✓	✓	✓	✓	✓	✓		
Product Catalog Matched Is License Required	Flag indicating whether that normalized software title requires a license (TRUE/**1**) or not (FALSE/**0**).	✓	✓	✓	✓	✓	✓	✓		
Product Catalog Matched Release Date	Normalized software release date of that version. For example, **31-10-2008**.	✓	✓	✓	✓	✓	✓	✓		
Product Catalog Match	Normalized software title. For example, **Office**.	✓	✓	✓	✓	✓	✓	✓		

Rule name	Description	SCCM	ServiceNow	Tachyon	OracleLMS	BigFix	BigFixInv	Intune	vCenter	WSUS
ed Title										
Product Catalog Matched Vendor	Normalized software vendor name. For example, **Microsoft Corporation**.	✓	✓	✓	✓	✓	✓	✓		
Product Catalog Matched Version	Normalized software version. For example, **10.2.233**.	✓	✓	✓	✓	✓	✓	✓		
Product Catalog Title	Software title contained in the inventory source. For example, **Office Standard en_pack**.	✓	✓	✓	✓	✓	✓	✓		
Product Catalog UN Standard Product Service Code	UNSPC code of the normalized software title.	✓	✓	✓	✓	✓	✓	✓		
Product Catalo	Software vendor name contained in the inventory	✓	✓	✓		✓	✓	✓		

Rule name	Description	SCCM	ServiceNow	Tachyon	OracleLMS	BigFix	BigFixInv	Intune	vCenter	WSUS
g Vendor	source. For example, **Microsoft**.									
Product Catalog Version	Software version number contained in the inventory source. For example, **10.2.233**.	✓	✓	✓	✓	✓	✓	✓		
Product Install Date	Date that software installation was installed according to the inventory source.	✓		✓						
Product Instance Name	Instance name if used by a product, for example **MSSQLSERVER** for SQL Server.	✓	✓	✓	✓	✓				
Product Last Used date	Date that software installation was last run according to the inventory source.	✓		✓						
Product Usage Category	Usage category assigned to a specific installation of a normalized software title. Potential categories are: - Used - Unused - Rarely used - Unreported	✓	✓	✓	✓					

1.11.12 Tachyon Product Packs reference

Reference information for Product Packs included in the Tachyon Platform zip. These Tachyon Platforms are required to support various features of Tachyon.

The Tachyon Platform zip is downloaded from the 1E Support Portal https://support.1e.com/. Additional Product Packs are available from 1E Exchange (1E Exchange) that are not documented here.

- **Classic Product Packs** contain instructions, for use in Explorerand other Tachyon applications.
- **Integrated Product Packs** contain policies, rules and fragments for use by Guaranteed State, and may also include instructions.

Note

You can create your own platform instructions using SCALE.

SCALE is a powerful, lightweight, cross-platform programming language which combines 1E Client Methods and Modules with SQL commands to enable you to create questions, actions, preconditions, checks, and fixes that can automate almost anything on a Windows, Linux or macOS device.

Refer to 1E SDK.

1.11.12.1 1E ConfigMgrConsoleExtensions product pack

Classic Product Pack used to create the **1E ConfigMgrConsoleExtensions** instruction set required by the Tachyon Configuration Manager console extensions. For more details please refer to:

- Preparing for the Tachyon extensions for the Configuration Manager Console.
- Using Tachyon in Configuration Manager

1.11.12.1.1 Instructions

Instruction text (ReadablePayload)	Type	Description	Instruction file name	Version
What is the health of the SCCM clients (checking inventory has run and policy has been evaluated in the last <numdays> days)?	Question	Evaluates the ConfigMgr Client health on the device over the last <numdays> days. The health will be	**1E-ConfigMgrConsoleExtensions-ClientHealth**	17

Instruction text (ReadablePayload)	Type	Description	Instruction file name	Version
		reported as 'Poor' if it has not updated any one of the three time critical items. If all updated then they are considered 'Average' if two thirds of all the checks are ok, and 'Good' if everything is within expected parameters. This instruction makes use of a PowerShell script and will only work on Windows devices.		
What components are installed on the SCCM clients?	Question	Returns all the SCCM client components installed on the	**1E-ConfigMgrConsoleExtensions-InstalledComponents**	17

Instruction text (ReadablePayload)	Type	Description	Instruction file name	Version
		device. This instruction makes use of a PowerShell script and will only work on Windows devices.		
What Management Points are the SCCM clients using?	Question	Returns the ConfigMgr management points configured on the device. This instruction makes use of a PowerShell script and will only work on Windows devices.	**1E-ConfigMgrConsoleExtensions-ManagementPoint**	17
Enable and start the ConfigMgr client service (CcmExec) with a stagger of <limitSecs> seconds.	Question	Enables and starts the ConfigMgr client service (CcmExec). The service start will	**1E-ConfigMgrConsoleExtensions-StartConfigMgrClientService**	14

Instruction text (ReadablePayload)	Type	Description	Instruction file name	Version
		be delayed by a number of seconds up to the specified stagger value.		
Emergency stop and disabling of the ConfigMgr client service (CcmExec).	Question	Stops and disables the ConfigMgr client service (CcmExec).	**1E-ConfigMgrConsoleExtensions-StopConfigMgrClientService**	14
Trigger ConfigMgr client application deployment evaluation cycle with a stagger of <limitSecs> seconds.	Action	Triggers the application deployment evaluation cycle. This trigger will be delayed by a number of seconds up to the specified stagger value.	**1E-ConfigMgrConsoleExtensions-TriggerApplicationDeploymentEvaluationCycle**	14
Trigger ConfigMgr client health check and remediation with a stagger	Action	Trigger a client health check and remediation. This	**1E-ConfigMgrConsoleExtensions-TriggerClientHealthCheck**	15

Instruction text (ReadablePayload)	Type	Description	Instruction file name	Version
of <limitSecs> seconds.		trigger will be delayed by a number of seconds up to the specified stagger value.		
Trigger ConfigMgr client discovery data collection cycle with a stagger of <limitSecs> seconds.	Action	Trigger the discovery data collection cycle. This trigger will be delayed by a number of seconds up to the specified stagger value.	**1E-ConfigMgrConsoleExtensions-TriggerDiscoveryDataCollectionCycle**	14
Trigger a ConfigMgr client file collection cycle with a stagger of <limitSecs> seconds.	Action	Trigger a file collection cycle. This trigger will be delayed by a number of seconds up to the specified stagger value.	**1E-ConfigMgrConsoleExtensions-TriggerFileCollectionCycle**	14

Instruction text (ReadablePayload)	Type	Description	Instruction file name	Version
Trigger a ConfigMgr client hardware inventory cycle with a stagger of <limitSecs> seconds.	Action	Trigger a hardware inventory cycle. This trigger will be delayed by a number of seconds up to the specified stagger value.	**1E-ConfigMgrConsoleExtensions-TriggerHardwareInventoryCycle**	14
Trigger a ConfigMgr client machine policy retrieval and evaluation cycle with a stagger of <limitSecs> seconds.	Action	Trigger a machine policy retrieval and evaluation cycle. This trigger will be delayed by a number of seconds up to the specified stagger value.	**1E-ConfigMgrConsoleExtensions-TriggerMachinePolicyRetrievalAndEvaluationCycle**	14
Trigger a ConfigMgr client software inventory cycle with a stagger of <limitSecs> seconds.	Action	Triggers the software inventory cycle. This trigger will be delayed by a	**1E-ConfigMgrConsoleExtensions-TriggerSoftwareInventoryCycle**	14

Instruction text (ReadablePayload)	Type	Description	Instruction file name	Version
		number of seconds up to the specified stagger value.		
Trigger a ConfigMgr client software metering usage report cycle with a stagger of <limitSecs> seconds.	Action	Trigger a software metering usage report cycle. This trigger will be delayed by a number of seconds up to the specified stagger value	**1E-ConfigMgrConsoleExtensions-TriggerSoftwareMeteringUsageReportCycle**	14
Trigger a ConfigMgr client software update deployment evaluation cycle with a stagger of <limitSecs> seconds.	Action	Triggers a software update deployment evaluation cycle. This trigger will be delayed by a number of seconds up to the specified stagger value.	**1E-ConfigMgrConsoleExtensions-TriggerSoftwareUpdatesDeploymentEvaluationCycle**	14

Instruction text (ReadablePayload)	Type	Description	Instruction file name	Version
Trigger a ConfigMgr client software update scan cycle with a stagger of <limitSecs> seconds.	Action	Triggers a software update scan cycle. This trigger will be delayed by a number of seconds up to the specified stagger value.	**1E-ConfigMgrConsoleExtensions-TriggerSoftwareUpdatesScanCycle**	14
Triggers a ConfigMgr client Windows installer source list update cycle with a stagger of <limitSecs> seconds.	Action	Triggers a Windows installer source list update cycle. This trigger will be delayed by a number of seconds up to the specified stagger value.	**1E-ConfigMgrConsoleExtensions-TriggerWindowsInstallerSourceListUpdateCycle**	14

1.11.12.2 1E Experience product pack

Classic product pack used to create the **1E Experience** instruction set in Tachyon, required by the Experience features of the Device View.

1.11.12.2.1 Instructions

This product pack contains Server instructions.

Server instructions are special type of instruction, which cannot be run in Explorer. They are for internal use only, run on the server, and used to carry out on-demand or scheduled processing of data across various

datasources, such as SQL databases. For example, the Dashboards app uses them to populate tiles and charts with data from Tachyon Master and Experience databases.

1.11.12.3 1E Explorer TachyonAgent product pack

Classic Product Pack used to create the **1E Explorer TachyonAgent** instruction set that can be used to configure and query Tachyon clients.

Please refer to:

- Explorer - Using Device Criticality about instructions used to get and set **Criticality** devices
- Explorer - Using Location about instructions used to get and set **Location** on devices
- Explorer - Tachyon Activity Record about instructions used to configure 1E Client configuration settings for Tachyon Agent inventory

1.11.12.3.1 Instructions

Instruction text (Readable Payload)	Type	Description	Instruction file name	Version
What is the Tachyon Agent's connection summary?	Question	Retrieves connectivity diagnostic information from Tachyon Agents.	**1E-Explorer-TachyonAgent-AgentConnectionDiagnostics**	11
What is the Tachyon Agent diagnostic information detail?	Question	Get live diagnostic information from Tachyon Agents.	**1E-Explorer-TachyonAgent-AgentDiagnostics**	11
What is the Tachyon Agent instruction	Question	Retrieves instruction execution diagnostic information from Tachyon Agents.	**1E-Explorer-TachyonAgent-AgentExecutionDiagnostics**	11

Instruction text (Readable Payload)	Type	Description	Instruction file name	Version
execution summary?				
Which devices are connected to which Tachyon Switches?	Question	Get Switch connection information for each device.	**1E-Explorer-TachyonAgent-AgentSwitchConnections**	11
How many 1E Clients are installed?	Question	Returns a count of each version of 1E Client installed.	**1E-Explorer-TachyonAgent-AgentVersionCount**	11
Disable 1E Client process usage inventory collection	Action	Disables process usage inventory collection. This only affects Windows devices, and will take up to the 1E Client configuration setting 'ConnectionRetryTimeInSecondsMax' to take effect. Please refer to Tachyon Activity Record.	**1E-Explorer-TachyonAgent-DisableProcessUsage**	4
Echo message <msg>	Question	Send an echo request to devices	**1E-Explorer-TachyonAgent-Echo**	11
Enable 1E Client process usage inventory collection	Action	Enables process usage inventory collection. This only affects Windows devices, and will take up to the 1E Client configuration setting 'ConnectionRetryTimeInSecondsMax' to take effect. .Tachyon Activity RecordPlease refer to	**1E-Explorer-TachyonAgent-EnableProcessUsage**	4
What are the modules and providers	Question	Get a list of modules and providers registered with each 1E Client.	**1E-Explorer-TachyonAgent-Extensibility**	11

Instruction text (Readable Payload)	Type	Description	Instruction file name	Version
reported by the 1E Client Extensibility Update?				
What are the 1E Client settings?	Question	Returns values of settings configured on the 1E Client. This instruction makes use of a PowerShell script and will only work on Windows devices. Uses **getConfig.ps1** script to get the following subset of configuration settings for the Tachyon client: • AuthenticationPolicy • BackgroundChannelUrl • ConnectionKeepaliveTimeInSecondsMax • ConnectionKeepaliveTimeInSecondsMin • ConnectionRetryTimeInSecondsMax • ConnectionRetryTimeInSecondsMin • ConnectionTimeout • CRLChecks • CRLTimeoutInSeconds • DefaultStaggerRangeSeconds • EnablePayloadCompression • LoggingLevel • NomadContentDownloadEnabled • NomadContentDownloadTimeoutSecs • Switch	**1E-Explorer-TachyonAgent-GetAgentConfigValues**	14

Instruction text (Readable Payload)	Type	Description	Instruction file name	Version
		• WorkerThreads Please refer to Tachyon client settings.		
What 1E Client Windows settings are configured for historical data collection for the <source> capture source?	Question	Return the 1E Client configuration settings for Tachyon Agent inventory. The 1E Client configuration settings are read to determine if a supplied inventory source is enabled or disabled. Allowable inventory sources are DNS, Process, Software and TCP. Response speed will be affected by the 1E Client setting 'DefaultStaggerRangeSeconds'. Windows devices only. Uses **getInventoryConfig.ps1** script. .Tachyon Activity RecordPlease refer to	**1E-Explorer-TachyonAgent-GetAgentHistoricDataCaptureConfig**	15
What is the criticality of my devices?	Question	Retrieves the criticality of a device.	**1E-Explorer-TachyonAgent-GetCriticality**	4
Get the location of my devices	Question	Gets the location of a device. This instruction retrieves the device static location information.	**1E-Explorer-TachyonAgent-GetLocation**	4
What are the statistics for previously executed instructions?	Question	Returns statistics for previously executed instructions.	**1E-Explorer-TachyonAgent-InstructionStatistics**	11

Instruction text (Readable Payload)	Type	Description	Instruction file name	Version
Trigger client reinstallation for targeted devices using <ClientVersion> supplying switch name of <switch> and a background channel url of <backgroundchannel url>	Action	Triggers 1E Client uninstallation followed by an installation via scheduled task for targeted devices. Will use the existing switch and port information (3.0 and above). Only supported on Windows. Uses installers uploaded to the 1E Client installer page within Configuration under the Settings app. Uses **TachyonAgentReinstallation.ps1** script.	**1E-Explorer-TachyonAgent-ReinstallationOfAgent**	27
Set a 1E Client configuration property <agentconfig> to <agentconfigvalue> for the Tachyon Agent	Action	Set a 1E Client configuration property for the Tachyon Agent. Please note this can and will replace anything found, and can cause the Agent to stop responding. This instruction is for Windows devices only. Uses **setConfig.ps1** script to set the same subset of configuration settings for the Tachyon client as the #UUIDaa6bde5719524cf774d047e5d9ef37e8_id_id1EExplorerTachyonAgentproductpack1EExplorerTachyonAgentGetAgentConfigValues instruction above.	**1E-Explorer-TachyonAgent-SetAgentConfigValue**	14
Set the criticality of my devices to	Action	Sets the criticality of a device.	**1E-Explorer-TachyonAgent-SetCriticality**	4

Instruction text (Readable Payload)	Type	Description	Instruction file name	Version
<criticality>				
Set the location of my devices to <location>	Action	Sets the location of a device. This instructions set the device static location information.	**1E-Explorer-TachyonAgent-SetLocation**	4
Check for 1E Client updates and apply them	Action	Instructs the 1E Client to check for extensibility updates and apply them. Supports Windows, Linux, Solaris and Android.	**1E-Explorer-TachyonAgent-UpdateExtensibility**	11
Trigger 1E Client upgrade to <ClientVersion> for targeted devices	Action	Triggers 1E Client upgrade via scheduled task for targeted devices. Will use the existing switch and port information (3.1 and above). Only supported on windows 7 and above. Uses installers that are uploaded to the 1E Client installer page within Configuration under the Settings app. Note the build numbers must match between the instruction parameters and the version specified in the 1E Client installer page. Uses **TachyonAgentUpgrade.ps1** script.	**1E-Explorer-TachyonAgent-UpgradeAgent**	29

1.11.12.4 1E Inventory product pack

Classic Product Pack used to create the **1E Inventory** instruction set required by the **Tachyon Powered Inventory** feature.

For more details please refer to Tachyon connector.

1.11.12.4.1 Instructions

<table>
<tr><th>Instruction text (ReadablePayload)</th><th>Type</th><th>Description</th><th>Data to Sync category</th><th>Instruction file name</th><th>Version</th></tr>
<tr><td>Which processors are in the device? With a stagger of <limitSecs> seconds.</td><td>Question</td><td>Processor details

Uses Device.GetProcessors method.

Note
Click here to expand details of data collected...

<table><tr><td>Method</td><td>GetProcessors</td></tr><tr><td>Library</td><td>Core</td></tr><tr><td>Action</td><td>Retrieves information about the CPUs plugged in to the motherboard of the device.</td></tr><tr><td>Parameters</td><td>(None)</td></tr><tr><td>Return values</td><td>Vendor (string): The vendor of the processor

Name (string): The vendor-defined name of this processor package

CoreCount (int): The number of cores inside this package

SpeedMhz(int): The clock speed of the processor in its current operating mode</td></tr></table></td><td>Processor</td><td>1E-Inventory-Device-GetProcessors</td><td>3</td></tr>
</table>

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		From v5.1 onwards these columns also appear : *LogicalCoreCount* (int) : The number of logical cores inside this package *Hyperthreading* (bool): Indicates whether the cores are hyperthreaded, true for yes, false for no.			
	Example	`Device.GetProcessors();`			
	Platforms	• Windows • Linux • MacOS • Solaris Intel • Solaris Sparc			
	Notes	*Name* is the immutable string that the CPU reports to SMBIOS. This often contains the publicly marketed and sold average speed of the CPU, which usually differs to the actual speed of the processor instance. *SpeedMhz* on Windows can change over time for one particular CPU.			

Instruction text (ReadablePayload)	Type	Description		Data to Sync category	Instruction file name	Version
			Modern CPU's can adjust their clock in response to heat and power from moment to moment. This parameter cannot be relied upon for scoping future instruction executions unless some kind of range of values is in the scope to cope with natural speed variance.			
Inventory - what is the summary of file usage since <startDate>? With a stagger of <limitSecs> seconds.	Question	Process Usage data inventory for SLA Uses the **$ProcessUsage_Daily** inventory table, if **Module.Inventory.ProcessUsage.Enabled** setting is true (default) in the 1E Client configuration file. Please refer to 1E Client - Tachyon client settings: Capture source settings. **Note** Click here to expand details of data collected... Windows only. The following table shows fields available in the **$ProcessUsage_Daily** table.		Software Usage	**1E-Inventory-FileUsageSummary**	3

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version

Field	Data type	Description	Sample value	Tables
CommandLine	string	This is a string of	C:\Program Files\Git\mingw64\libexec\git-core\git-credential-manager.exe	

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		the command used to launch that instance,			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		mostprobablythefirstone.Itwillnotco			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		n t a i n a n y d i f f e r e n c e s i f o t h e r i n s t a n c e s			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		arelaunchedwithhaslightlydifferentco			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		mandline. It is an indication of a typical			

Instruction text (ReadablePayload)	Type	Description				Data to Sync category	Instruction file name	Version
				command line for this instance.				
		Durati	integer	The enum	1			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
	on	error of minutes covered by the individual ex			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		execution(s) of at least one instance of thi			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		sexecutable. Duration cannever be more t			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		han1440minutes,beingthenumberofminu			

Instruction text (ReadablePayload)	Type	Description				Data to Sync category	Instruction file name	Version
				testing a day.				
		ExecutableHash	string	The MD5 hash of the binary that	ad3ec70ae9e82582bdf6aa6fd5811376			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		t c o n t a i n s t h e e n t r y p o i n t (u s u a l l y a n e x			

Instruction text (ReadablePayload)	Type	Description			Data to Sync category	Instruction file name	Version
				e)			
		ExecutableName	string	The name of the binary that contains the	git-credential-manager.exe		

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		entrypoint to obtain ed from ms tamped ver si			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		on information where possible, the file n			

Instruction text (ReadablePayload)	Type	Description				Data to Sync category	Instruction file name	Version
				ameifnot.				
		ExecutableSize	integer	The size of the binary that is	131168			

Instruction text (ReadablePayload)	Type	Description				Data to Sync category	Instruction file name	Version
				ashedbelow				
		ExecutableVersion	string	The version information sta	1.5.0.0			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		mpedintotheexecutablewhereravailabl			

Instruction text (ReadablePayload)	Type	Description			Data to Sync category	Instruction file name	Version
				e.			
		ExecutionCount	integer	The number of instances observed during the	2		

Instruction text (ReadablePayload)	Type	Description				Data to Sync category	Instruction file name	Version
				ngthe Duration period				
		IsOSProcess	integer	Avalueof1indica	0			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		testthatthisiscategorisedasanoperati			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		ngsystembythe rulesinplace. Avalueof0			

Instruction text (ReadablePayload)	Type	Description			Data to Sync category	Instruction file name	Version
				indicates that it is not.			
		LastSeen	integer	The UTC Time sta	1526982245		

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		mpofwhenthelastinstanceoftheexecuta			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		b l e (o f a l l t h e a c c u m u l a t e d s u b j e c t s o f t h			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		is record) was last seen (polling) or actu			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		already existed (events). While starting any instanc			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		e i s r u n n i n g , f o r t h e c u r r e n t d a y r e c o r d s ,			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		Last Seen will create pacross the day and dur			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		ationwillincreaseastimepassesifthep			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		rocessremainsrunning. Oncemidnightis			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		crossed the end the daily record s for ory yes ter r			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		daysare'closedoff'bysettingLastSeen=			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		TS+864000(thenumberofsecondsinaday),			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		which is midnight of the next day. If all in			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		stancesofonebinaryarreexitedandneverer			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		running in that day, then the Last Seen field			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		dforthatdailyrecordshouldd'stick'ato			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		never value and never revert change again. Inot			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		herwordsthemaximumdifferencebetween			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		TSandLastSeeninasinglerowisatmost86			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		400, being the number of seconds in a day.			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		Tracking of an execution summary from one			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		day to another ("carry-over") can be achi			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		evedbylookingforarecordbasedonTS tom			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		or row = LastSeen today with all the other rk			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		eyinformationthesameey. Ifthatexactkey			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		record with the 'carryover' conditionsi			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		snotfoundthenthepprocessdidnotthheore			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		tically continue across smidnight. Note t			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		hatapprocesstthatdiesafter23:59:00and			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		starts before 00:01:00 the next day will			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		p p e a r t o b e a c o n t i n u o u s p r o c e s s i n t h e s u m			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		mary tables. Event hought could the oret			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		ically have stopped for near ly two minute e			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		s. This is is because the resolution of the eta			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		bleibt stehen, bis der Vorgang abgeschlossen ist.			

Instruction text (ReadablePayload)	Type	Description				Data to Sync category	Instruction file name	Version
				currredin.				
		TS	integer	When the record was added to	1526947200			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		hetable.SeeTimestamps.MidnightUTCth			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		atisthestartdayofthe24hourscoveredb			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		y t h i s r e c o r d .			
		The Tachyon client captures executable usage; this is from the moment the executable is turned into a process, hence the process usage. The Process Usage data presented is grouped by executable binary, and parallel runs are accumulated in the ExecutionCount, but not in the Duration, where coverage time period is desired instead.			
Inventory - what software is installed? With a stagger of <limitSecs> seconds.	Question	Software inventory for SLA Uses a combination of: • Software.GetInstallations method • Software.GetUserInstallations method • SQL Server registry values **Note** Click here to expand details of data collected...	Installed Software	**1E-Inventory-Software**	3

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		Method	**GetInstallations**		
		Module	Software		
		Library	Core		
		Action	Gets a list of the installed software available to all users, optionally filtered by product and/or publisher.		
		Parameters	*Product* (string; optional): If specified, search for just this product. *Publisher* (string; optional): If specified, get just this publisher's software.		
		Return values	A table of: • – *Product* (string): The product name. – *Publisher* (string): The publisher of the product. – *Version* (string): The		

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		version of the product. – *InstallDate* (string): If available, when the product was installed. – *Architecture* (string): Platform architecture of this installation (e.g. x86, x64)			

		Example
		Get all software:
		`Software.GetInstallations();`
		Find and remove all installed instances of Calculator Plus:
		`Software.GetInstallations( Publisher : "Microsoft", Product : "Microsoft Calculator Plus");`
		`evaluate;`
		`Agent.Echo( Message: "Is installed");`
		`Software.Uninstall( Publisher : "Microsoft", Product : "Microsoft Calculator Plus");`			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version

		To select a specific version, use a SQL WHERE clause:
		`@installs = Software.GetInstallations( Publisher : "Microsoft", Product : "Office Professional");`
		`SELECT DISTINCT * FROM @installs WHERE Version LIKE "16.0%";`			

		Platforms • Windows • Linux • MacOS • Solaris Intel • Solaris Sparc • Android			
		Notes To find additional software installed for specific users, use Software.GetUserInstallations.			
	Method	**GetUserInstallations**			
	Li	Core			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
	b r a r y				
	A c t i o n	Gets a list of the software installed for specific users, optionally filtered by product and/or publisher.			
	P a r a m e t e r s	*Product* (string; optional): If specified, search for just this product. *Publisher* (string; optional): If specified, get just this publisher's software.			
	R e t u r n v a l u e s	A table of: • – *Architecture* (string): Platform architecture of this installation (e.g. x86, x64) – *InstallDate* (string): If available, when the product was installed.			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		– *Product* (string): The product name. – *Publisher* (string): The publisher of the product. – *Sid* (string): The user identifier for whom this software has been installed. – *Username* (string): Friendly representation of the *Sid* - this will only be resolved locally. – *Version* (string): The version of the product.			
	Example	Get all user specific software: `Software.GetUserInstallations();`			
	Platforms	• Windows			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
	Notes	• *Sid* resolution may fail as this method will not go over the wire. In this case Username will be NULL. • The file modified and accessed time attributes of the NTUSER.dat directory entries under the %USERPROFILE% folder for each user and service principal might be updated to some time during the execution of this method. This is a side effect of loading and unloading the user hive and is housekeeping performed by Windows, not the 1E Client. This can cause "unused" profiles to appear to be used if the modified times are employed to determine whether a user has logged in, which is not a reliable method of establishing this fact. • This method reads user uninstall registry keys from HKU, but will not load hives. • Installs for this function are retrieved from *HKU:\<SID>\Software\Microsoft\Windows\CurrentVersion\Uninstall*			

<table>
<tr><th>Instruction text (ReadablePayload)</th><th>Type</th><th>Description</th><th>Data to Sync category</th><th>Instruction file name</th><th>Version</th></tr>
<tr><td>Inventory - summary of which users have logged on since <startDate>? With a stagger of <limitSecs> seconds.</td><td>Question</td><td>User data inventory for SLA

Uses the $UserUsage_Daily inventory table, if Module.Inventory.UserUsage.Enabled setting is true (default) in the 1E Client configuration file. Top Console User is also calculated from this table.

Please refer to 1E Client - Tachyon client settings: Capture source settings.

Note
Click here to expand details of data collected...
Windows only. The following table shows fields available in the $UserUsage_Daily table.

<table><tr><th>Field</th><th>Data type</th><th>Description</th><th>Sample value</th><th>Tables</th></tr><tr><td>Duration</td><td>integer</td><td>The enumber</td><td>12</td><td>• $UserUsag</td></tr></table></td><td>User</td><td>1E-Inventory-UserUsageSummary</td><td>3</td></tr>
</table>

Instruction text (ReadablePayload)	Type	Description			Data to Sync category	Instruction file name	Version
			of minutes covered by the individual user	e_Daily			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		session(s) of at least one instance of thi			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		slogin. Duration cannever be more than 14			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		40 minutes, being the enumber of minutes in			

Instruction text (ReadablePayload)	Type	Description				Data to Sync category	Instruction file name	Version
				aday.				
		Email	string	The email address that is cached in	abrown@acme.org	• $UserUsage_Daily		

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		these system for this user. This may not nece			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		ssarilybetheemailaddressstousesetoccont			

Instruction text (ReadablePayload)	Type	Description				Data to Sync category	Instruction file name	Version
		activ the user service account for the email.						
FirstN	string	The for	Alice	• $User				

Instruction text (ReadablePayload)	Type	Description			Data to Sync category	Instruction file name	Version
		name	enamethatthesystemhascachedforthesus	sage_Daily			

Instruction text (ReadablePayload)	Type	Description			Data to Sync category	Instruction file name	Version
		er.					
	LastName	string	The surname that the system has cache	Brown	• $UserUsage_Daily		

Instruction text (ReadablePayload)	Type	Description				Data to Sync category	Instruction file name	Version
		for the user						
	LastSeen	integer	The UTC Timestamp of when the	1526990846	• $UserUsage_Daily			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		elastinstanceoftheusersessionon(ofall			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		the accumulated subjects of this record)			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		was last seen (polling) or actually existe			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		d(events), rounded down to the start of the			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		e m i n u t e i n w h i c h t h e e v e n t o c c u r r e d . W h i l			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		stanysessionisinprogress,forthecurr			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		entdayrecordss,LastSeenwillcreepacro			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		s s t h e d a y a n d t h e d u r a t i o n w i l l i n c r e a s e a			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		stimepassessiftheuserremainsloggedin			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		.That is Duration and Last Seen will incre			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		a s e e a c h t i m e y o u q u e r y t h e t a b l e (w i t h a t l			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		east a minute between queries). Once a min			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		ightisscrossedthenthedailyrecordsfor			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		yesterdayarre'closedoff'bysettingLas			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		t S e e n = T S + 8 6 4 0 0 (t h e n u m b e r o f s e c o n d s i n			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		aday), whichismidnightoftheneextday.			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		If all users sessions for one user are exit			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		e d a n d n e v e r o c c u r a g a i n t h a t d a y , t h e n t h e			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		LastSeenfieldfortharthatdailyrecordshou			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		Id'stick'atonevalueandnevereverchan			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		geagain. Inotherwordsthemaximumdiffe			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		r e n c e b e t w e e n T S a n d L a s t S e e n i n a s i n g l e r			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		owisatmost86400,beingthenumberofsec			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		ondsinadday.Trackingofausersessionsu			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		mmaryfromonedaytoanotherr("carry-ove			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		r"). can be achieved by looking for a record			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		based on TS to mor row = Last Seen to day with			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		all the other key information on the same. If			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		that exact key record with the 'carryover'			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
' condition is not found then the user ses					

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		sionditdnotththeoretically continueacro			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		ssmidnight. Note that a session that ate exit			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		safter23:59:00andstartsagainbefore0			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		0:01:00 then next day will appear to be acon			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		tinuoususersessionintheesummarytable			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		s. Even though it could theoretically have v			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		e n o t e x i s t e d f o r n e a r l y t w o m i n u t e s . T h i s			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		is because the resolution of the table is

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		other start of the minute the event occurre			

Instruction text (ReadablePayload)	Type	Description				Data to Sync category	Instruction file name	Version
				din. See Timestamps.				
		SID	string	The Windows NT SID of	S-1-5-21-xxx-yyyy-	• $UserUsage_Daily		

Instruction text (ReadablePayload)	Type	Description					Data to Sync category	Instruction file name	Version
				the user.	zzz				
		TS	integer	When the record was added to the	1526947200	• $UserUsage_Daily			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		table. See Timestamps.			
Username	string	The user account	alice bacme\Alice B	• $UserUsage_Dai	

Instruction text (ReadablePayload)	Type	Description				Data to Sync category	Instruction file name	Version
			ame, with a domain prefix if applicable.	rown	ly			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		For Windows devices not a in a domain, the '			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		domain' is the local machine name. For non			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		-Windowsdevicessuchas Linuxthereisno			

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
		domain part. The Tachyon client captures user sessions (usage); this is from the moment the user instigates a login/logout, hence User Usage. The usage data presented is grouped by SID and Username, and parallel login durations are really the coverage of the time period, not the total time for all the individual sessions. User and administrator accounts are included, either local or remote. System accounts, and accounts used to run services, are excluded.			
Returns patch status for 1E Inventory consumption, staggering for <limitSec	Question	Returns patch status for 1E Inventory consumption	Patch	**1E-PatchSuccess-PatchStatus**	5.0

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
s> seconds.					
Tip The **1E-PatchSuccess-PatchStatu**					

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
s i n s t r u c t i o n i s n o t r e q u i r e d i f y o u d o n o t					

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
intendtousethePatchSuccessapplicati					

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
on, and will not run unify you do not have valid ice					

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
nsforPatchSuccess.Formoreinformati					

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
onaboutconfiguringPatchSuccessplease					

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
e r e f e r t o C o n f i g u r i n g P a t c h S u c c e s s . **W a r n i**					

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
ng This instruction is part of this **1E** **Inv**					

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
entory instructionsetusedbythe Tachyo					

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
nConnector.Donotmoveittothe**1E** **Patch**					

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
Success instructions set used by the bubutt					

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
onsvisibleinthePatchSuccessapplicat					

Instruction text (ReadablePayload)	Type	Description	Data to Sync category	Instruction file name	Version
ion.					

1.11.12.5 1E Nomad product pack

Classic product pack used to create the **1E Nomad** instruction set in Tachyon, required by the following Nomad features:

- Downloads tab on Device views - instructions used to populate details about Content download and other Nomad features
- Nomad Download Pause - instructions used by the CM Admin Console extensions
- Instructions to help with the following Nomad features: Nomad cache, CacheCleaner, Single Site Download, Nomad jobs, NomadBranch service.

1.11.12.5.1 Instructions

Nomad feature	Instruction text (ReadablePayload)	Type	Description	FileName	Version
Nomad cache Nomad jobs	**Get the percentage of content %ContentId% in the local Nomad cache**	Question	Get the percentage of the specified content in the local Nomad cache.	**1E-Nomad-CachedPkgStatus**	8
Nomad cache	**Clean the SCCM and Nomad cache for an application %packageId%**	Action	Cleans the SCCM and Nomad	**1E-Nomad-CleanNomadCacheForApplication**	16

Nomad feature	Instruction text (ReadablePayload)	Type	Description	FileName	Version
CacheCleaner Nomad jobs			cache for an application with the specified package ID. This package ID is the Content ID of the deployment type of the application.		
Nomad cache CacheCleaner Nomad jobs	**Clean the SCCM and Nomad cache for a package %packageId% and %packageVersion%**	Action	Cleans the SCCM and Nomad cache for the package with the specified ID and version.	**1E-Nomad-CleanNomadCacheForPackage**	16
Nomad cache Nomad jobs	**Find the Nomad host that has the greatest percentage of content %ContentId%**	Question	Find the Nomad host that has the greatest percentage of the specified content.	**1E-Nomad-FindBestPkgCache**	8

Nomad feature	Instruction text (ReadablePayload)	Type	Description	FileName	Version
Nomad jobs	**Find the ConfigMgr locations (i.e. on DPs) that have content %ContentId% at version %Version%**	Question	Find the ConfigMgr locations (i.e. on DPs) that have the specified content.	**1E-Nomad-GetCmContentLocations**	8
Nomad jobs	**Get the status of Nomad jobs**	Question	Get the status of Nomad jobs.	**1E-Nomad-NomadJobsStatus**	11
Nomad jobs	**Get the status of Nomad**	Question	Get the status of Nomad.	**1E-Nomad-NomadStatus**	11
Nomad jobs	**Pause any current Nomad job**	Action	Pause any current Nomad job.	**1E-Nomad-PauseCurrentNomadJob**	12
Nomad Download Pause Nomad jobs	**Pause the Nomad job queue for %PauseDurationMinutes% minutes**	Action	Pause Nomad job queue.	**1E-Nomad-PauseNomadJobQueue**	14
Nomad Download Pause Nomad jobs	**Resume the paused Nomad job queue**	Action	Resume paused Nomad job queue.	**1E-Nomad-ResumeNomadJobQueue**	11

Nomad feature	Instruction text (ReadablePayload)	Type	Description	FileName	Version
Nomad jobs	**Resume any paused Nomad job**	Action	Resume any paused Nomad job.	**1E-Nomad-ResumePausedNomadJob**	12
Single Site Download	**Ask SSD site master with %deviceIdType% '%deviceId%' whether any device has more than %percent%% of content %contentId% v%version% with format %format%**	Question	Ask SSD site master whether any device has more than the specified percentage of the specified content.	**1E-Nomad-RunPkgStatusRequest**	9
Single Site Download	**Use SSD to find where at least %percent% percent of content %contentId% v%version% with format %format% is cached with extent %extent% and AllSubnets %allSubnets%, returning up to %maxDevices% devices**	Question	Use Nomad's Single Site Download feature to find where the specified content is cached.	**1E-Nomad-RunSsdQuery**	8
NomadBranch service	**Start the Nomad service**	Action	Start the Nomad service.	**1E-Nomad-StartNomadService**	12
Nomad jobs	**Stop any current Nomad job**	Action	Stop any current	**1E-Nomad-StopCurrentNomadJob**	12

Nomad feature	Instruction text (ReadablePayload)	Type	Description	FileName	Version
			Nomad job.		
NomadBranch service	**Stop the Nomad service**	Action	Stop the Nomad service.	**1E-Nomad-StopNomadService**	12

1.11.12.6 1E Patch Success Product pack

Classic Product Pack used to create the **1E Patch Success** instruction set required by the Patch Success application.

For more details please refer to:

- Configuring Patch Success for steps required to upload this product pack and create set
- Using Patch Success.

1.11.12.6.1 Instructions

Instruction text (ReadablePayload)	Type	Description	Instruction file name	Version
<action> patch(es) specified by <patchSpec> identifier(s) from <source> source to targeted device(s) Where: • **<action>** is either **Deploy** or **Download only** • **<patchSpec>** is a list of comma separated GUIDs and/or KB numbers (without KB prefix) of patches to be installed • **<source>** is the patch download source: – • **WSUSR** - Microsoft	Action	Deploys a specific patch or patches to targeted devices. **Note** Unlike the other instructions, the **<patchSpec>** parameter in this instruction does not support **all**. You must be specific which KBs you want to deploy. This instruction is used by the **Deploy** and **Download only** buttons, which allow users to	**1E-PatchSuccess-Deploy**	5

Instruction text (ReadablePayload)	Type	Description	Instruction file name	Version
Update via the Internet • **WSUSL** - WSUS • **SCCM** - Configuration Manager • **Default** - the value of **PatchSuccessSource** in the **GlobalSettings** table of the **TachyonMaster** database, as described in Configuring the source for Patch downloads.		deploy selected patches to devices. The **1E Patch Success Actioners** role requires **Actioner** permissions to see the **Deploy** and the **Download only** buttons. See /document/preview/737277#UUID-a92aef8e-bef6-7780-79c9-2eca1aa05429 in the Tachyon SDK.		
Returns patch status from <source> for <patchSpec> identifier(s) Where : • **<source>** is the patch download source, as above • **<patchSpec>** is either **all**, or a list of comma separated GUIDs and/or KB numbers (without KB prefix) of patches to be reported.	Question	Returns patch status for given KB article numbers on targeted devices. The instruction is used by the **Check Status** button, which allow users to check the patch status of the selected patches and represent the results in Explorer for further investigations. The **1E Patch Success Actioners** role requires **Questioner**	**1E-PatchSuccess-Explore**	5

Instruction text (ReadablePayload)	Type	Description	Instruction file name	Version
		permissions to see the **Check Status** button. See /document/preview/737298#UUID-a4b375c7-8e52-116d-0fb5-edff09511079 in the Tachyon SDK.		
Returns patch status from <source> of given<patchSpec> identifier(s) for PatchSuccess consumption Where: • **<source>** is the patch download source, as above • **<patchSpec>** is either **all**, or a list of comma separated GUIDs and/or KB numbers (without KB prefix) of patches to be reported.	Question	Returns patch status for all known patches on targeted devices. Information is based on offline cache. When run, its response data is offloaded direct to the SLA-BI cube. The instruction is used by the **Update Status** button, which allows users to update the dashboard with the status of selected patches, to see for example **Pending reboot** and **Installed** states. The **1E Patch Success Actioners** role requires **Questioner** permissions to see the **Update status** button. See /document/preview/737298#UUID-a4b375c7-8e52-116d-0fb5-edff09511079 in the Tachyon SDK.	**1E-PatchSuccess-Refresh**	5

1.11.12.7 1E Tachyon Platform product pack

Classic Product Pack used to create the **1E Tachyon Platform** instruction set required by the Tachyon Platform verification process.

For more details please refer to Verifying.

1.11.12.7.1 Instructions

Instruction text (ReadablePayload)	Type	Description	Instruction file name	Version
Tachyon Platform verification stage 1	Question	Stage 1 of the Tachyon Platform verification will return all software installed on each 1E Client endpoint. Verification stage 1 is a simple question-type instruction used to verify: • authenticated user is able to access and use Tachyon Explorer • end-to-end communication between the Tachyon system, the **Switch** and Tachyon client.	**1E-TachyonPlatform-VerificationStage1**	19
Tachyon Platform verification stage 2 (all platforms)	Action	Stage 2 of the Tachyon Platform verification will run a PowerShell script to return a subset of the current configuration of the Tachyon client features of 1E Client. Verification Stage 2 is normally expected to be run as a follow-up action for Verification Stage 1. Verification stage 2 is a simple action-type instruction used to verify:	**1E-TachyonPlatform-VerificationStage2**	21

Instruction text (ReadablePayload)	Type	Description	Instruction file name	Version
		• two-factor authentication (if enabled) and approval workflow, which tests email (if enabled) - necessary for action-type instructions • end-to-end communication between the Tachyon system, the **Background Channel** and Tachyon client • the client is able to run PowerShell scripts on Windows OS - many Tachyon instructions and Guaranteed State rules use PowerShell version 3.0 and later • the client is able to run Bash script on non-Windows OS. For details about PowerShell and Bash support please refer to Tachyon scripting requirements. The rate at which Responses are returned to the Tachyon system via the Switch is affected by the 1E Client setting **DefaultStaggerRangeSeconds**. This setting governs a random delay before the instruction downloads the script from the Background Channel. This stagger setting is ignored on Windows OS if Nomad client is enabled - instead only one client per subnet (or site if Nomad SSD		

Instruction text (ReadablePayload)	Type	Description	Instruction file name	Version
		is used) will act as master and download the script from the Background Channel, and peer clients will download the script from the master.		

1.11.12.8 1E Explorer TachyonCore product pack

Classic Product Pack used to create the **1E Explorer TachyonCore** instruction set that includes instructions for Tagging and Quarantine.

Please refer to:

- Creating the Tags instruction set for steps required to upload this product pack and create the **Tags** instruction set
- Tagging client devices for details on setting, deleting, querying and using **tags**
- Tachyon Quarantine for guidance on using the **quarantine** device instructions.

1.11.12.8.1 Instructions

Instruction text (ReadablePayload)	Type	Description	Instruction file name	Version
Add <action> action Windows firewall rule to IP address <ipaddress>	Action	Add a specified action firewall rule to a specified IP address. Windows only.	**1E-Explorer-TachyonCore-AddFirewallRule**	7
What software is installed?	Question	Returns all installed software.	**1E-Explorer-TachyonCore-AllInstalledSoftware**	7
What audio devices are installed?	Question	Returns details of audio devices. Windows only.	**1E-Explorer-TachyonCore-AudioDeviceDetails**	6
What BIOS firmware is installed?	Question	Returns details of BIOS firmware.	**1E-Explorer-TachyonCore-BiosDetails**	6

Instruction text (ReadablePayload)	Type	Description	Instruction file name	Version
What on-board cache memory is available?	Question	Returns details of the processor's cache memory.	**1E-Explorer-TachyonCore-CacheMemoryDetails**	6
What optical drives are installed?	Question	Returns details of all optical drives.	**1E-Explorer-TachyonCore-CdRomDriveDetails**	6
Change service <servicename> and its dependencies to <state> state	Action	Starts or stops a service and any services that are dependent on it.	**1E-Explorer-TachyonCore-ChangeServiceStateWithDependencies**	6
Does coverage tag <tagname> exist?	Question	Reports the existance of the specified coverage tag	**1E-Explorer-TachyonCore-CheckIfCoverageTagExists**	6
Is coverage tag <tagname> set to <tagvalue>?	Question	Reports whether the defined coverage tag has the specified value	**1E-Explorer-TachyonCore-CheckIfCoverageTagHasGivenValue**	6
Does freeform tag <tagname> exist?	Question	Reports whether the specified freeform tag exists	**1E-Explorer-TachyonCore-CheckIfFreeformTagExists**	6
Is freeform tag <tagname> set to <tagvalue>?	Question	Reports whether the defined freeform tag has the specified value	**1E-Explorer-TachyonCore-CheckIfFreeformTagHasGivenValue**	6
Which devices respond to a check for a simple IoC that evaluates the indicators: <IP_Address> <Ports> <FileSpec> <Domain> <IP_Range> <URL>, gathered since	Question	Check a simple Indicator of Compromise.	**1E-Explorer-TachyonCore-CheckSimpleIoC**	6

Instruction text (ReadablePayload)	Type	Description	Instruction file name	Version
<Search_Period_days> days ago?				
Flush the DNS cache	Action	Flushes the DNS cache on the machine	**1E-Explorer-TachyonCore-CommandLineFlushDns**	6
Ping <targetmachine> using <ipversion>	Action	Ping a specific IP address	**1E-Explorer-TachyonCore-CommandLinePing**	6
Set service <servicename> startup type to <startuptype> and state to <state>	Action	Changes the startup type and the state of an operating system service	**1E-Explorer-TachyonCore-ControlService**	6
How many coverage tags are there?	Question	Returns the number of coverage tags.	**1E-Explorer-TachyonCore-CountCoverageTags**	6
How many freeform tags are there?	Question	Returns the number of freeform tags.	**1E-Explorer-TachyonCore-CountFreeformTags**	6
Create an empty freeform tag named <tagname>	Action	Creates a freeform tag with an empty value. If this tag already exists, its value will be removed.	**1E-Explorer-TachyonCore-CreateEmptyFreeformTag**	6
Delete all coverage tags	Action	Deletes all coverage tags. This is a high impact instruction and should be used with care.	**1E-Explorer-TachyonCore-DeleteAllCoverageTags**	6
Delete all freeform tags	Action	Deletes all freeform tags. This	**1E-Explorer-TachyonCore-DeleteAllFreeformTags**	6

Instruction text (ReadablePayload)	Type	Description	Instruction file name	Version
		is a high impact instruction and should be used with care.		
Delete coverage tag named <tagname>	Action	Deletes specified coverage tag	**1E-Explorer-TachyonCore-DeleteCoverageTag**	6
Delete file at <path>	Action	Deletes a file with specified path	**1E-Explorer-TachyonCore-DeleteFileByPath**	6
Delete <action> Windows firewall action rule assigned to IP address <ipaddress>	Action	Deletes specified firewall action rule assigned to specified IP address. Windows only.	**1E-Explorer-TachyonCore-DeleteFirewallRule**	6
Delete freeform tag named <tagname>	Action	Deletes specified freeform tag	**1E-Explorer-TachyonCore-DeleteFreeformTag**	6
What device drivers are installed?	Question	Returns details of device drivers.	**1E-Explorer-TachyonCore-DeviceDrivers**	6
Which devices currently have active network connections to <ipAddress>?	Question	Gets all devices that currently have any open TCP connections to the specified IP address. It includes information about processes and ports.	**1E-Explorer-TachyonCore-DevicesConnectedToEndpoint**	6
Which devices are listening on port <port>?	Question	Gets devices listening on a specific network port. It also includes information about	**1E-Explorer-TachyonCore-DevicesListeningOnAPort**	6

Instruction text (ReadablePayload)	Type	Description	Instruction file name	Version
		the listening process.		
Which Windows services are disabled?	Question	Shows count of disabled Windows services.	**1E-Explorer-TachyonCore-DisabledServices**	6
What video adapters are installed?	Question	Returns details of video graphic adapters. Windows only.	**1E-Explorer-TachyonCore-DisplayAdapterDetails**	6
<EnableOrDisable> the Windows firewall for the following profile(s): <profile>	Action	Enable or Disable Windows Advanced Firewall for a given profile. Note that this enables locally, and that GPO will override if set.	**1E-Explorer-TachyonCore-EnableDisableFirewall**	3
What does the WMI query <query> on <namespace> return?	Question	Executes a WMI query and returns result. The query execution will be successfull only if the WMI namespace and class exists. Windows only.	**1E-Explorer-TachyonCore-ExecuteWmiQuery**	6
Which devices have a directory named <directoryname> on a fixed disk?	Question	Finds a directory by name.	**1E-Explorer-TachyonCore-FindDirectoryByName**	6
Which devices have a file named <filename> on a fixed disk?	Question	Finds a file by name.	**1E-Explorer-TachyonCore-FindFileByName**	6

Instruction text (ReadablePayload)	Type	Description	Instruction file name	Version
Which devices have a file of <filesize> bytes with a SHA256 hash of <hash> on a fixed disk?	Question	Finds a file by size and SHA256 hash.	**1E-Explorer-TachyonCore-FindFileBySizeAndHash**	6
What is the file version infomation of <filename> on a fixed disk?	Question	Finds file version, Original Filename, Product Name and Product version of a file you specify	**1E-Explorer-TachyonCore-FindFileVersionInfoByName**	5
What are the coverage tags?	Question	Returns all coverage tag values	**1E-Explorer-TachyonCore-GetAllCoverageTags**	6
What are the freeform tags?	Question	Returns all freeform tag values	**1E-Explorer-TachyonCore-GetAllFreeformTags**	6
What is the value of the coverage tag <tagname>?	Question	Returns value of a specific coverage tag	**1E-Explorer-TachyonCore-GetCoverageTag**	6
How much memory is installed?	Question	Memory details for each installed DIMM.	**1E-Explorer-TachyonCore-GetCurrentInstalledMemoryDetails**	6
What is the current Powershell execution policy?	Question	Returns the Powershell execution policy on the device.	**1E-Explorer-TachyonCore-GetExecutionPolicyPowershellCommandLine**	6
What is the content of <filename>?	Question	Retrieve the content of files matching the given file path search pattern. Wildcard characters and environment	**1E-Explorer-TachyonCore-GetFile**	7

Instruction text (ReadablePayload)	Type	Description	Instruction file name	Version
		variables may be used.		
Which lines of <filename> match the pattern <pattern>?	Question	Retrieves the lines of files matching the given file path search pattern. Wildcard characters and environment variables may be used.	**1E-Explorer-TachyonCore-GetFileByLines**	6
What operating system details exist for <filePath>, optionally computing the hash (<computeHash>)	Question	What details does the operating system have about a particular file	**1E-Explorer-TachyonCore-GetFileDetails**	10
What access permissions exist on <filePath>?	Question	What access permissions exist for a particular file	**1E-Explorer-TachyonCore-GetFilePermissions**	12
What files are in <folder> folder?	Question	Retrieve the files in a specified folder. Windows Only.	**1E-Explorer-TachyonCore-GetFilesInFolder**	6
What files are in <folder> folder, including subfolders?	Question	Retrieve the files in a specified folder and all subfolders. Windows Only.	**1E-Explorer-TachyonCore-GetFilesInFolderRecursively**	6
Which devices have <action> action Windows firewall rule assigned to IP address <ipaddress>?	Question	Gets devices with a specified action firewall rule assigned to a specified IP address. Windows Only.	**1E-Explorer-TachyonCore-GetFirewallRule**	6

Instruction text (ReadablePayload)	Type	Description	Instruction file name	Version
List <ruleState> firewall rules	Question	Returns firewall rules filtered by state	**1E-Explorer-TachyonCore-GetFirewallRulesFiltered**	3
What is the value of the freeform tag <tagname>?	Question	Returns the value of a specific freeform tag	**1E-Explorer-TachyonCore-GetFreeformTag**	6
What historical inbound connections are recorded?	Question	Retrieves the historical inbound connections recorded on the device	**1E-Explorer-TachyonCore-GetInboundConnectionHistory**	5
What historical inbound mapped drives are recorded?	Question	Retrieves the historical inbound mapped drives recorded on the device	**1E-Explorer-TachyonCore-GetInboundMappedDriveHistory**	5
What shared printers are being used on the machine?	Question	What shared printers are being used on the machine?	**1E-Explorer-TachyonCore-GetInboundPrinters**	5
Which Windows hotfixes are installed?	Question	Returns a list of installed Windows hotfixes.	**1E-Explorer-TachyonCore-GetInstalledWindowsHotfixes**	6
Which IP addresses are assigned to devices?	Question	Gets the IP addresses assigned to devices. Windows Only.	**1E-Explorer-TachyonCore-GetIpAddresses**	6
Who is currently logged in?	Question	Shows a list of all users logged into devices, including interactive and	**1E-Explorer-TachyonCore-GetLoggedInUsers**	6

Instruction text (ReadablePayload)	Type	Description	Instruction file name	Version
		remote desktop sessions.		
What historical outbound connections are recorded?	Question	Retrieves the historical outbound connections recorded on the device	**1E-Explorer-TachyonCore-GetOutboundConnectionHistory**	5
What outbound shared drives usage has been recorded?	Question	Retrieves the historical and currently exposed shared drive usage recorded on the device	**1E-Explorer-TachyonCore-GetOutboundMappedDriveHistory**	5
What printers are shared from the machine?	Question	What printers are shared from the machine?	**1E-Explorer-TachyonCore-GetOutboundPrinters**	4
What processes are running?	Question	Get all running processes.	**1E-Explorer-TachyonCore-GetProcesses**	6
Are my devices quarantined? Warning: Please read the description before use	Question	Queries the quarantine status of the device. Please use with care, and please read the documentation for the quarantine feature before use.	**1E-Explorer-TachyonCore-GetQuarantineStatus**	5
What services are running?	Question	Retrieves all the running services. Windows Only.	**1E-Explorer-TachyonCore-GetServiceInfo**	6
Which Hyper-V virtual machines are running?	Question	Returns details for virtualized Hyper-V	**1E-Explorer-TachyonCore-HyperVGuestDetails**	6

Instruction text (ReadablePayload)	Type	Description	Instruction file name	Version
		guest machines that are currently running. Windows hosts only.		
What memory chips are installed?	Question	Details of RAM chips. Windows Only.	**1E-Explorer-TachyonCore-InstalledMemoryDetails**	6
How many of each operating system versions are installed?	Question	Return a count of all distinct Operating Systems, Version and Virtual platform for each Tachyon-connected device.	**1E-Explorer-TachyonCore-InstalledOS**	6
Which versions of <appname> are installed?	Question	Returns count of all distinct versions of the specified product. Note the value entered does not need to be complete e.g. enter chrome and all products containing chrome will be returned.	**1E-Explorer-TachyonCore-InstalledSoftwareProduct**	7
Which versions of <publisher> <appname> are installed?	Question	Returns count of all distinct versions of the specified publisher and product. Note the values entered do not need to be complete e.g. enter Micro and all publishers	**1E-Explorer-TachyonCore-InstalledSoftwarePublisherProduct**	7

Instruction text (ReadablePayload)	Type	Description	Instruction file name	Version
		containing Micro will be returned.		
What USB devices are installed?	Question	Returns details of installed USB devices. Windows only.	**1E-Explorer-TachyonCore-InstalledUsbDevices**	8
Kill process <processId>	Action	Terminate a single process.	**1E-Explorer-TachyonCore-KillProcess**	6
Kill process(es) with image name matching <exename>	Action	Terminate all instances of a specified executable.	**1E-Explorer-TachyonCore-KillProcesses**	6
How many local groups is <accountName> a member of?	Question	Get the number of local groups each matching account is a member of. Windows Only.	**1E-Explorer-TachyonCore-LocalGroupMemberSummary**	7
Which logical drives are available?	Question	Get details of logical drives, including network drives. Windows Only.	**1E-Explorer-TachyonCore-LogicalDiskDetails**	6
Log off <user>	Action	Logs off %user% from all specified machines. The account should not contain a prefix. The user will be forcibly logged off - unsaved work or documents will be lost. Windows Only.	**1E-Explorer-TachyonCore-LogoffUser**	6

Instruction text (ReadablePayload)	Type	Description	Instruction file name	Version
How are network adapters configured?	Question	Get the configuration of the network adapters. Windows Only.	**1E-Explorer-TachyonCore-NetworkAdapterConfigurationDetails**	6
Which network adapters are installed?	Question	Gets details of network adapters. Windows Only.	**1E-Explorer-TachyonCore-NetworkAdapterDetails**	6
What processes are listening on which ports?	Question	Gets network listening processes and ports.	**1E-Explorer-TachyonCore-NetworkListeningProcessesAndPorts**	6
What does the nslookup for <address> return?	Question	Performs an nslookup on a specified address and returns the output as a string.	**1E-Explorer-TachyonCore-NslookupCmd**	6
Which hard drives are installed?	Question	Get details of physical disk drives. Windows Only.	**1E-Explorer-TachyonCore-PhysicalDiskDetails**	6
Which plug-and-play devices are installed?	Question	Get details of plug and play devices. Windows Only.	**1E-Explorer-TachyonCore-PlugAndPlayDevices**	6
Which printers are installed?	Question	Get details of installed printers. Windows only.	**1E-Explorer-TachyonCore-PrinterDetails**	6
Which devices are currently running <ProcessName> as local admin?	Question	Finds all devices that currently have the specified process running with local	**1E-Explorer-TachyonCore-ProcessAsLocalAdmin**	6

Instruction text (ReadablePayload)	Type	Description	Instruction file name	Version
		administrator privilages.		
Which processors are installed?	Question	Details of processors installed. Windows Only.	**1E-Explorer-TachyonCore-ProcessorDetails**	6
What processor types are being used?	Question	Gets processor types being used by devices. Windows only.	**1E-Explorer-TachyonCore-ProcessorDetailsByType**	6
Quarantine selected devices. Warning: Please read the description before use	Action	Quarantines the device. The device will only be able to contact Tachyon. CRL checks must be set to soft. Certificate expiry can cause the agent to fail to connect to the switch. If an agent is no longer connected to Tachyon after quarantine, it will remain in quarantine. Please use with care, and please read the documentation for the quarantine feature before use.	**1E-Explorer-TachyonCore-QuarantineDevice**	5
Shutdown and reboot devices in <timeToReboot> seconds	Action	Schedules a reboot in a specified number of seconds. This will	**1E-Explorer-TachyonCore-RebootMachineInXSeconds**	3

Instruction text (ReadablePayload)	Type	Description	Instruction file name	Version
		not prompt for user interaction!		
Refresh the Windows CRL cache	Action	Refreshes the CRL cache by setting the ChainCacheResyncFiletime. This means that windows will attempt to retrieve a CRL the next time it is called upon for verification.	**1E-Explorer-TachyonCore-RefreshCrlCache**	6
Delete registry key <hive>:<subkey> recursively	Action	Delete an entire registry key. Windows Only.	**1E-Explorer-TachyonCore-RegistryDeleteKey**	7
Delete key <subkey> for every user in the HKEY_USERS hive	Action	Delete a specified key for each user in the HKEY_USERS hive. Windows Only.	**1E-Explorer-TachyonCore-RegistryDeleteUserKey**	7
Delete a <value> under <subkey> for every user in the HKEY_USERS hive	Action	Delete a specified registry entry for each user in the HKEY_USERS hive. Windows Only.	**1E-Explorer-TachyonCore-RegistryDeleteUserValues**	7
Delete registry entry <hive> <subkey> <name>	Action	Delete a specified registry entry. Windows Only.	**1E-Explorer-TachyonCore-RegistryDeleteValue**	7
What are all the keys under the registry key <hive> <subkey>?	Question	Get all sub keys for a Registry key. Windows Only.	**1E-Explorer-TachyonCore-RegistryEnumerateKeys**	10

Instruction text (ReadablePayload)	Type	Description	Instruction file name	Version
What are all the keys under a registry <subkey> for each user in the HKEY_USERS hive?	Question	Get all the keys under a subkey for each user in the HKEY_USERS hive. Windows Only.	**1E-Explorer-TachyonCore-RegistryEnumerateUserKeys**	5
What are all the values under a registry <subkey> for each user in the HKEY_USERS hive?	Question	Get all the values under a subkey for each user in the HKEY_USERS hive. Windows Only.	**1E-Explorer-TachyonCore-RegistryEnumerateUserValues**	7
What are all the values under the registry key <hive> <subkey>?	Question	Get all values for a Registry key. Windows Only.	**1E-Explorer-TachyonCore-RegistryEnumerateValues**	7
What is the value of <value> under <subkey> for each user in the HKEY_USERS hive?	Question	Get a registry value for each user in the HKEY_USERS hive. Windows Only.	**1E-Explorer-TachyonCore-RegistryGetUserValues**	8
What is the value of the registry entry <hive> <subkey> <name>?	Question	Get the value for a Registry entry. Windows Only.	**1E-Explorer-TachyonCore-RegistryGetValue**	7
Which devices have the registry key <hive> <subkey>?	Question	Determine whether a given Registry key exists. Windows Only.	**1E-Explorer-TachyonCore-RegistryKeyExists**	7
Set <name> as <valuetype> to <value> under <subkey> for every user in the HKEY_USERS hive	Action	Set a registry entry for each user in the HKEY_USERS hive. Windows Only.	**1E-Explorer-TachyonCore-RegistrySetUserValues**	7

Instruction text (ReadablePayload)	Type	Description	Instruction file name	Version
Set registry entry <hive> <subkey> <name> to <valuetype> <value>	Action	Set the value for a given Registry entry. Windows Only.	**1E-Explorer-TachyonCore-RegistrySetValue**	7
Which users in the HKEY_USERS hive have <subkey>?	Question	Determine whether a registry key exists for each user in the HKEY_USERS hive. Windows Only.	**1E-Explorer-TachyonCore-RegistryUserKeyExists**	6
Which users in the HKEY_USERS hive have a <value> under <subkey>?	Question	Determine whether a registry entry exists for each user in the HKEY_USERS hive. Windows Only.	**1E-Explorer-TachyonCore-RegistryUserValueExists**	6
Which devices have the registry entry <hive> <subkey> <name>?	Question	Determine whether a given Registry entry exists. Windows Only.	**1E-Explorer-TachyonCore-RegistryValueExists**	7
Which removable drives are installed?	Question	Returns information about removable drives. Windows Only.	**1E-Explorer-TachyonCore-RemovableDiskDetails**	6
Which devices are running <executable>?	Question	Shows machines running a specific executable. Windows Only.	**1E-Explorer-TachyonCore-RunningProcess**	7
Set coverage tag <tagname> to <tagvalue>	Action	Sets a value for a coverage tag on devices. This tag can be used to narrow down	**1E-Explorer-TachyonCore-SetCoverageTag**	6

Instruction text (ReadablePayload)	Type	Description	Instruction file name	Version
		target devices for instructions.		
Set freeform tag <tagname> to <tagvalue>	Action	Sets a value for a freeform tag on devices. This tag and value combination can be arbitrary. This tag cannot be used to narrow down target devices for instructions.	**1E-Explorer-TachyonCore-SetFreeFormTag**	6
Set PowerShell execution policy to <executionPolicy>	Action	Sets the PowerShell execution policy on devices. The new execution policy will be returned after being set.	**1E-Explorer-TachyonCore-SetPowerShellExecutionPolicy**	6
Remove application <appname> published by <publisher>	Action	Removes all versions of the specified application published by the specified publisher, if present.	**1E-Explorer-TachyonCore-UninstallApplicationAllVersions**	6
Remove version <version> of application <appname> published by <publisher>	Action	Removes the specified version of the the specified application published by the specified publisher, if it is present.	**1E-Explorer-TachyonCore-UninstallApplicationSpecificVersion**	6

Instruction text (ReadablePayload)	Type	Description	Instruction file name	Version
Releases selected devices from quarantine. Warning: Please read the description before use	Action	Unquarantines the device. Please use with care, and please read the documentation for the quarantine feature before use.	**1E-Explorer-TachyonCore-UnquarantineDevice**	5
Which unsigned device drivers are installed?	Question	Gets device drivers which are not digitally signed. Windows only.	**1E-Explorer-TachyonCore-UnsignedDeviceDrivers**	6
Which devices is <domainName>\<accountName> currently logged on?	Question	Find all devices on which the given user is currently logged in. Windows Only.	**1E-Explorer-TachyonCore-UserLoggedInDevices**	7
Which Windows updates are pending a reboot?	Question	Gets Windows updates with a count of each device that is pending a reboot for this update to take effect. Windows only.	**1E-Explorer-TachyonCore-WindowsUpdatesPendingReboot**	6

1.11.12.9 MEMCM Client Health integrated product pack

Integrated Product Pack used to create the **MEMCM Client Health** policy.

For more information please refer to Guaranteed State - MEMCM Client Health Policy.

1.11.12.9.1 Overview

Many businesses rely on Microsoft Endpoint Manager Configuration Manager (MEMCM) to deploy software, patches and updates across their company networks. It is crucial that Configuration Manager is working effectively.

The MEMCM Client Health policy monitors Configuration Manager client health and performance. It checks for cache availability, inventory cycles, service availability and Configuration Manager WMI integrity - common causes of Configuration Manager client problems on devices.

The MEMCM Client Health policy replaces the previous SCCM Client Health policy and covers the following:

- Ensure the correct version of the CM client is installed and running and assigned to the correct site
- Ensure the CM client is not stuck in provisioning mode
- Ensure that heartbeat discovery, inventory and state messages are being sent regularly
- Ensures the CM client cache is set to the correct size
- Ensure the CM client log settings are correct
- Ensure the BITS service exists, configured to start up automatically and is running
- Ensure the Windows Time service exists with correct startup settings
- Ensure the Windows Management Instrumentation (WMI) service exists, configured to start automatically and is running
- Ensure WMI is healthy, the core CIMv2 and ccm namespaces and classes exist and that the WMI repository is consistent
- Ensure the Windows Update service exists with correct startup settings, is configured to use the correct source (CM, WSUS or Microsoft Update) and that the service can connect to the source.

Note

This policy is intended for deployment to Windows devices only.

1.11.12.9.1.1Instructions

This product pack contains no instructions.

1.11.12.9.1.2Policies

The following table shows the policies included in the Integrated Product Pack.

Name	Description
MEMCM Client Health	The MEMCM (Microsoft Endpoint Manager - Configuration Manager) Client Health policy ensures that the MEMCM client and surrounding technologies are healthy.

1.11.12.9.1.3Rules

Note

The following table shows the rules included in the above policy. Any parameter values shown in the **Check and Fix fragments**, **Triggers** and **Precondition fragment** columns are

specifically set in the rules when the pack is uploaded. These may be different to the default values shown in the Fragments table. You can modify these if required.

Name	Type	Description	Check and Fix fragments	Triggers	Precondition fragment
MEMCM Client Assignment	Fix	Ensure the client is assigned to the right site. Assign it if it isn't.	1E-GuaranteedState-Check-MEMCM-AssignedSite 1E-GuaranteedState-Fix-MEMCM-SetAssignedSite	Periodic (24 hours)	1E-GuaranteedState-Precondition-Multiple • 1EClientVersionToCompare=0 • 1EClientVersionDesiredResult=SameOrHigher • DeviceChassisTypeList=% • DeviceCpuTypeList=% • DeviceDomainList=% • DeviceFqdnList=% • DeviceManufacturerList=% • DeviceModelList=% • DeviceRamMBMin=0 • DeviceRamMBMax=2147483647 • DeviceTimeZoneOffsetList= -720;-660;-600;-570;-540;-480; -420;-360;-300;-240;-180;-150; -120;-60;0;60;120;180;240; 270;300;330;345;360;390;

Name	Type	Description	Check and Fix fragments	Triggers	Precondition fragment
					420;480;525;540;570;600; 630;660;720;765;780;840 • DirectoryExists=Exists • DirectoryName=% • DnsLookupFqdnList=% • FileNameExists=Exists • FileName=% • OsTypeList=Windows • OsArchitectureList=% • ProcessExists=Doesn't Exist • ProcessExecutableList=ccmsetup.exe • QuarantineStatus=% • RegistryExists=Exists • RegistryHive=HKLM • RegistryKey=% • RegistryValue=% • RegistryData=% • ServiceExists=Exists • ServiceName=Winmgmt • ServiceStartAccountName=%

Name	Type	Description	Check and Fix fragments	Triggers	Precondition fragment
					• ServiceStartType=% • ServiceState=Running • ServiceTriggerStart=% • ServiceType=% • SoftwareExists=Exists • SoftwareProduct=Configuration Manager Client • SoftwarePublisher=Microsoft% • SoftwareVersionToCompare=0 • SoftwareVersionDesiredResult=SameOrHigher • WindowsUpdateSource=% • WmiNamespace=ROOT\ccm\StateMsg • WmiClass=CCM_StateMsg • WmiColumn=% • WmiWhereClause={none} • WmiVersionToCompare=0 • WmiDesiredResult=SameOrHigher

Name	Type	Description	Check and Fix fragments	Triggers	Precondition fragment
MEMCM Client Cache Size	Fix	Ensure the MEMCM client cache is set to the right size. Set it if it isn't.	1E-GuaranteedState-Check-MEMCM-CacheSizeBetween 1E-GuaranteedState-Fix-MEMCM-SetCacheSize	Periodic (24 hours)	
MEMCM Client ClassExists	Check(1)	Ensure the default CCM class exists in WMI.	1E-GuaranteedState-Check-Wmi-ClassExists 1E-GuaranteedState-Fix-MEMCM-InstallClient (1)	Periodic (24 hours)	1E-GuaranteedState-Precondition-Multiple
MEMCM Client ClientProvisioningMode	Fix	Ensure the client is not stuck in provisioning mode. Turn it off if it is.	1E-GuaranteedState-Check-MEMCM-ClientProvisioningMode 1E-GuaranteedState-Fix-MEMCM-SetClientProvisioningMode	Periodic (24 hours)	1E-GuaranteedState-Precondition-Multiple
MEMCM Client DataDiscoveryRecordSent	Check	Ensure that a data discovery record (DDR) is being sent regularly.	1E-GuaranteedState-Check-MEMCM-DataDiscoveryRecordSent	Periodic (24 hours)	1E-GuaranteedState-Precondition-Multiple
MEMCM Client FileCollectionSent	Check	Ensure that file collection is being sent regularly.	1E-GuaranteedState-Check-MEMCM-FileCollectionSent	Periodic (24 hours)	1E-GuaranteedState-Precondition-Multiple

Name	Type	Description	Check and Fix fragments	Triggers	Precondition fragment
MEMCM Client HardwareInventorySent	Check	Ensure that hardware inventory is being sent regularly.	1E-GuaranteedState-Check-MEMCM-HardwareInventorySent	Periodic (24 hours)	1E-GuaranteedState-Precondition-Multiple
MEMCM Client IDMIFCollectionSent	Check	Ensure that IDMIF collection is being sent regularly.	1E-GuaranteedState-Check-MEMCM-IDMIFCollectionSent	Periodic (24 hours)	1E-GuaranteedState-Precondition-Multiple
MEMCM Client Logging	Check	Ensure the MEMCM client log settings are set to the right values.	1E-GuaranteedState-Check-MEMCM-GlobalLoggingConfiguration	Periodic (24 hours)	1E-GuaranteedState-Precondition-Multiple
MEMCM Client NamespaceExists	Check[(1)]	Ensure the MEMCM (CCM) namespace exists in WMI.	1E-GuaranteedState-Check-Wmi-NamespaceExists 1E-GuaranteedState-Fix-MEMCM-InstallClient [(1)]	Periodic (24 hours)	1E-GuaranteedState-Precondition-Multiple
MEMCM Client SoftwareInventorySent	Check	Ensure that software inventory is being sent regularly.	1E-GuaranteedState-Check-MEMCM-SoftwareInventorySent	Periodic (24 hours)	1E-GuaranteedState-Precondition-Multiple
MEMCM Client StateMessagesSent	Check	Ensure that state messages are being sent regularly.	1E-GuaranteedState-Check-MEMCM-StateMessagesSent	Periodic (24 hours)	1E-GuaranteedState-Precondition-Multiple

Name	Type	Description	Check and Fix fragments	Triggers	Precondition fragment
MEMCM Client Version	Check[1]	Ensure the right version of the client is installed.	1E-GuaranteedState-Check-Software-Version 1E-GuaranteedState-Fix-MEMCM-InstallClient [1]	Periodic (24 hours)	1E-GuaranteedState-Precondition-Multiple
Network IPv4 PrimaryAddressInDNS	Check	Check the FQDN matches DNS by looking up the primary IPv4 address in DNS	1E-GuaranteedState-Check-Network-PrimaryIPv4InDNS	Periodic (24 hours)	1E-GuaranteedState-Precondition-Multiple
Service BITS DelayedStart	Fix	Ensure that the BITS (Background Intelligent Transfer Service) service is set to Automatic (Delayed Start). Set it if not.	1E-GuaranteedState-Check-Service-StartType 1E-GuaranteedState-Fix-Service-SetStartTypeAutomaticDelayedStart	Periodic (24 hours)	1E-GuaranteedState-Precondition-Multiple
Service BITS Exists	Check	Ensure that the BITS (Background Intelligent Transfer Service) service exists.	1E-GuaranteedState-Check-Service-Exists	Periodic (24 hours)	1E-GuaranteedState-Precondition-Multiple
Service BITS Running	Fix	Ensure that the BITS (Background Intelligent	1E-GuaranteedState-Check-Service-State	Service Status	1E-GuaranteedState-Precondition-Multiple

Name	Type	Description	Check and Fix fragments	Triggers	Precondition fragment
		Transfer Service) service is running. Start it if it isn't	1E-GuaranteedState-Fix-Service-Start	Change	
Service ccmexec DelayedStart	Fix	Ensure that the ccmexec (SMS Agent Host) service is set to Automatic (Delayed Start). Set it if not.	1E-GuaranteedState-Check-Service-StartType 1E-GuaranteedState-Fix-Service-SetStartTypeAutomaticDelayedStart	Periodic (24 hours)	1E-GuaranteedState-Precondition-Multiple
Service ccmexec Exists	Check(1)	Ensure that the ccmexec (SMS Agent Host) service exists.	1E-GuaranteedState-Check-Service-Exists 1E-GuaranteedState-Fix-MEMCM-InstallClient (1)	Periodic (24 hours)	1E-GuaranteedState-Precondition-Multiple
Service ccmexec Running	Fix	Ensure that the ccmexec (SMS Agent Host) service is running. Start it if it isn't	1E-GuaranteedState-Check-Service-State 1E-GuaranteedState-Fix-Service-Start	Service Status Change	1E-GuaranteedState-Precondition-Multiple
Service W32Time Exists	Check	Ensure that the W32Time (Windows Time) service exists.	1E-GuaranteedState-Check-Service-Exists	Periodic (24 hours)	1E-GuaranteedState-Precondition-Multiple

Name	Type	Description	Check and Fix fragments	Triggers	Precondition fragment
Service W32Time Manual	Fix	Ensure that the W32Time (Windows Time) service is set to manual. Set it to manual if it's not.	1E-GuaranteedState-Check-Service-StartType 1E-GuaranteedState-Fix-Service-SetStartTypeManual	Periodic (24 hours)	1E-GuaranteedState-Precondition-Multiple
Service W32Time TriggerStart	Check	Ensure that the W32Time (Windows Time) service is set to trigger start.	1E-GuaranteedState-Check-Service-TriggerStart	Periodic (24 hours)	1E-GuaranteedState-Precondition-Multiple
Service Winmgmt Automatic	Fix	Ensure that the Winmgmt (Windows Management Instrumentation) service is set to automatic. Set it to automatic if it's not.	1E-GuaranteedState-Check-Service-StartType 1E-GuaranteedState-Fix-Service-SetStartTypeAutomatic	Periodic (24 hours)	1E-GuaranteedState-Precondition-Multiple
Service Winmgmt Exists	Check	Ensure that the Winmgmt (Windows Management Instrumentation) service exists.	1E-GuaranteedState-Check-Service-Exists	Periodic (24 hours)	1E-GuaranteedState-Precondition-Multiple
Service Winmgmt Running	Fix	Ensure that the Winmgmt (Windows Management	1E-GuaranteedState-Check-Service-State	Service Status	1E-GuaranteedState-Precondition-Multiple

Name	Type	Description	Check and Fix fragments	Triggers	Precondition fragment
		Instrumentation) service is running. Start it if it isn't	1E-GuaranteedState-Fix-Service-Start	Change	
Service wuauserv Exists	Check[2]	Ensure that the wuauserv (Windows Update) service exists.	1E-GuaranteedState-Check-Service-Exists 1E-GuaranteedState-Fix-WindowsUpdate-ResetWindowsUpdate [2]	Periodic (24 hours)	1E-GuaranteedState-Precondition-Multiple
Service wuauserv Manual	Fix	Ensure that the wuauserv (Windows Update) service is set to manual. Set it to manual if it's not.	1E-GuaranteedState-Check-Service-StartType 1E-GuaranteedState-Fix-Service-SetStartTypeManual	Periodic (24 hours)	1E-GuaranteedState-Precondition-Multiple
Service wuauserv TriggerStart	Check	Ensure that the wuauserv (Windows Update) service is set to trigger start.	1E-GuaranteedState-Check-Service-TriggerStart	Periodic (24 hours)	1E-GuaranteedState-Precondition-Multiple
WindowsUpdate ConnectionOK	Check	Ensure the connection to Windows Update is OK	1E-GuaranteedState-Check-WindowsUpdate-ConnectionOK	Periodic (24 hours)	1E-GuaranteedState-Precondition-Multiple

Name	Type	Description	Check and Fix fragments	Triggers	Precondition fragment
WindowsUpdate Source	Check	Ensure the connection to Windows Update is using the right source (Configuration Manager, WSUS, Microsoft Update)	1E-GuaranteedState-Check-WindowsUpdate-Source	Periodic (24 hours)	1E-GuaranteedState-Precondition-Multiple
WMI cimv2 NamespaceExists	Check	Ensure the default (cimv2) namespace exists in WMI.	1E-GuaranteedState-Check-Wmi-NamespaceExists	Periodic (24 hours)	1E-GuaranteedState-Precondition-Multiple
WMI Repository Consistency	Fix	Ensure the WMI repository is consistent. Salvage the repository or (optionally) reset it if inconsistent.	1E-GuaranteedState-Check-Wmi-Repository 1E-GuaranteedState-Fix-Wmi-Repository	Periodic (24 hours)	1E-GuaranteedState-Precondition-Multiple
WMI Win32_ComputerSystem ClassExists	Check	Ensure the default Win32_ComputerSystem class exists in WMI.	1E-GuaranteedState-Check-Wmi-ClassExists	Periodic (60 min)	1E-GuaranteedState-Precondition-Multiple

1.11.12.9.1.4Fragments

Note

The **Parameters** column in the following table shows the ranges and default values for the parameters. The default values are used when you create custom rules using these fragments, unless you select alternative values.

1.11.12.9.1.4.1 Fragments used in MEMCM Client Health Policy rules

The following fragments are used by the rules defined above in the MEMCM Client Health policy.

Name	Type	Readable Payload and summary	Parameters
1E-GuaranteedState-Check-MEMCM-AssignedSite	Check	**Check the CM client has been assigned to site %SiteCode%**	**SiteCode** Check to see if the MEMCM client is assigned to this site code
1E-GuaranteedState-Check-MEMCM-CacheSizeBetween	Check	**Check the CM cache size is between %MinMB% and %MaxMB%**	**MinMB** The cache size should be at least this big (in Megabytes) **MaxMB** The cache size should be at most this big (in

Name	Type	Readable Payload and summary	Parameters
			Megabytes)
1E-GuaranteedState-Check-MEMCM-ClientProvisioningMode	Check	**Check the CM ClientProvisioningMode is set to %TrueFalse%**	**TrueFalse** True represents client provisioning ON, False represents client provisioning OFF
1E-GuaranteedState-Check-MEMCM-DataDiscoveryRecordSent	Check	**Check the CM client has sent a DDR (Data Discovery Record) within the last %Days% days**	**Days** Look for DDRs sent back in this number of days
1E-GuaranteedState-Check-MEMCM-FileColl	Check	**Check the CM client has performed a file collection within the last %Days% days**	**Days** Look for file collection sent back in this number of days

Name	Type	Readable Payload and summary	Parameters
ectionSent			
1E-GuaranteedState-Check-MEMCM-GlobalLoggingConfiguration	Check	**Check the CM client logging is configured with %Loglevel%, %MaxSize%, %MaxHistoryFiles% and %DebugLogging% settings**	**LogLevel** The logging level Valid Values: Verbose, Normal, None **MaxSize** The maximum size (in Bytes) that the MEMCM logs may grow before rolling over **MaxHistoryFiles** The number of incremented log files to accumulate

Name	Type	Readable Payload and summary	Parameters
			before deleting **DebugLogging** True means debug logging should be on, False means it should be off
1E-GuaranteedState-Check-MEMCM-HardwareInventorySent	Check	**Check the CM client has sent hardware inventory within the last %Days% days**	**Days** Look for hardware inventory data sent back in this number of days
1E-GuaranteedState-Check-MEMCM-IDMIFCollectionSent	Check	**Check the CM client has performed an IDMIF collection within the last %Days% days**	**Days** Look for IDMIFs sent back within this number of days

Name	Type	Readable Payload and summary	Parameters
1E-GuaranteedState-Check-MEMCM-SoftwareInventorySent	Check	**Check the CM client has sent software inventory within the last %Days% days**	**Days** Look for software inventory data sent back within this number of days
1E-GuaranteedState-Check-MEMCM-StateMessagesSent	Check	**Check the CM client has sent state messages within the last %Days% days**	**Days** Look for state messages sent back within this number of days
1E-GuaranteedState-Check-Network-IPv4-PrimaryAddressInDNS	Check	**Check the Device FQDN matches the value from DNS** Take the primary IP address for the default route and look it up in DNS. Make sure the fqdn from device summary matches the fqdn returned from DNS	
1E-GuaranteedState-	Check	**Check that %ServiceName% service exists**	**Service Name**

Name	Type	Readable Payload and summary	Parameters
Check-Service-Exists			Shortname of the service
1E-GuaranteedState-Check-Service-StartType	Check	**Check that %ServiceName% start type is %StartType%**	**Service Name** Shortname of the service **StartType** The startup setting for the service Valid Values: • Automatic • Automatic (

Name	Type	Readable Payload and summary	Parameters
			DelayedStart) • Boot • Disabled • Manual • System

Name	Type	Readable Payload and summary	Parameters
1E-GuaranteedState-Check-Service-State	Check	**Check the %ServiceName% service is in %State% state** For completeness, all valid service states are included. Realistically, however, making a precondition out of transition states like • About To Continue • Pausing • Starting • Stopping isn't a very good idea as a service will only be in that state for a very short time.	**Service Name** Shortname of the service **State**The state the service should be in Valid Values: • AboutToContinue • Pausing • Pa

Name	Type	Readable Payload and summary	Parameters
			used • Running • Starting • Stopping • Stopped
1E-GuaranteedState-	Check	**Check the %ServiceName% service is set to start on a trigger** The actual trigger is not checked or reported	**Service Name** Shortname of

Name	Type	Readable Payload and summary	Parameters
Check-Service-Trigger Start			the service
1E-GuaranteedState-Check-Software-Version	Check	**Check for the existence of %Publisher% %Product% with version %VersionDesiredResult% than %VersionToCompare%** Checks if the specified Publisher and Product is installed and that the version is lower, same or higher than the target (VersionToCompare)	**Publisher** Check for this publisher name **Product** Check for this product name **VersionToCompare** The software product version to use as the comparison DEFAULT: 0 **VersionDesiredResult**The outcome that's

Name	Type	Readable Payload and summary	Parameters
			desired when the software product version is compared to VersionToCompare Valid values: • SameOrLower • Lower • Lower_M

Name	Type	Readable Payload and summary	Parameters
			ajorLower • Lower_SameMajor • Lower_SameMajorM

Name	Type	Readable Payload and summary	Parameters
			inor • Lower_SameMajorMinorRelease • Same • High

Name	Type	Readable Payload and summary	Parameters
			er_SameMajorMinorRelease • Higher_SameMajor

Name	Type	Readable Payload and summary	Parameters
			Minor • Higher_SameMajor • Higher_MajorHigher

Name	Type	Readable Payload and summary	Parameters
			• Higher • SameOrHigher DEFAULT: SameOrHigher
1E-GuaranteedState-Check-WindowsUpdate-ConnectionOK	Check	**Check that the client can connect to the configured Windows Update source**	
1E-GuaranteedState-Check-Windo	Check	**Check Windows Update agent is configured to use %Source% as source** If Source is set to % (Default) this will check each of the sources and pass with the first one that succeeds.	**Source** The windows update source

Name	Type	Readable Payload and summary	Parameters
wsUpdate-Source			(% wildcard accepted) Valid Values: • SCCM(MEMCM) • WSUSL(WSUS-Local) • WSUSR

Name	Type	Readable Payload and summary	Parameters
			(WSUS-Remote) • % DEFAULT: %
1E-GuaranteedState-Check-Wmi-ClassExists	Check	**Check that WMI %Class% exists in %Namespace%**	**Namespace** The WMI namespace to check existence (ROOT\cimv2 for example) **Class**The WMI class that should exist in specified

Name	Type	Readable Payload and summary	Parameters
			namespace
1E-GuaranteedState-Check-Wmi-NamespaceExists	Check	**Check that WMI %Namespace% exists**	**Namespace** The WMI namespace to check existence (ROOT\cimv2 for example)
1E-GuaranteedState-Check-Wmi-Repository	Check	**Check that the WMI repository is consistent** Runs winmgmt.exe /verifyrepository and fails if 'is not consistent' appears in the returned result	
1E-GuaranteedState-Fix-MEMCM-SetAssignedSite	Fix	**Set CM assigned site to %SiteCode%** Namespace: ROOT\CCM Class: SMS_CLIENT Method: SetAssignedSite sSiteCode: %SiteCode%	**SiteCode** Assign the client to this site code
1E-GuaranteedState-Fix-	Fix	**Set CM client cache size to %MaxMB% MB** Com Object: UIResource.UIResourceMgr.GetCacheInfo().TotalSize	**MaxMB** The cache

Name	Type	Readable Payload and summary	Parameters
MEMCM-SetCacheSize			size should be at least this size (in MB) DEFAULT: 5120
1E-GuaranteedState-Fix-MEMCM-SetClientProvisioningMode	Fix	**Set MEMCM client provisioning mode to %TrueFalse%** Namespace: ROOT\CCM Class: SMS_CLIENT Method: SetClientProvisioningMode bEnable: <true/false>	**TrueFalse** *True* sets client provisioning mode to ON *False* sets client provisioning mode to OFF DEFAULT: False Valid Values: True False
1E-GuaranteedState-Fix-	Fix	**Set %ServiceName% service to Automatic start type and confirm change within %Timeout% seconds**	**Service Name**

Name	Type	Readable Payload and summary	Parameters
Service-SetStartTypeAutomatic			The name of the service on which we want to operate **Timeout** The maximum number of seconds to wait for the fix to enforce the correct state before considering it "fixed" or not DEFAULT: 15
1E-GuaranteedState-Fix-Service-SetStartTypeAutomat	Fix	**Set %ServiceName% service to Automatic (Delayed Start) start type and confirm change within %Timeout% seconds**	**Service Name** The name of the service on

Name	Type	Readable Payload and summary	Parameters
icDelayedStart			which we want to operate **Timeout** The maximum number of seconds to wait for the fix to enforce the correct state before considering it "fixed" or not DEFAULT: 15
1E-GuaranteedState-Fix-Service-SetStartTypeManual	Fix	**Set %ServiceName% service to Manual start type and confirm change within %Timeout% seconds**	**Service Name** The name of the service on which we want to operate

Name	Type	Readable Payload and summary	Parameters
			Timeout The maximum number of seconds to wait for the fix to enforce the correct state before considering it "fixed" or not DEFAULT: 15
1E-GuaranteedState-Fix-Service-Start	Fix	**Start %ServiceName% service and confirm as started within %Timeout% seconds**	**Service Name** The name of the service on which we want to operate **Timeout** The maximum number

Name	Type	Readable Payload and summary	Parameters
			of seconds to wait for the fix to enforce the correct state before considering it "fixed" or not DEFAULT: 15
1E-GuaranteedState-Fix-Wmi-Repository	Fix	**Fix the consistency of the WMI Repository and ResetRepository command if %ResetRepository%=True** SALVAGE: winmgmt /salvagerepository RESET: (optional) winmgmt /resetrepository	**ResetRepository** *True* will reset the WMI repository (only if salvage fails) *False* will only try to salvage
1E-GuaranteedState-Precondition-	PreCondition	**Multiple checks using specified parameters %1EClientVersionToCompare% %1EClientVersionDesiredResult% %DeviceChassisTypeList% %DeviceCpuTypeList% %DeviceDomainList% %DeviceFqdnList% %DeviceManufacturerList% %DeviceModelList% %DeviceRamMBMin% %DeviceRamMBMax% %DeviceTimeZoneOffsetList% %DirectoryExists% %DirectoryName% %DnsLookupFqdnList% %FileNameExists% %FileName% %OsTypeList% %OsArchitectureList% %ProcessExists% %ProcessExecutableList% %QuarantineStatus% %RegistryExists% %Regist**	1E Client... **1EClientVersionToCompare**

Name	Type	Readable Payload and summary	Parameters
Multiple		**ryHive% %RegistryKey% %RegistryValue% %RegistryData% %ServiceExists% %ServiceName% %ServiceStartAccountName% %ServiceStartType% %ServiceState% %ServiceTriggerStart% %ServiceType% %SoftwareExists% %SoftwareProduct% %SoftwarePublisher% %SoftwareVersionToCompare% %SoftwareVersionDesiredResult% %WindowsUpdateSource% %WmiNamespace% %WmiClass% %WmiColumn% %WmiWhereClause% %WmiVersionToCompare% %WmiDesiredResult%** Most parameters will be ignored if % is entered so they don't take up any resources trying to lookup a precondition on something that isn't relevant. The default values for the parameters will do this. In other words, if you don't want to search for a precondition on something like a directory, leave it's parameters at their defaults and it will skip the search for that.	The version to use as the comparison DEFAULT: 0 **1EClient Version Desired Result** The outcome that's desired when the 1E Client Version is compared to the passed in version DEFAULT: Same or Higher Device details... **DeviceChassisTypeList**

Name	Type	Readable Payload and summary	Parameters
			A semi-colon separated list of acceptable ChassisType values. (% wildcards are acceptable within each item) DEFAULT: % **DeviceCpuTypeList** A semi-colon separated list of acceptable CpuType values. (% wildcards are acceptable within each item

Name	Type	Readable Payload and summary	Parameters
			DEFAULT: % **DeviceDomainList** A semi-colon separated list of acceptable Domain values. (% wildcards are acceptable within each item) DEFAULT: % **DeviceFqdnList** A semi-colon separated list of acceptable Fqdn values. (% wildcards are acceptable within

Name	Type	Readable Payload and summary	Parameters
			each item) DEFAULT: % **DeviceManufacturerList** A semi-colon separated list of acceptable Manufacturer values. (% wildcards are acceptable within each item) DEFAULT: % **DeviceModelList** A semi-colon separated list of acceptable Model

Name	Type	Readable Payload and summary	Parameters
			values. (% wildcards are acceptable within each item) DEFAULT: % **DeviceRamMBMin** The minimum amount of RAM (in MB) a device should have DEFAULT: 0 **DeviceRamMBMax** The minimum amount of RAM (in MB) a device

Name	Type	Readable Payload and summary	Parameters
			should have DEFAULT: 9223372036854775807 **DeviceTimeZoneOffsetList** A semi-colon separated list of acceptable time zone offsets Directory and File... **DirectoryExists** *Exists* if the directory should exist *Doesn't Exist* if the directory shouldn't exist

Name	Type	Readable Payload and summary	Parameters
			DEFAULT: % **DirectoryName** The name of the directory to check for existence DEFAULT: % **FileNameExists** *Exists* if the file should exist *Doesn't Exist* if the file shouldn't exist DEFAULT: Exists **FileName** The name of the file to check for

Name	Type	Readable Payload and summary	Parameters
			existence DEFAULT: % DNS... **DnsLookupFqdnList** A semi-colon separated list of acceptable Fqdns that have been looked up in DNS by the device DEFAULT: % Operating System... **OsArchitectureList** A semi-colon separated list of

Name	Type	Readable Payload and summary	Parameters
			acceptable OS Architectures DEFAULT: % **OsTypeList** A semi-colon separated list of acceptable OS Types DEFAULT: % Process... **Process Exists** *Exists* if the process should exist *Doesn't Exist* if the process shouldn't exist DEFAULT: Exists

Name	Type	Readable Payload and summary	Parameters
			ProcessExecutableList A semi-colon separated list of acceptable processes DEFAULT: % Quarantine... **QuarantineStatus** *Quarantined* if the device should be quarantined *NotQuarantined* if the device should not be quarantined DEFAULT: %

Name	Type	Readable Payload and summary	Parameters
			Registry Key... **Registry Exists** *Exists* if the registry key should exist *Doesn't Exist* if the registry key should not exist DEFAULT: Exists **Registry Hive** The registry hive in which the registry key should exist. Valid Values: • HK

Name	Type	Readable Payload and summary	Parameters
			CR • HKCC • HKCU • HKLM • HKU • % DEFAULT: % **Registry Key** The registry key to find in the specified hive DEFAULT: % **Registry Value**

Name	Type	Readable Payload and summary	Parameters
			Exists if the registry key value should exist *Doesn't Exist* if the registry key value should not exist DEFAULT: Exists **Registry Data** *Exists* if the registry key value data should exist *Doesn't Exist* if the registry key value data should not exist

Name	Type	Readable Payload and summary	Parameters
			DEFAULT: Exists Service... **ServiceExists** *Exists* if the registry key value data should exist *Doesn't Exist* if the registry key value data should not exist DEFAULT: Exists **Service Name** The short name of the service DEFAULT: % **ServiceStartAcco**

Name	Type	Readable Payload and summary	Parameters
			untName The account name under which the service starts DEFAULT: % **ServiceStartType** The start type of the service. Valid Values: • Automatic • Automati

Name	Type	Readable Payload and summary	Parameters
			c (DelayedStart) • Boot • Disabled • Manual • Syst

Name	Type	Readable Payload and summary	Parameters
			em • % DEFAULT: % **ServiceState** The state the service should be in Valid Values: • About to Continue • Pausing

Name	Type	Readable Payload and summary	Parameters
			• Paused • Running • Starting • Stopping • Stopped • %

Name	Type	Readable Payload and summary	Parameters
			DEFAULT: % **ServiceTriggerStart** Is the service set to TriggerStart Valid Values: • True • False • % DEFAULT: % **ServiceType** The type of service (use {none} to match null/em

Name	Type	Readable Payload and summary	Parameters
			pty value) Valid Values: • {none} • Filesystemdriver • Kernelldriver • Own

Name	Type	Readable Payload and summary	Parameters
			process • Sharedprocess • % DEFAULT: % Software... **SoftwareExists** *Exists* if the software should exist *Doesn't Exist* if the softwar

Name	Type	Readable Payload and summary	Parameters
			e shouldn't exist DEFAULT: Exists **SoftwareProduct** Check for this product name DEFAULT: % **SoftwarePublisher** Check for this publisher name DEFAULT: % **SoftwareVersionToCompare**The software product version to use as the comparison

Name	Type	Readable Payload and summary	Parameters
			DEFAULT: 0 **SoftwareVersionDesiredResult** The outcome that's desired when the software product version is compared to SoftwareVersionToCompare Valid values: • SameOrLower • Lo

Name	Type	Readable Payload and summary	Parameters
			wer • Lower_MajorLower • Lower_SameMajor • Lower

Name	Type	Readable Payload and summary	Parameters
			_SameMajorMinor • Lower_SameMajorMinorRelea

Name	Type	Readable Payload and summary	Parameters
			se • Same • Higher_SameMajorMinorRelease • Highe

Name	Type	Readable Payload and summary	Parameters
			r_SameMajorMinor • Higher_SameMajor • Higher_M

Name	Type	Readable Payload and summary	Parameters
			ajorHigher • Higher • SameOrHigher DEFAULT: SameOrHigher Windows Update...

Name	Type	Readable Payload and summary	Parameters
			WindowsUpdateSource The source to check for Windows Update connectivity Valid Values: • SCCM(MEMCM) • WSUSL(WSUS-Lo

Name	Type	Readable Payload and summary	Parameters
			call) • WSUSR (WSUS-Remote) • % DEFAULT: % WMI... **WmiNamespace** The WMI namespace to check existence (ROOT\cimv2 for

Name	Type	Readable Payload and summary	Parameters
			example) **WmiClass**The WMI class that should exist in specified namespace (ignored if %) **WmiWhereClause** The WHERE clause to use when querying this class (use {none} for no filter) **WmiColumn** The column name from querying the class

Name	Type	Readable Payload and summary	Parameters
			which holds a version string **WmiVersionToCompare** The software product version to use as the comparison DEFAULT: 0 **WmiVersionDesiredResult**The outcome that's desired when the software product version is compared to SoftwareVersionToCompare

Name	Type	Readable Payload and summary	Parameters
			Valid values: • SameOrLower • Lower • Lower_MajorLower • Lowe

Name	Type	Readable Payload and summary	Parameters
			r_SameMajor • Lower_SameMajorMinor • Lower_Sam

Name	Type	Readable Payload and summary	Parameters
			eMajorMinorRelease • Same • Higher_SameMajorMi

Name	Type	Readable Payload and summary	Parameters
			nor Release • Higher_SameMajorMinor • Higher_Sa

Name	Type	Readable Payload and summary	Parameters
			meMajor • Higher_MajorHigher • Higher • SameOrHi

Name	Type	Readable Payload and summary	Parameters
			gher DEFAULT: SameOrHigher

1.11.12.9.1.4.2 Spare fragments

The following fragments are included in the MEMCM Client Health Integrated Product Pack but are not used in any predefined rules. You can use these in rules that you create or modify in any policy.

Name	Type	Readable Payload and summary	Parameters
1E-GuaranteedState-Check-MEMCM-CertificateInStore	Check	**Check that the CM certificate is in the certificate store by looking in the CM client logs located in %**MEMCMLogsDirectory% This checks the ClientIDManagerStartup.log for "Failed to find the certificate in the store" error messages, which indicates the CM client certificate is likely missing.	**MEMCMLogs Directory** The full path to the MEMCM client logs directory (%Environment% variables accepted)
1E-GuaranteedState-Check-MEMCM-ClientCommunication	Check	**Check that the CM client has sent data back within the last %Days% days.** This checks to see if hardware inventory, software inventory, DDRs or IDMIFs have been sent anytime in the past %Days% days.	**Days** Look for client messages sent back in this number of days

Name	Type	Readable Payload and summary	Parameters
1E-GuaranteedState-Check-MEMCM-MachinePolicyValid	Check	**Check that the CM client has checked for machine policy with in the last %Days% days**	**Days** Look for machine policy validated within this number of days
1E-GuaranteedState-Check-MEMCM-UserPolicyValid	Check	**Check that the CM client has checked for user policy within the last %Days% days**	**Days** Look for user policy validated within this number of days
1E-GuaranteedState-Fix-MEMCM-InstallClient	Fix	**Install the CM client using CCMSETUP.EXE from %CcmSetupFileUrl% having size %CcmSetupFileSize% and hash %CcmSetupFileHash% with command line options %SourceList%, %MpList%, %RetryMinutes%, %ServiceNoService%, %InstallUninstall%, %Logon%, %ForceReboot%, %BITSPriority%, %DownloadTimeout%, %UsePKICert%, %NoCRLCheck%, %ConfigFile%, %SkipPrereqFileList%, %ForceInstall%, %ExcludeFeaturesList%, %CcmSetupMsiProperties%, %ClientMsiProperties%** This is essentially a front-end for the ccmsetup.exe installation parameters found in Microsoft Documentation. See https://docs.microsoft.com/en-us/configmgr/core/clients/deploy/about-client-installation-properties for more information about the installation parameters.	Expand parameters... **CcmSetupFileUrl**Either the full HTTP or HTTPS URL path to the ccmsetup.exe file on a web server or the relative path to be appended to the Content directory under the background channel URL

Name	Type	Readable Payload and summary	Parameters
			DEFAULT: ccmsetup.exe **CcmSetupFileSize**The size of the ccmsetup.exe file in bytes DEFAULT: 4099328 **CcmSetupFileHash** The SHA256 hash of the ccmsetup.exe file DEFAULT: ab85f58b0cc257d25628384b0ec8fab1f9e15ca2b110a1e425e86e56b47ebde1 **SourceList** A semicolon ; delimited list of download locations for setup media DEFAULT: {none} **MpList** A semicolon ; delimited list

Name	Type	Readable Payload and summary	Parameters
			of management points or cloud management gateway DEFAULT: {none} **RetryMinutes** The retry interval in minutes to retry setup if it fails to download installation files. -1 to ignore this parameter DEFAULT: -1 **ServiceNoService**Tells setup to install as a service or no service DEFAULT: Service Valid Values: Service NoService **InstallUninstall**

Name	Type	Readable Payload and summary	Parameters
			Tell setup to install or uninstall the client DEFAULT: Install Valid Values: Install Uninstall **Logon** If any version of the client is already installed, install will stop DEFAULT: False Valid Values: True False **ForceReboot** Setup should force the client to reboot if necessary to complete installation Valid Values:

Name	Type	Readable Payload and summary	Parameters
			True False **BITSPriority** Download priority when client installation files are downloaded over HTTP connection DEFAULT: Normal Valid Values: Foreground High Normal Low **DownloadTimeout** Length of time in minutes that setup tries to download the installation files before stopping DEFAULT: 1440 **UsePKICert**

Name	Type	Readable Payload and summary	Parameters
			Uses a PKI cert that includes client authentication, if available. If can't find a valid cert, it uses HTTP with self-signed cert. DEFAULT: False Valid Values: True False **NoCRLCheck** Client won't check the cert revocation list when it uses HTTPS with PKI cert DEFAULT: False Valid Values: True False **ConfigFile** The name of a text file that lists client

Name	Type	Readable Payload and summary	Parameters
			installation properties DEFAULT: {none} **SkipPrereqFileList** A semicolon ; delimited list of prerequisite files that will be skipped during install DEFAULT: {none} **ForceInstall** Uninstall any existing client and install a new client DEFAULT: False Valid Values: True False **ExcludeFeaturesList** Do not install the semicolon ; delimited list of features

Name	Type	Readable Payload and summary	Parameters
			(ClientUI is supported) when installing the client DEFAULT: {none} Valid Values: ClientUI **CcmSetupMsiProperties** Properties that modify the installation behavior of ccmsetup.msi DEFAULT: {none} **ClientMsiProperties** Properties that modify the installation behavior of client.msi DEFAULT: {none}
1E-GuaranteedState-Fix-	Fix	**Invoke CM Application manager global evaluation action** Namespace: ROOT\CCM	

Name	Type	Readable Payload and summary	Parameters
MEMCM-InvokeApplicationManagerGlobalEvaluationAction		Class: SMS_CLIENT Method: TriggerSchedule ScheduleId: {00000000-0000-0000-0000-000000000123}	
1E-GuaranteedState-Fix-MEMCM-InvokeApplicationManagerPolicyAction	Fix	**Invoke CM Application manager policy action** Namespace: ROOT\CCM Class: SMS_CLIENT Method: TriggerSchedule ScheduleId: {00000000-0000-0000-0000-000000000121}	
1E-GuaranteedState-Fix-MEMCM-InvokeApplicationManagerUserPolicyAction	Fix	**Invoke CM Application manager user policy action** Namespace: ROOT\CCM Class: SMS_CLIENT Method: TriggerSchedule ScheduleId: {00000000-0000-0000-0000-000000000122}	
1E-GuaranteedState-Fix-MEMCM-InvokeBranchDistributionPointMaint	Fix	**Invoke CM branch distribution point maintenance task** Namespace: ROOT\CCM Class: SMS_CLIENT Method: TriggerSchedule ScheduleId: {00000000-0000-0000-0000-000000000109}	

Name	Type	Readable Payload and summary	Parameters
enanceTask			
1E-GuaranteedState-Fix-MEMCM-InvokeClearingProxySettingsCache	Fix	**Invoke CM clearing proxy settings cache action** Namespace: ROOT\CCM Class: SMS_CLIENT Method: TriggerSchedule ScheduleId: {00000000-0000-0000-0000-000000000037}	
1E-GuaranteedState-Fix-MEMCM-InvokeClientMachineAuthentication	Fix	**Invoke CM client machine authentication action** Namespace: ROOT\CCM Class: SMS_CLIENT Method: TriggerSchedule ScheduleId: {00000000-0000-0000-0000-000000000012}	
1E-GuaranteedState-Fix-MEMCM-InvokeDataDiscoveryRecord	Fix	**Invoke CM data discovery record action** Namespace: ROOT\CCM Class: SMS_CLIENT Method: TriggerSchedule ScheduleId: {00000000-0000-0000-0000-000000000001}	
1E-GuaranteedState-Fix-MEMCM-InvokeDiscoveryDa	Fix	**Invoke CM discovery data collection cycle** Namespace: ROOT\CCM Class: SMS_CLIENT Method: TriggerSchedule	

Name	Type	Readable Payload and summary	Parameters
taCollectionCycle		ScheduleId: {00000000-0000-0000-0000-000000000103}	
1E-GuaranteedState-Fix-MEMCM-InvokeEndpointAMPolicyReevaluate	Fix	**Invoke CM Endpoint Protection Antimalware policy reevaluation** Namespace: ROOT\CCM Class: SMS_CLIENT Method: TriggerSchedule ScheduleId: {00000000-0000-0000-0000-000000000222}	
1E-GuaranteedState-Fix-MEMCM-InvokeEndpointDeploymentReevaluate	Fix	**Invoke CM Endpoint Protection deployment reevaluation** Namespace: ROOT\CCM Class: SMS_CLIENT Method: TriggerSchedule ScheduleId: {00000000-0000-0000-0000-000000000221}	
1E-GuaranteedState-Fix-MEMCM-InvokeExternalEventDetection	Fix	**Invoke CM external event detection** Namespace: ROOT\CCM Class: SMS_CLIENT Method: TriggerSchedule ScheduleId: {00000000-0000-0000-0000-000000000223}	
1E-GuaranteedState-Fix-MEMCM-	Fix	**Invoke CM file collection** Namespace: ROOT\CCM Class: SMS_CLIENT	

Name	Type	Readable Payload and summary	Parameters
InvokeFileCollection		Method: TriggerSchedule ScheduleId: {00000000-0000-0000-0000-000000000010}	
1E-GuaranteedState-Fix-MEMCM-InvokeFileCollectionCycle	Fix	**Invoke CM file collection cycle** Namespace: ROOT\CCM Class: SMS_CLIENT Method: TriggerSchedule ScheduleId: {00000000-0000-0000-0000-000000000104	
1E-GuaranteedState-Fix-MEMCM-InvokeHardwareInventory	Fix	**Invoke CM hardware inventory** Namespace: ROOT\CCM Class: SMS_CLIENT Method: TriggerSchedule ScheduleId: {00000000-0000-0000-0000-000000000001}	
1E-GuaranteedState-Fix-MEMCM-InvokeHardwareInventoryCollectionCycle	Fix	**Invoke MEMCM hardware inventory collection cycle** Namespace: ROOT\CCM Class: SMS_CLIENT Method: TriggerSchedule ScheduleId: {00000000-0000-0000-0000-000000000101}	
1E-GuaranteedState-Fix-MEMCM-InvokeID	Fix	**Invoke CM IDMIF collection** Namespace: ROOT\CCM Class: SMS_CLIENT Method: TriggerSchedule	

Name	Type	Readable Payload and summary	Parameters
MIFCollection		ScheduleId: {00000000-0000-0000-0000-000000000011}	
1E-GuaranteedState-Fix-MEMCM-InvokeIDMIFCollectionCycle	Fix	**Invoke CM IDMIF collection cycle** Namespace: ROOT\CCM Class: SMS_CLIENT Method: TriggerSchedule ScheduleId: {00000000-0000-0000-0000-000000000105}	
1E-GuaranteedState-Fix-MEMCM-InvokeLSRefreshLocationsTask	FIx	**Invoke CM client Location Services refresh locations task** Namespace: ROOT\CCM Class: SMS_CLIENT Method: TriggerSchedule ScheduleId: {00000000-0000-0000-0000-000000000024}	
1E-GuaranteedState-Fix-MEMCM-InvokeLSTimeoutRefreshTask	Fix	**Invoke CM client Location Services timeout refresh action** Namespace: ROOT\CCM Class: SMS_CLIENT Method: TriggerSchedule ScheduleId: {00000000-0000-0000-0000-000000000025}	
1E-GuaranteedState-Fix-MEMCM-InvokeMachinePol	Fix	**Invoke CM machine policy agent cleanup action** Namespace: ROOT\CCM Class: SMS_CLIENT Method: TriggerSchedule	

Name	Type	Readable Payload and summary	Parameters
icyAgent Cleanup		ScheduleId: {00000000-0000-0000-0000-000000000040}	
1E-GuaranteedState-Fix-MEMCM-InvokeMachinePolicyAssignmentsRequest	Fix	**Invoke CM machine policy assignments request** Namespace: ROOT\CCM Class: SMS_CLIENT Method: TriggerSchedule ScheduleId: {00000000-0000-0000-0000-000000000021}	
1E-GuaranteedState-Fix-MEMCM-InvokeMachinePolicyEvaluation	Fix	**Invoke CM machine policy evaluation** Namespace: ROOT\CCM Class: SMS_CLIENT Method: TriggerSchedule ScheduleId: {00000000-0000-0000-0000-000000000022}	
1E-GuaranteedState-Fix-MEMCM-InvokePeerDpPendingPackageCheckSchedule	Fix	**Invoke CM peer DP pending package check schedule** Namespace: ROOT\CCM Class: SMS_CLIENT Method: TriggerSchedule ScheduleId: {00000000-0000-0000-0000-000000000062}	
1E-GuaranteedState-Fix-MEMCM-	Fix	**Invoke CM peer DP status reporting** Namespace: ROOT\CCM Class: SMS_CLIENT	

Name	Type	Readable Payload and summary	Parameters
InvokePeerDpStatusReporting		Method: TriggerSchedule ScheduleId: {00000000-0000-0000-0000-000000000061}	
1E-GuaranteedState-Fix-MEMCM-InvokePolicyAgentEvaluateAssignmentUser	Fix	**Invoke CM User policy evaluation** Namespace: ROOT\CCM Class: SMS_CLIENT Method: TriggerSchedule ScheduleId: {00000000-0000-0000-0000-000000000027}	
1E-GuaranteedState-Fix-MEMCM-InvokePolicyAgentRequestAssignmentUser	Fix	**Invoke CM User policy request** Namespace: ROOT\CCM Class: SMS_CLIENT Method: TriggerSchedule ScheduleId: {00000000-0000-0000-0000-000000000026}	
1E-GuaranteedState-Fix-MEMCM-InvokePolicyAgentValidateMachinePolicyAssignment	Fix	**Invoke CM machine policy / assignment validation** Namespace: ROOT\CCM Class: SMS_CLIENT Method: TriggerSchedule ScheduleId: {00000000-0000-0000-0000-000000000042}	

Name	Type	Readable Payload and summary	Parameters
1E-GuaranteedState-Fix-MEMCM-InvokePolicyAgentValidateUserPolicyAssignment	Fix	**Invoke CM user policy / assignment validation** Namespace: ROOT\CCM Class: SMS_CLIENT Method: TriggerSchedule ScheduleId: {00000000-0000-0000-0000-000000000043}	
1E-GuaranteedState-Fix-MEMCM-InvokePowerManagementStartSummarizer	Fix	**Invoke CM power management start summarizer** Namespace: ROOT\CCM Class: SMS_CLIENT Method: TriggerSchedule ScheduleId: {00000000-0000-0000-0000-000000000131}	
1E-GuaranteedState-Fix-MEMCM-InvokeRefreshDefaultMPTask	Fix	**Invoke CM refresh default MP task** Namespace: ROOT\CCM Class: SMS_CLIENT Method: TriggerSchedule ScheduleId: {00000000-0000-0000-0000-000000000023}	
1E-GuaranteedState-Fix-MEMCM-InvokeRe	Fix	**Invoke CM retrying/refreshing certificates in AD on MP** Namespace: ROOT\CCM Class: SMS_CLIENT Method: TriggerSchedule	

Name	Type	Readable Payload and summary	Parameters
tryingRefreshingCertificatesInAdOnMp		ScheduleId: {00000000-0000-0000-0000-000000000051}	
1E-GuaranteedState-Fix-MEMCM-InvokeScanByUpdateSource	Fix	**Invoke CM scan by update source** Namespace: ROOT\CCM Class: SMS_CLIENT Method: TriggerSchedule ScheduleId: {00000000-0000-0000-0000-000000000113}	
1E-GuaranteedState-Fix-MEMCM-InvokeSchedule	Fix	**Invoke CM client %Schedule% action** Namespace: ROOT\CCM Class: SMS_CLIENT Method: TriggerSchedule ScheduleId: <ScheduleID> **Tip** Click here to expand list of ScheduleIDs... Name / ScheduleId Hardware Inventory / {00000000-0000-0000-0000-000000000001} Software Inventory / {00000000-0000-0000-0000-000000000002} Data Discovery Record / {00000000-0000-0000-0000-000000000003}	**Schedule** The MEMCM client schedule (client action) to trigger Valid Values: Select a name from the table in the Summary column. These are presented as a dropdown in the UI. The string values are converted to the ScheduleID required by

Name	Type	Readable Payload and summary		Parameters
		File Collection	{00000000-0000-0000-0000-000000000010}	the WMI method.
		IDMIF Collection	{00000000-0000-0000-0000-000000000011}	
		Client Machine Authentication	{00000000-0000-0000-0000-000000000012}	
		Machine Policy Assignments Request	{00000000-0000-0000-0000-000000000021}	
		Machine Policy Evaluation	{00000000-0000-0000-0000-000000000022}	
		Refresh Default MP Task	{00000000-0000-0000-0000-000000000023}	
		LS (Location Service) Refresh Locations Task	{00000000-0000-0000-0000-000000000024}	
		LS (Location Service) Timeout Refresh Task	{00000000-0000-0000-0000-000000000025}	
		Policy Agent Request Assignment (User)	{00000000-0000-0000-0000-000000000026}	
		Policy Agent Evaluate Assignment (User)	{00000000-0000-0000-0000-000000000027}	
		Software Metering Generating Usage Report	{00000000-0000-0000-0000-000000000031}	

Name	Type	Readable Payload and summary	Parameters
		Source Update Message	{00000000-0000-0000-0000-000000000032}
		Clearing proxy settings cache	{00000000-0000-0000-0000-000000000037}
		Machine Policy Agent Cleanup	{00000000-0000-0000-0000-000000000040}
		User Policy Agent Cleanup	{00000000-0000-0000-0000-000000000041}
		Policy Agent Validate Machine Policy / Assignment	{00000000-0000-0000-0000-000000000042}
		Policy Agent Validate User Policy / Assignment	{00000000-0000-0000-0000-000000000043}
		Retrying/Refreshing certificates in AD on MP	{00000000-0000-0000-0000-000000000051}
		Peer DP Status reporting	{00000000-0000-0000-0000-000000000061}
		Peer DP Pending package check schedule	{00000000-0000-0000-0000-000000000062}
		SUM Updates install schedule	{00000000-0000-0000-0000-000000000063}
		Hardware Inventory Collection Cycle	{00000000-0000-0000-0000-000000000101}

Name	Type	Readable Payload and summary	Parameters
		Software Inventory Collection Cycle	{00000000-0000-0000-0000-000000000102}
		Discovery Data Collection Cycle	{00000000-0000-0000-0000-000000000103}
		File Collection Cycle	{00000000-0000-0000-0000-000000000104}
		IDMIF Collection Cycle	{00000000-0000-0000-0000-000000000105}
		Software Metering Usage Report Cycle	{00000000-0000-0000-0000-000000000106}
		Windows Installer Source List Update Cycle	{00000000-0000-0000-0000-000000000107}
		Software Updates Assignments Evaluation Cycle	{00000000-0000-0000-0000-000000000108}
		Branch Distribution Point Maintenance Task	{00000000-0000-0000-0000-000000000109}
		Send Unsent State Message	{00000000-0000-0000-0000-000000000111}
		State System policy cache cleanout	{00000000-0000-0000-0000-000000000112}
		Scan by Update Source	{00000000-0000-0000-0000-000000000113}

Name	Type	Readable Payload and summary	Parameters
		Update Store Policy	{00000000-0000-0000-0000-000000000114}
		State system policy bulk send high	{00000000-0000-0000-0000-000000000115}
		State system policy bulk send low	{00000000-0000-0000-0000-000000000116}
		Application manager policy action	{00000000-0000-0000-0000-000000000121}
		Application manager user policy action	{00000000-0000-0000-0000-000000000122}
		Application manager global evaluation action	{00000000-0000-0000-0000-000000000123}
		Power management start summarizer	{00000000-0000-0000-0000-000000000131}
		Endpoint deployment reevaluate	{00000000-0000-0000-0000-000000000221}
		Endpoint AM policy reevaluate	{00000000-0000-0000-0000-000000000222}
		External event detection	{00000000-0000-0000-0000-000000000223}
1E-GuaranteedState-	Fix	**Invoke CM send unsent state message action**	

Name	Type	Readable Payload and summary	Parameters
Fix-MEMCM-InvokeSendUnsentStateMessage		Namespace: ROOT\CCM Class: SMS_CLIENT Method: TriggerSchedule ScheduleId: {00000000-0000-0000-0000-000000000111}	
1E-GuaranteedState-Fix-MEMCM-InvokeSoftwareInventory	Fix	**Invoke CM software inventory action** Namespace: ROOT\CCM Class: SMS_CLIENT Method: TriggerSchedule ScheduleId: {00000000-0000-0000-0000-000000000002}	
1E-GuaranteedState-Fix-MEMCM-InvokeSoftwareInventoryCollectionCycle	Fix	**Invoke CM software inventory collection cycl**e Namespace: ROOT\CCM Class: SMS_CLIENT Method: TriggerSchedule ScheduleId: {00000000-0000-0000-0000-000000000102}	
1E-GuaranteedState-Fix-MEMCM-InvokeSoftwareMeteringGeneratingUsageReport	Fix	**Invoke CM software metering generate usage report action** Namespace: ROOT\CCM Class: SMS_CLIENT Method: TriggerSchedule ScheduleId: {00000000-0000-0000-0000-000000000031}	

Name	Type	Readable Payload and summary	Parameters
1E-GuaranteedState-Fix-MEMCM-InvokeSoftwareMeteringUsageReportCycle	Fix	**Invoke CM software metering usage report cycle** Namespace: ROOT\CCM Class: SMS_CLIENT Method: TriggerSchedule ScheduleId: {00000000-0000-0000-0000-000000000106}	
1E-GuaranteedState-Fix-MEMCM-InvokeSoftwareUpdatesAssignmentsEvaluationCycle	Fix	**Invoke CM software updates assignments evaluation cycle** Namespace: ROOT\CCM Class: SMS_CLIENT Method: TriggerSchedule ScheduleId: {00000000-0000-0000-0000-000000000108}	
1E-GuaranteedState-Fix-MEMCM-InvokeSourceUpdateMessage	Fix	**Invoke CM source update message** Namespace: ROOT\CCM Class: SMS_CLIENT Method: TriggerSchedule ScheduleId: {00000000-0000-0000-0000-000000000032}	
1E-GuaranteedState-Fix-MEMCM-InvokeSt	Fix	**Invoke CM state system policy bulk send high** Namespace: ROOT\CCM Class: SMS_CLIENT Method: TriggerSchedule	

Name	Type	Readable Payload and summary	Parameters
ateSystemPolicyBulkSendHigh		ScheduleId: {00000000-0000-0000-0000-000000000115}	
1E-GuaranteedState-Fix-MEMCM-InvokeStateSystemPolicyBulkSendLow	Fix	**Invoke CM state system policy bulk send low** Namespace: ROOT\CCM Class: SMS_CLIENT Method: TriggerSchedule ScheduleId: {00000000-0000-0000-0000-000000000116}	
1E-GuaranteedState-Fix-MEMCM-InvokeStateSystemPolicyCacheCleanout	Fix	**Invoke CM state system policy cache cleanout** Namespace: ROOT\CCM Class: SMS_CLIENT Method: TriggerSchedule ScheduleId: {00000000-0000-0000-0000-000000000112}	
1E-GuaranteedState-Fix-MEMCM-InvokeSumUpdatesInstallSchedule	Fix	**Invoke CM Software Updates install schedule** Namespace: ROOT\CCM Class: SMS_CLIENT Method: TriggerSchedule ScheduleId: {00000000-0000-0000-0000-000000000063}	
1E-GuaranteedState-	Fix	**Invoke CM update store policy**	

Name	Type	Readable Payload and summary	Parameters
Fix-MEMCM-InvokeUpdateStorePolicy		Namespace: ROOT\CCM Class: SMS_CLIENT Method: TriggerSchedule ScheduleId: {00000000-0000-0000-0000-000000000114}	
1E-GuaranteedState-Fix-MEMCM-InvokeUserPolicyAgentCleanup	Fix	**Invoke CM user policy agent cleanup** Namespace: ROOT\CCM Class: SMS_CLIENT Method: TriggerSchedule ScheduleId: {00000000-0000-0000-0000-000000000041}	
1E-GuaranteedState-Fix-MEMCM-InvokeWindowsInstallerSourceListUpdateCycle	Fix	**Invoke CM Windows Installer source list update cycle** Namespace: ROOT\CCM Class: SMS_CLIENT Method: TriggerSchedule ScheduleId: {00000000-0000-0000-0000-000000000107}	
1E-GuaranteedState-Fix-MEMCM-RefreshServerComplianceState	Fix	**Refresh CM server compliance state** Com Object: Microsoft.CCM.UpdatesStore.RefreshServerComplianceState()	

<table>
<tr><th>Name</th><th>Type</th><th>Readable Payload and summary</th><th>Parameters</th></tr>
<tr><td>1E-GuaranteedState-Fix-MEMCM-ResetPolicy</td><td>Fix</td><td>Reset CM policy
Namespace: ROOT\CCM
Class: SMS_CLIENT
Method: ResetPolicy
uFlags: <see list below>
<table><tr><th>Name</th><th>Flag</th></tr><tr><td>RequestFullPolicy</td><td>0</td></tr><tr><td>PurgeAndRequestFullPolicy</td><td>1</td></tr></table></td><td>ResetOption
Valid values
• RequestFullPolicy will request a full instead of delta.
• PurgeAndRequestFull will completely remove the existing policy and request full (possibly re-running deployments).
These are presented as a dropdown in the UIO and</td></tr>
</table>

Name	Type	Readable Payload and summary	Parameters
			converted to the numeric value required by the WMI method.
1E-GuaranteedState-Fix-WindowsUpdate-ResetWindowsUpdate	Fix	**Completely reset Windows Update from scratch (Experimental)** Process mostly inspired by https://gallery.technet.microsoft.com/Reset-WindowsUpdateps1-e0c5eb78 and tweaked a little to be more forceful Process also inspired by https://www.definit.co.uk/2012/02/powershell-recursively-taking-ownership-of-files-and-folders-and-adding-permissions-without-removing-existing-permissions/ **Warning** This is a very destructive and involved process. It should only be used as a last resort to fix a broken Windows Update system. The machine will be somewhat unusable until it is rebooted and should be rebooted right away. Many different and unrelated apps may throw odd and misleading errors until the reboot happens General process: 1. Stop Windows Update Services a. Stop BITS b. Stop wuauserv c. Stop appidsvc d. Stop cryptsvc 2. Remove QMGR Data File 3. Rename the software distribution and CatRoot folders	

Name	Type	Readable Payload and summary	Parameters
		4. Remove the old Windows Update log 5. Reset the Windows Update services to default settings (bits and wuauserv anyway) 6. Re-Register a pile of DLLS related to windows update and surrounding technologies 7. Remove the WSUS client settings from the registry 8. Reset WinSock 9. Delete any-and-all BITS jobs 10. Install the Windows Update Agent (KB2937636) 11. Force discovery 12. Reboot	
1E-GuaranteedState-Precondition-1EClient-Version	PreCondition	**Checks for the existence of the 1E client with version lower, same or higher (%DesiredResults%) than %VersionToCompare%.**	**VersionToCompare** A version number to compare against the installed 1E Client version number. Examples: 5 5.0 5.0.0 5.0.0.745 DEFAULT: 0 **DesiredResults**The outcome

Name	Type	Readable Payload and summary	Parameters
			that's desired when actual version is compared to passed in version. DEFAULT: SameOrHigher Valid values: • SameOrLower • Lower • Lower_MajorLower • Lower_SameMajor • Lower_SameMajorMinor • Lower_SameMajorMinorRelease • Same

Name	Type	Readable Payload and summary	Parameters
			• Higher_SameMajorMinorRelease • Higher_SameMajorMinor • Higher_SameMajor • Higher_MajorHigher • Higher • SameOrHigher
1E-GuaranteedState-Precondition-MEMCM-AssignedSite	Precondition	**Check the CM client is assigned to %SiteCode%**	**SiteCode** Check to see if the MEMCM client is assigned to this site code
1E-GuaranteedState-Precondit	Pre Co	**Check the CM cache size is between %MinMB% and %MaxMB%**	**MinMB** The cache size should be at least this

Name	Type	Readable Payload and summary	Parameters
ion-MEMCM-CacheSizeBetween	ndition		big (in Megabytes) **MaxMB**The cache size should be at most this big (in Megabytes)
1E-GuaranteedState-Precondition-MEMCM-CertificateInStore	PreCondition	**Check the CM certificate is in the certificate store by checking CM log files in %**MEMCMLogsDirectory% This checks the ClientIDManagerStartup.log for "Failed to find the certificate in the store" error messages, which indicates the CM client certificate is likely missing.	**MEMCMLogs Directory** The full path to the MEMCM client logs directory (%Environment% variables accepted)
1E-GuaranteedState-Precondition-MEMCM-ClientCommunication	PreCondition	**Check the CM client has sent data back within the last %Days% days** This checks to see if hardware inventory, software inventory, DDRs or IDMIFs have been sent anytime in the past %Days% days.	**Days** Look for client messages sent back in this number of days
1E-GuaranteedState-Precondition-MEMCM-ClientPro	PreConditi	**Check if the CM ClientProvisioningMode is set to %TrueFalse%**	**TrueFalse** True represents client provisioning ON, False represents client

Name	Type	Readable Payload and summary	Parameters
visioningMode	on		provisioning OFF
1E-GuaranteedState-Precondition-MEMCM-DataDiscoveryRecordSent	PreCondition	**Check the CM client has sent a DDR (Data Discovery Record) within the last %Days% days**	**Days** Look for DDRs sent back in this number of days
1E-GuaranteedState-Precondition-MEMCM-FileCollectionSent	PreCondition	**Check the CM client has performed a file collection within the last %Days% days**	**Days** Look for file collection sent back in this number of days
1E-GuaranteedState-Precondition-MEMCM-GlobalLogginConfiguration	PreCondition	**Check the CM client logging is configured with %Loglevel%, %MaxSize%, %MaxHistoryFiles% and %DebugLogging% settings configuration %LogLevel% %MaxSize% %MaxHistoryFiles% %DebugLogging%**	**LogLevel** The logging level Valid Values: Verbose, Normal, None **MaxSize** The maximum size (in Bytes) that the MEMCM logs may grow

Name	Type	Readable Payload and summary	Parameters
			before rolling over **MaxHistoryFiles** The number of incremented log files to accumulate before deleting **DebugLogging** True means debug logging should be on, False means it should be off
1E-GuaranteedState-Precondition-MEMCM-HardwareInventorySent	PreCondition	**Check the CM client has sent hardware inventory within the last %Days% days**	**Days** Look for hardware inventory data sent back in this number of days
1E-GuaranteedState-Precondition-MEMCM-IDMIFColl	PreConditi	**Check the CM client has performed an IDMIF collection within the last %Days% days**	**Days** Look for IDMIFs sent back within this number of days

Name	Type	Readable Payload and summary	Parameters
ectionSent	on		
1E-GuaranteedState-Precondition-MEMCM-MachinePolicyValid	PreCondition	**Check the CM client has checked for machine policy within the last %Days% days**	**Days** Look for machine policy validated within this number of days
1E-GuaranteedState-Precondition-MEMCM-SoftwareInventorySent	PreCondition	**Check the CM client has sent software inventory within the last %Days% days.**	**Days** Look for software inventory data sent back within this number of days
1E-GuaranteedState-Precondition-MEMCM-StatusMessagesSent	PreCondition	**Check the CM client has sent status messages within the last %Days% days.**	**Days** Look for status messages sent back within this number of days
1E-GuaranteedState-Precondition-MEMCM-	PreConditi	**Check the CM client has checked for user policy within the last %Days% days**	**Days** Look for user policy validated within this

Name	Type	Readable Payload and summary	Parameters
UserPolicyValid	on		number of days
1E-GuaranteedState-Precondition-Process-Exists	PreCondition	**Check the %Executable% process exists (is running)**	**Executable** The name of the executable that should be running
1E-GuaranteedState-Precondition-Service-Exists	PreCondition	**Check the %ServiceName% service exists**	**ServiceName** Shortname of the service
1E-GuaranteedState-Precondition-Software-Exists	PreCondition	**Check for the existence of %Publisher% %Product% with version %VersionDesiredResult% than %VersionToCompare%** Checks if the specified Publisher and Product is installed and that the version is lower, same or higher than the target (VersionToCompare	**Publisher** Check for this publisher name **Product** Check for this product name **VersionToCompare** The software product version to use

Name	Type	Readable Payload and summary	Parameters
			as the comparison DEFAULT: 0 **VersionDesiredResult**The outcome that's desired when the software product version is compared to SoftwareVersionToCompare Valid values: • SameOrLower • Lower • Lower_MajorLower • Lower_SameMajor • Lower_SameMajorMinor • Lower_SameMajorMinor

Name	Type	Readable Payload and summary	Parameters
			Release • Same • Higher_SameMajorMinorRelease • Higher_SameMajorMinor • Higher_SameMajor • Higher_MajorHigher • Higher • SameOrHigher DEFAULT: SameOrHigher
1E-GuaranteedState-Precondition-Windows Update-	PreConditi	**Check that the Windows Update connection is OK**	

Name	Type	Readable Payload and summary	Parameters
ConnectionOK	on		
1E-GuaranteedState-Precondition-Windows Update-Source	PreCondition	**Check that the connection to the %Source% Windows Update source is OK**	**Source** The windows update source (% wildcard accepted) Valid Values: • SCCM (MEMCM) • WSUSL (WSUS-Local) • WSUSR (WSUS-Remote) • % DEFAULT: %
1E-GuaranteedState-Precondition-Windows	PreConditi	**Check that a Windows Update connection is OK for %SourceId%**	**SourceId** The identity of the source of updates. E.g. for a '*SCCM*' source this will be

Name	Type	Readable Payload and summary	Parameters
Update-SourceId	on		the site ID, or for WSUS it will be the URL to WSUS.
1E-GuaranteedState-Precondition-Wmi-ClassColumnVersion	PreCondition	**Check if the value of the WMI attribute defined by %Namespace%, %Class%, %ColumnName% (and optional %WhereClause%) is a version number (e.g. 7.2.5.612) that is lower, higher or the same (defined by %DesiredResult%) as %VersionToCompare%**	**Namespace** The WMI namespace to check existence (ROOT\cimv2 for example) **Class**The WMI class that should exist in specified namespace (ignored if %) **WhereClause** The WHERE clause to use when querying this class (use {none} for no filter) **ColumnName** The column name from querying the class which holds a version string **VersionToCompare**

Name	Type	Readable Payload and summary	Parameters
			The software product version to use as the comparison DEFAULT: 0 **DesiredResult** The outcome that's desired when the software product version is compared to SoftwareVersionToCompare Valid values: • Same OrLower • Lower • Lower_MajorLower • Lower_SameMajor • Lower_SameMajorMinor • Lower_Same

Name	Type	Readable Payload and summary	Parameters
			Major Minor Release • Same • Higher_Same Major Minor Release • Higher_Same Major Minor • Higher_Same Major • Higher_MajorHigher • Higher • SameOrHigher DEFAULT: SameOrHigher
1E-GuaranteedState-Precondition-Wmi-	PreCon	**Check for the existence of WMI %Class% in %NameSpace%**	**Namespace** The WMI namespace to check

Name	Type	Readable Payload and summary	Parameters
ClassExists	dition		existence (ROOT\cimv2 for example) **Class**The WMI class that should exist in specified namespace (ignored if %)
1E-GuaranteedState-Precondition-Wmi-ClassQuery	PreCondition	**Check for any data returned from specified WMI %Class% and %Namespace% using (optional) %WhereClause% and %ColumnList%**	**Namespace** The WMI namespace to check existence (ROOT\cimv2 for example, ignored if %) **Class**The WMI class that should exist in specified namespace (ignored if %) **WhereClause** The WHERE clause to use when querying this class (use {none} for no filter) **ColumnList** A list of columns to

Name	Type	Readable Payload and summary	Parameters
			select from the WMI class (use {all} for all columns)
1E-GuaranteedState-Precondition-Wmi-NamespaceExists	Precondition	**Check for the existence of WMI %Namespace%**	**Namespace** The WMI namespace to check existence (ROOT\cimv2 for example)
1E-GuaranteedState-Precondition-Wmi-RepositoryConsistent	Precondition	**Check that the WMI repository is consistent** Runs winmgmt.exe /verifyrepository and fails if 'is not consistent' appears in the returned result	

1.11.12.9.1.5 Trigger templates

The following table shows the trigger templates included in the Nomad Client Health Integrated Product Pack.

> **Note**
>
> The **Parameters** column in the following table shows the ranges and default values for the parameters. The default values are used when you create custom rules using these templates, unless you select alternative values.

Name	Readable Payload and summary	Parameters
TriggerTemplate-FileChange	**On change of file "<fileName>"** When a file changes (Windows only)	**File Name** • File path of

Name	Readable Payload and summary	Parameters
		file to be monitored, default is null.
TriggerTemplate-IntervalHours	**Every <intervalHours> hours** Periodic (hours)	**Interval Hours** • 0 to 999 hours (approximately 42 days), default interval is 12 hours.
TriggerTemplate-IntervalMinutes	**Every <intervalMinutes> minutes** Periodic (minutes)	**Interval Minutes** • 0 to 99,999 minutes (approximately 69 days), default interval is 30 minutes.
TriggerTemplate-IntervalSeconds	**Every <intervalSeconds> seconds** Periodic (seconds)	**Interval Seconds** • 0 to 999,99

Name	Readable Payload and summary	Parameters
		9 seconds (approximately 11 days), default interval is 3600 seconds (1 hour).
TriggerTemplate-ProcessCrash	**On crash of process "<executable>"** When a process crashes (Windows only) Monitors the Windows Application Event Log for event 1000. Executable is case insensitive but is required to be the whole filename without the folder path, such as unreliableapp.exe A partial string such as unreliableapp will not trigger on a crash of unreliableapp.exe.	**Executable** • Filename of executable to be monitored, default is empty.
TriggerTemplate-ProcessLaunch	**On launch of process "<executable>"** When a process starts (Windows only) Monitors the Windows Security Event Log for event 4688.	**Executable** • File path of executable to be monitored, default is empty.
TriggerTemplate-	**On change of running state of the "<serviceName>" service**	**Service Name**

Name	Readable Payload and summary	Parameters
ServiceStatusChange	When the state of the named Windows service changes You can determine the short name of a service using the PowerShell cmdlet `get-service -DisplayName "Network Location Awareness"` This will return **NlaSvc** in the above example. It is this short name you specify in the <ServiceName> parameter.	• Short name of service - for example Nomad Branch.

TriggerTemplate-WindowsEventLog	**On Windows"<channel>"; event log entry matching "<query>" (debounce for <debounce> seconds)**
	
	When an event log entry is created (Windows only)
	
	A **channel** is an event sink, example standard channel names are Application or Security.
	
	To determine the available event channels execute the following PowerShell command:
	
	`Get-WinEvent -ListLog *`
	
	Or to view the event channels on a remote computer:
	
	`Get-WinEvent -ListLog * -ComputerName <hostname>`
	
	Similarly to view event log entries for a given channel either use Event Viewer or from PowerShell for example:
	
	`Get-EventLog application | where {($_.EntryType -Match "Error") -or ($_.EntryType -Match "Warning")}`
	
	Or:
	
	`[dateTime]$oneWeekAgo = (get-date).addDays(-7)`
	`Get-EventLog -LogName Application -After $oneWeekAgo -computerName . \| ? {$_.EventID -eq 1000}`
		Channel
		• Text string, default null.
		
		Query
		• Text string, default null.
		
		Debounce Time Seconds
		• 0 to 99 seconds, default 0.

Name	Readable Payload and summary	Parameters
	A **query** is used to filter the event log messages for a given channel. Examples can be found at https://docs.microsoft.com/en-us/windows/win32/wes/consuming-events. For example to query all OneNote application crashes error log messages: *[System[(Level=2) and (EventID=1000)]] and *[EventData[Data='onenote.exe']] **Debounce** is a settling period to ensure that in the case of multiple events, only a single event is registered within the space of a given time period.	
TriggerTemplate-WindowsRegistryChange	**On change of registry values in "<hive>\<subkey>" (include subkeys=<includeSubkeys>)** When the value of a Windows registry key changes.	**Hive**, which must be one of: • HKLM (default) • HKCR **Subkey**: free text string, default empty. **Include Sub Keys** : 1/0 default 0.

1.11.12.10 1E Nomad product pack

Classic product pack used to create the **1E Nomad** instruction set in Tachyon, required by the following Nomad features:

- Downloads tab on Device views - instructions used to populate details about Content download and other Nomad features
- Nomad Download Pause - instructions used by the CM Admin Console extensions
- Instructions to help with the following Nomad features: Nomad cache, CacheCleaner, Single Site Download, Nomad jobs, NomadBranch service.

1.11.12.10.1 Nomad Client Health integrated product pack

Integrated Product Pack used to create the **Nomad Client Health** instruction set and **Nomad Client Health** policy.

For more information, please refer to Nomad Client Health Policy.

Nomad is included as part of the 1E Client, and as part of that integration, we offer a Nomad client health compliance policy in Guaranteed State. This verifies common Nomad requirements such as ACP registration, disk availability, firewall exceptions, crash notifications and cache monitoring.

The Nomad client health policy replaces the client health tile in the Nomad dashboard plus additional remediation steps:

- Keeps content distribution services up and running on Nomad clients, so that users are secure and productive
- Ensures Alternative Content Provider (ACP) registration configuration is set
- Maintains optimal disk availability and monitors cache size for storage capacity planning
- Enforces Firewall exceptions.

Note

This policy is intended for deployment to Windows devices only.

1.11.12.10.1.1 Instructions

The following table shows the instructions included in the Integrated Product Pack. Unless already uploaded, the following instructions are added to an Instruction set named: **Nomad Client Health**

Readable Payload	Type	Description	Name	Version
P2P election weight vs criticality	Question	Returns the Nomad peer-to-peer election weight and the criticality of the device. This instruction is useful if you use - and want to correlate - the Nomad feature Sensitive server weighting and the Tachyon feature Using Device Criticality. The P2PElectionWeight registry entry does not exist unless it is explicitly set - for example by a Configuration Manager baseline or Tachyon instruction. If the registry entry does not exist the response will be **Not set**. Similarly, the	**1E-Explorer-NomadClientHealth-ElectionWeightVsCriticality**	3

Readable Payload	Type	Description	Name	Version
		default criticality value assigned to a device is **Undefined**. The following is an extract from Election weighting: Click here to expand... Nomad performs automatic weighting depending on its situation, according to the criteria listed below, and stores the value in memory (not registry). The higher the value, the greater the probability of winning the election. • 61 – the agent is running on a server OS and it is not a domain controller (DC) • 40 – the agent is running on a laptop • 30 – the agent is running on a wireless network • 10 – the agent is running on WinPE • 50 – default If necessary, you can use the P2PElectionWeight registry setting to increase or decrease a Nomad client's probability of being elected a master. The range for this registry value must be between 0 and 99 inclusive. If not set, Nomad uses the values listed above. • The registry key is located at: *HKLM\software\1e\NomadBranch\P2PElectionWeight* To take effect after setting the registry value, the client service must be restarted. This method is not recommended because Nomad is already quite efficient in the way it		

Readable Payload	Type	Description	Name	Version

elects a master and needs very little intervention in this process. However, you may want to reduce the chance of computers with low processing power, or prevent critical servers, becoming a master.

You should also consider the following points before you influence the weighting:

- Use this technique in exceptional circumstances and only after testing has shown that you need to make a particular computer more or less likely to be elected as a master for specific operational reasons.
- Choose the simplest weighting strategy possible - for example, set servers at 90, laptops at 10 and workstations at 50.
- The weighting does not guarantee that the more heavily weighted computers will win the election – they may be turned off or another local peer may have already cached more of the requested content.
- The final weighting value used by the computer during an election may differ from the registry value as Nomad will automatically adjust it depending on the chassis and the network connection used.
- In the event you no longer need the values to be set, you should remove it and restart the service to resume dynamic election weighting.

Setting to 0 is a special case called Sensitive server weighting designed for use on critical

Readable Payload	Type	Description	Name	Version
		servers. The 0 value prevents Nomad from acting as master, and devices with this value will not respond to election requests.		

1.11.12.10.1.2 Policies

The following table shows the policies included in the Nomad Client Health Integrated Product Pack:

Name	Description
Nomad Client Health	The Nomad Client Health policy ensures that the health of the Nomad client is compliant with a reference baseline.

1.11.12.10.1.3 Rules

The following table shows the rules included in the Nomad Client Health Integrated Product Pack:

> **Note**
>
> Any parameter values shown in the table below are specifically set in the rules when the pack is uploaded. These may be different to the default values shown in the Fragments and Trigger templates tables. You can modify these if required.

Name	Type	Description	Check and Fix fragments	Triggers	Precondition fragment
Check Nomad ActiveEfficiency connectivity status	Check	Checks the Nomad agent connectivity to ActiveEfficiency.	1E-GuaranteedState-Nomad-Check-AEConnectivity • No parameters	TriggerTemplate-WindowsRegistryChange • Hive=*HKLM* • *Subkey=Software\1E\Nomad Branch\ActiveEfficiency* • Include Sub keys=0 TriggerTemplate-IntervalHours • intervalHours=1	1E-GuaranteedState-Nomad-PreCondition-MultiTests • hasCmClient=0 • sccmDp=0

Name	Type	Description	Check and Fix fragments	Triggers	Precondition fragment
					• smbEnabled=0
Check Nomad can communicate through the Windows Firewall	Check	Check that there are Windows Firewall program exceptions for Nomad and its related executables.	1E-GuaranteedState-Nomad-Check-FirewallExceptions • No parameters	TriggerTemplate-WindowsRegistryChange • Hive=*HKLM* • *Subkey=Software\1E\Nomad Branch\NomadBranch* • Include Sub keys=1 TriggerTemplate-IntervalHours • intervalHours=1	1E-GuaranteedState-Nomad-PreCondition-MultiTests • hasCmClient=0 • sccmDp=0 • smbEnabled=0
Ensure Nomad can communicate through the Windows Firewall	Fix	Ensures there are Windows Firewall program exceptions for Nomad and its related executables.	1E-GuaranteedState-Nomad-Check-FirewallExceptions • No parameters 1E-GuaranteedState-Nomad-Fix-FirewallExceptions • No para	TriggerTemplate-IntervalHours • intervalHours=1	1E-GuaranteedState-Nomad-PreCondition-MultiTests • hasCmClient=0 • sccmDp=0 • smbEnabled=0

Name	Type	Description	Check and Fix fragments	Triggers	Precondition fragment
			meters		
Check Nomad can generate LSZ files on ConfigMgr distribution points	Check	Check that LSZ generation is enabled on ConfigMgr distribution points.	1E-GuaranteedState-Nomad-Check-DpLszEnabled • No parameters	TriggerTemplate-WindowsRegistryChange • Hive=*HKLM* • *Subkey=Software\1E\Nomad Branch\NomadBranch* • Include Sub keys=1 TriggerTemplate-IntervalHours • intervalHours=1	1E-GuaranteedState-Nomad-PreCondition-MultiTests • hasCmClient=0 • **sccmDp=1** • smbEnabled=0
Check Nomad can hash content	Check	Checks Nomad content hashing is enabled.	1E-GuaranteedState-Nomad-Check-HashingEnabled • No parameters	TriggerTemplate-WindowsRegistryChange • Hive=*HKLM* • *Subkey=Software\1E\Nomad Branch\NomadBranch* • Include Sub keys=1 TriggerTemplate-IntervalHours • intervalHours=1	1E-GuaranteedState-Nomad-PreCondition-MultiTests • hasCmClient=0 • sccmDp=0 • smbEnabled=0
Check Nomad crash	Check	Checks whether Nomad has	1E-GuaranteedState-Nomad-	TriggerTemplate-WindowsRegistryChange • Hive=*HKLM*	1E-GuaranteedState-Nomad-

Name	Type	Description	Check and Fix fragments	Triggers	Precondition fragment
dumps status		generated any crash dump in the last seven days.	Check-CrashDumps • No parameters	• *Subkey=Software\1E\NomadBranch\NomadBranch* • Include Sub keys=1 TriggerTemplate-IntervalHours • intervalHours=1	PreCondition-MultiTests • hasCmClient=0 • sccmDp=0 • smbEnabled=0
Check Nomad does not have its content indexed by ConfigMgr software inventory checks	Check	Checks whether skpswi.dat exists in the Nomad cache directory.	1E-GuaranteedState-Nomad-Check-SkpSwiDat • No parameters	TriggerTemplate-FileChange • File Name=C:\ProgramData\1E\NomadBranch\skpswi.dat TriggerTemplate-IntervalHours • intervalHours=1 **Warning** Do NOT use this Check if you have changed your cache location.	1E-GuaranteedState-Nomad-PreCondition-MultiTests • hasCmClient=0 • sccmDp=0 • smbEnabled=0
Ensure Nomad does not have its content indexed by ConfigMgr software	Fix	Ensures that skpswi.dat exists in the Nomad cache directory.	1E-GuaranteedState-Nomad-Check-SkpSwiDat • No parameters	TriggerTemplate-FileChange • File Name=C:\ProgramData\1E\NomadBranch\skpswi.dat TriggerTemplate-IntervalHours • intervalHours=1 **Warning**	1E-GuaranteedState-Nomad-PreCondition-MultiTests • hasCmClient=0

Name	Type	Description	Check and Fix fragments	Triggers	Precondition fragment
inventory checks			1E-GuaranteedState-Nomad-Fix-SkpSwiDat • No parameters	Do NOT use this Fix if you have changed your cache location.	• sccmDp=0 • smbEnabled=0
Check Nomad has a virtual directory on ConfigMgr distribution points to perform LSZ generation	Check	Check that an LSZFILES virtual directory has been created on a ConfigMgr distribution point.	1E-GuaranteedState-Nomad-Check-DpLszVirtualDirectory • No parameters	TriggerTemplate-WindowsRegistryChange • Hive=*HKLM* • *Subkey=Software\1E\Nomad Branch\NomadBranch* • Include Sub keys=1 TriggerTemplate-IntervalHours • intervalHours=1	1E-GuaranteedState-Nomad-PreCondition-MultiTests • hasCmClient=0 • **sccmDp=1** • smbEnabled=0
Ensure Nomad has a virtual directory on ConfigMgr distribution points to perform LSZ	Fix	Ensure that an LSZFILES virtual directory has been created on a ConfigMgr distribution point.	1E-GuaranteedState-Nomad-Check-DpLszVirtualDirectory • No parameters 1E-GuaranteedState-Nomad-Fix-	TriggerTemplate-IntervalHours • intervalHours=1	1E-GuaranteedState-Nomad-PreCondition-MultiTests • hasCmClient=0 • **sccmDp=1**

Name	Type	Description	Check and Fix fragments	Triggers	Precondition fragment
generation			DpLszVirtualDirectory • No parameters		• smbEnabled=0
Check Nomad has sufficient disk space to download content	Check	Check the drive that Nomad is using for content download has sufficient disk space.	1E-GuaranteedState-Nomad-Check-DiskAvailablility • No parameters	TriggerTemplate-WindowsRegistryChange • Hive=*HKLM* • *Subkey=Software\1E\NomadBranch\NomadBranch* • Include Sub keys=1 TriggerTemplate-IntervalHours • intervalHours=1	1E-GuaranteedState-Nomad-PreCondition-MultiTests • hasCmClient=0 • sccmDp=0 • smbEnabled=0
Check Nomad is not using the Windows temp directory for caching	Check	Checks that Nomad is not configured to use the Windows temporary directory for caching.	1E-GuaranteedState-Nomad-Check-CacheInTemp • No parameters	TriggerTemplate-WindowsRegistryChange • Hive=*HKLM* • *Subkey=Software\1E\NomadBranch\NomadBranch* • Include Sub keys=1 TriggerTemplate-IntervalHours • intervalHours=1	1E-GuaranteedState-Nomad-PreCondition-MultiTests • hasCmClient=0 • sccmDp=0 • smbEnabled=0

Name	Type	Description	Check and Fix fragments	Triggers	Precondition fragment
Check Nomad is registered as an Alternate Content Provider with ConfigMgr	Check	Check that Nomad is correctly registered as an Alternate Content Provider with ConfigMgr.	1E-GuaranteedState-Nomad-Check-AlternateContentProvider • No parameters	TriggerTemplate-IntervalHours • intervalHours=1	1E-GuaranteedState-Nomad-PreCondition-MultiTests • **hasCmClient=1** • sccmDp=0 • smbEnabled=0
Ensure Nomad is registered as an Alternate Content Provider with ConfigMgr	Fix	Ensure Nomad is registered as an Alternate Content Provider with ConfigMgr, registering it if necessary.	1E-GuaranteedState-Nomad-Check-AlternateContentProvider • No parameters 1E-GuaranteedState-Nomad-Fix-AlternateContentProvider • No parameters	TriggerTemplate-IntervalHours • intervalHours=1	1E-GuaranteedState-Nomad-PreCondition-MultiTests • **hasCmClient=1** • sccmDp=0 • smbEnabled=0

Name	Type	Description	Check and Fix fragments	Triggers	Precondition fragment
Check Nomad run status	Check	Checks that the Nomad service is running.	1E-GuaranteedState-Nomad-Check-StartService • No parameters	TriggerTemplate-IntervalHours • intervalHours=1 TriggerTemplate-ServiceStatusChange • ServiceName=*NomadBranch*	1E-GuaranteedState-Nomad-PreCondition-MultiTests • hasCmClient=0 • sccmDp=0 • smbEnabled=0
Ensure Nomad is running	Fix	Ensure the Nomad service is running, starting the service if required.	1E-GuaranteedState-Nomad-Check-StartService • No parameters 1E-GuaranteedState-Nomad-Fix-StartService • No parameters	TriggerTemplate-IntervalHours • intervalHours=1 TriggerTemplate-ServiceStatusChange • ServiceName=*NomadBranch*	1E-GuaranteedState-Nomad-PreCondition-MultiTests • hasCmClient=0 • sccmDp=0 • smbEnabled=0
Check Nomad	Check	Checks whether the	1E-GuaranteedSt	TriggerTemplate-IntervalHours • intervalHours=1	1E-GuaranteedState-Nomad-

Name	Type	Description	Check and Fix fragments	Triggers	Precondition fragment
variant status		running Nomad service was one supplied with the 1E Client	ate-Nomad-Check-Variant • No parameters	TriggerTemplate-ServiceStatusChange • ServiceName=*NomadBranch*	PreCondition-MultiTests • hasCmClient=0 • sccmDp=0 • smbEnabled=0
Check Nomad's share directory is accessible	Check	Check whether Nomad needs a share, and if it does that it would be accessible to other devices.	1E-GuaranteedState-Nomad-Check-Share • No parameters	TriggerTemplate-WindowsRegistryChange • Hive=*HKLM* • *Subkey=Software\1E\Nomad Branch\NomadBranch* • Include Sub keys=1 TriggerTemplate-IntervalHours • intervalHours=1	1E-GuaranteedState-Nomad-PreCondition-MultiTests • hasCmClient=0 • sccmDp=0 • **smbEnabled=1**
Ensure Nomad's share directory is accessible	Fix	Ensures that Nomad's share is accessible if it is configured to	1E-GuaranteedState-Nomad-Check-Share • No parameters	TriggerTemplate-IntervalHours • intervalHours=1	1E-GuaranteedState-Nomad-PreCondition-MultiTests • hasCmCli

Name	Type	Description	Check and Fix fragments	Triggers	Precondition fragment
		require a share.	1E-GuaranteedState-Nomad-Fix-Share • No parameters		ent=0 • sccmDp=0 • **smbEnabled=1**
Check Nomad's share is accessible by specific accounts	Check	Checks that the correct accounts are able to access Nomad's share.	1E-GuaranteedState-Nomad-Check-ShareAccount • No parameters	TriggerTemplate-WindowsRegistryChange • Hive=*HKLM* • *Subkey=Software\1E\NomadBranch\NomadBranch* • Include Sub keys=1 TriggerTemplate-IntervalHours • intervalHours=1	1E-GuaranteedState-Nomad-PreCondition-MultiTests • hasCmClient=0 • sccmDp=0 • **smbEnabled=1**
Ensure Nomad's share is accessible by specific accounts	Fix	Ensures that the correct accounts are able to access Nomad's share	1E-GuaranteedState-Nomad-Check-ShareAccount • No parameters 1E-GuaranteedState-Nomad-	TriggerTemplate-IntervalHours • intervalHours=1	1E-GuaranteedState-Nomad-PreCondition-MultiTests • hasCmClient=0 • sccmDp=0

Name	Type	Description	Check and Fix fragments	Triggers	Precondition fragment
			Fix-ShareAccount • No parameters		• **smbEnabled=1**

1.11.12.10.1.4 Fragments

The following table shows the fragments included in the Nomad Client Health Integrated Product Pack:

> **Note**
>
> The **Parameters** column in the following table shows the ranges and default values for the parameters. The default values are used when you create custom rules using these fragments, unless you select alternative values.

Name	Type	Readable Payload and summary	Parameters
1E-GuaranteedState-Nomad-PreCondition-MultiTests	Precondition	**Check if standard conditions apply for Nomad plus optionally: is a ConfigMgr DP (<sccmDp>); has a ConfigMgr client (<hasCmClient>); SMB sharing is enabled (<smbEnabled>)** The precondition passes for all of the following standard tests: • The device is running a version of Windows - Nomad is only supported on Windows operating systems • The device is not running Windows XP - which is no longer supported by Nomad • The *NomadBranch* service is installed, although not necessarily running The precondition also tests for each of the following if it is enabled by changing its parameter from 0 to 1: • **hasCmClient** : The ConfigMgr client is installed • **sccmDp** : The device is a ConfigMgr Distribution Point (DP)	• hasCmClient • sccmDp • sm

Name	Type	Readable Payload and summary	Parameters
		• **smbEnabled** : SMB sharing of Nomad's cache is enabled. If **smbEnabled** test is set in the rule precondition then an additonal test is made to see if the device is a Domain Controller (DC). When installed on a DC Nomad must use its computer account instead of SMSNomadP2P& in order to share its cache. This requires registry value *HKLM\SOFTWARE\1E\NomadBranch\SpecialNetShare* to have its 0x80 bit set. If not set then Nomad does not share its cache on a DC and does not respond to elections. For early adopters, the readable payload of this precondition was: Carries out the specified checks; if any fail (i.e. they are logically AND-ed) then the preconditions fails.	bEnabled Range 0 or 1, defaults=0
1E-GuaranteedState-Nomad-Check-AEConnectivity	Check	**Check whether there is a working connection to ActiveEfficiency** Tests whether the URL given by registry value *HKLM\SOFTWARE\1E\NomadBranch\ActiveEfficiency\PlatformUrl*, if it is not empty, is contactable and returns a 200 code.	None
1E-GuaranteedState-Nomad-Check-AlternateContentProvider	Check	**Check whether Nomad is correctly registered within Microsoft ConfigMgr** Check that the ConfigMgr client's list of ACPs includes an object for Nomad in WMI class *ROOT\ccm\Policy\Machine\RequestedConfig\CCM_DownloadProvider*, with *CLSID* "*25A6160D-4543-495F-975E-32CFBD6F70E0*", *LogicalName* "*NomadBranch*", *V4CompatibleHash* is set, and just "*<Data></Data>*" in *GlobalSettings*.	None
1E-GuaranteedState-Nomad-Fix-AlternateContentProvider	Fix	**Ensures Nomad is correctly registered within Microsoft ConfigMgr** If the same checks as 1E-GuaranteedState-Nomad-Check-AlternateContentProvider are not satisfied, restarts the *NomadBranch* service, waits 10 seconds for Nomad to establish itself as an ACP, then carries out the checks again.	None

Name	Type	Readable Payload and summary	Parameters
1E-GuaranteedState-Nomad-Check-CacheInTemp	Check	**Check whether Nomad's cache is not in a temporary directory** The Nomad cache can sometimes be configured to be in the Windows *Temp* directory (usually *C:\Windows\Temp*) or one of its subdirectories. Since all the contents of the Windows *Temp* directory are considered to be transient and could be deleted at any time, this is not suitable for Nomad's cache which should be a permanent location. The check examines Nomad's *HKLM\SOFTWARE\1E\NomadBranch\LocalCachePath* registry value and verifies that the specified location actually exists. It then gets the *TEMP* environment variable, which, because both the *1E Client* and *NomadBranch* services run as *Local System*, is usually the WIndows *TEMP* directory. If the *LocalCachePath* value is the same as the *TEMP* environment variable, or *LocalCachePath* specifies a subdirectory within it, the check fails.	None
1E-GuaranteedState-Nomad-Check-CrashDumps	Check	**Check whether there have been any crashdump files created by Nomad in last 7 days** Nomad dump files are saved in the same directory as the log file, the parent directory of the *HKLM\SOFTWARE\1E\NomadBranch\LogFileNameLogFileName* registry value. The check looks in here for any files with a "*.dmp*" suffix (ignoring case), and if it finds any examines the modification time (not creation time!) of each, reporting as a failed check any that were modified in the last 7 days. So the check passes if there are no "*.dmp*" files or they are all older than 7 days.	None
1E-GuaranteedState-Nomad-Check-DiskAvailablility	Check	**Checks whether there is sufficient disk space for Nomad** This examines Nomad's *HKLM\SOFTWARE\1E\NomadBranch\PercentAvailableDisk* registry value. (It ignores the older *MaxCacheSizeMB* value which has been superseded by *PercentAvailableDisk*.) If the value is greater than or equal to 80, the check fails because the setting is too high. It then compares the size of the contents of the folder given by *HKLM\SOFTWARE\1E\NomadBranch\LocalCachePath* in the registry, i.e. Nomad's cache, with the free space of the drive on which the folder resides, as reported by WMI's *root\cimv\Win32_LogicalDisk*. The check fails if the percentage	None

Name	Type	Readable Payload and summary	Parameters
		of free space on the drive is less than or equal too *PercentAvailableDisk*.	
1E-GuaranteedState-Nomad-Check-DpLszEnabled	Check	**Check whether web LSZ generation is correctly configured on standalone distribution points** Nomad automatically sets up LSZ file generation on DPs that are ConfigMgr site servers, but extra configuration is required for standalone DPs. The device is a standalone DP if, under registry key *HKLM\SOFTWARE\Microsoft\SMS\Operations Management\SMS Server Role*, the subkey *SMS Distribution Point* exists but *SMS Site Server* does not. If the device is a standalone DP, registry value *HKLM\SOFTWARE\1E\\NomadBranch\SpecialNetShare* should have its 16384/0x4000 bit set to turn on web LSZ generation for HTTP/HTTPS enabled clients; if not, the check fails.	None
1E-GuaranteedState-Nomad-Check-DpLszVirtualDirectory	Check	**Check whether the LSZ directory is correctly configured on distribution points** At time of writing there is a bug such that the overall check status is usually "Passed" even when individually reported checks fail. If the device is a standalone DP, the check first verifes that registry value *HKLM\SOFTWARE\1E\\NomadBranch\SpecialNetShare* has its 16384/0x4000 bit set. (This bit is not required for a DP on a site server.) Then the *LSZFILES* web site is examined to verify that all these conditions are satisfied: • Anonymous authentication is enabled • Windows authentication is enabled • No SSL • Default document is enabled • Directory browsing is enabled, with Date, Time, Size, Extension and LongDate all available • Content indexing is disabled	None

Name	Type	Readable Payload and summary	Parameters
1E-GuaranteedState-Nomad-Fix-DpLszVirtualDirectory	Fix	**Ensure that the LSZ directory is correctly configured on distribution points** At time of writing there is a bug such that the overall check status is usually "Passed" even when individually reported checks fail. If any of the conditions described above for the corresponding check fragment is not true, the LSZFILES website is reconfigured to set that condition.	None
1E-GuaranteedState-Nomad-Check-FirewallExceptions	Check	**Checks whether firewall exceptions exist for Nomad** First is a check that at least one Windows firewall profile is enabled and that the firewall itself is enabled with either *HKLM\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile\EnableFirewall* set to 1 or *HKLM\SOFTWARE\Policies\Microsoft\WindowsFirewall\StandardProfile\EnableFirewall* set to 1 in the registry. If no firewall and no firewall profile is enabled then no firewall exceptions are necessary and so there is nothing more to do. Otherwise,the Nomad-related firewall rules are examined. These are the rules named: • *NomadBranch.exe* • *NomadPackageLocatorTcp* • *NomadPackageLocatorUdp* • *PackageStatusRequestTcp* • *PackageStatusRequestUdp* • *NomadBranchPeerHttp* • *NomadBranchPeerHttps* Using the *NomadBranch* service's path of *NomadBranch.exe*, the paths of *NomadPackageLocator.exe* and *PackageStatusRequest.exe* are deduced. Using the *HKLM\SOFTWARE\1E\NomadBranch\P2PEnabled* , *P2P_Port* , *P2PHttpPort* , and *P2PHttpsPort* settings in the registry, the	None

Name	Type	Readable Payload and summary	Parameters
		fragment works out which Nomad features are enabled and hence which firewall rules are required. The firewall rule checks involve: • Whether the rule even exists • That the rule is enabled and not blocked • The local port (which may be a specific one or all) • Which protocol (TCP or UDP) is involved • The path to the associated executable. Rulesfor *NomadBranch.exe* , *NomadPackageLocatorTcp* , *NomadPackageLocatorUdp* , *PackageStatusRequestTcp* and *PackageStatusRequestUdp* must always be correctly defined. *NomadBranchPeerHttp* is only required if the 0x20 bit of *P2P_Enabled* is set, and likewise the 0x40 bit requires *NomadBranchPeerHttps* .	
1E-GuaranteedState-Nomad-Fix-FirewallExceptions	Fix	**Ensures the required firewall exceptions exist for Nomad** This carries out all the checks as described above for 1E-GuaranteedState-Nomad-Check-FirewallExceptions then, for each absent or incorrectly configured rule that is required to support the *P2PEnabled* registry setting,configures that rule.	None
1E-GuaranteedState-Nomad-Check-HashingEnabled	Check	**Check whether hashing is enabled in Nomad** This examines the *HKLM\SOFTWARE\1E\NomadBranch\CompatibilityFlags* registry value. If the host is a ConfigMgr DP the 0x80000 bit should be set ("enable full hash generation for SIS content when an LsZ file is generated on a DP"), otherwise the 0x100000 bit ("abort download on the Nomad client if an LsZ hash mismatch is detected").	None
1E-GuaranteedState-Nomad-	Check	**Checks whether the Nomad share is available** This first checks the firewall settings. If the firewall is enabled then "*File and Printer Sharing*" (i.e. SMB) cannot be disabled. Next the 0x10 bit of registry value *HKLM\SOFTWARE\1E\\NomadBranch\SpecialNetShare* is	None

Name	Type	Readable Payload and summary	Parameters
Check-Share		examined to see if the share name is the default "*NomadSHR*" or the hidden "*NomadSHR$*". The share's security descriptor is read and check made that the local "*SMSNomadP2P&*" account has read permission. The share's properties are then verified as follows: • The shared directory is that named by registry value *HKLM\SOFTWARE\1E\NomadBranch\LocalCachePath* • The shared directory also matches the *Path* from WMI's *root\cimv2\Win32_Share* object for the share. • The *Status* of the *root\cimv2\Win32_Share* object is "*OK*". These additional checks are *not* carried out if the host is a server or a custom share is involved: • The maximum number of connections specified by the upper word of *SpecialNetShare* does not exceed the *MaximumAllowed* value of the WMI object. The *Data* value reported back by the check contains the results of the individual checks.	
1E-GuaranteedState-Nomad-Fix-Share	Fix	**Ensures the Nomad share is available** This carries out the checks as in 1E-GuaranteedState-Nomad-Check-Share above, then if any of them fails it restarts the *NomadBranch* service which should recreate the share correctly.	None
1E-GuaranteedState-Nomad-Check-ShareAccount	Check	**Checks whether the Nomad share account is correctly configured** If the machine account is used rather than the default "*SMSNomadP2P&*", as specified by bit 0x80 in registry value *HKLM\SOFTWARE\1E\\NomadBranch\SpecialNetShare* , no checks are carried out. A WMI *root\cimv2\Win32_UserAccount* object for the local *SMSNomadP2P&* account must exist and the account cannot be disabled.	None

Name	Type	Readable Payload and summary	Parameters
1E-GuaranteedState-Nomad-Fix-ShareAccount	Fix	**Ensures the Nomad share account is correctly configured** If the checks as described above for 1E-GuaranteedState-Nomad-Check-ShareAccount do not pass, the *NomadBranch* service is restarted to create a local *SMSNomadP2P&* account.	None
1E-GuaranteedState-Nomad-Check-SkpSwiDat	Check	**Check whether skpswi.dat exists on disk** A *skpswi.dat* file in a directory prevents ConfigMgr from falsely detecting that software is installed there during a Software Inventory scan, so Nomad requires one in its cache. Such a file must exist in the directory named by the *HKLM\SOFTWARE\1E\NomadBranch\LocalCachePath* registry value, and it must also be a hidden file.	None
1E-GuaranteedState-Nomad-Fix-SkpSwiDat	Fix	**Ensure skpswi.dat exists on disk** If the directory named by the *HKLM\SOFTWARE\1E\NomadBranch\LocalCachePath*registry value does not contain a "*skpswi.dat*" file, such a file is created and its hidden attribute set.	None
1E-GuaranteedState-Nomad-Check-StartService	Check	**Checks that Nomad is running** The *NomadBranch* service must be in "*Running*" or "*Starting*" state and be configured to start automatically.	None
1E-GuaranteedState-Nomad-Fix-	Fix	**Ensures that Nomad is running** If the *NomadBranch* service is not in "*Running*" or "*Starting*" state and configured to start automatically, it is started and configured to be so.	None

Name	Type	Readable Payload and summary	Parameters
StartService			
1E-GuaranteedState-Nomad-Check-Variant	Check	**Check whether the correct variant of Nomad (that supplied with the 1E Client, not standalone Nomad) is used for the service** This verifies that the parent directory of the executable that the Service Control Manager uses to run the *NomadBranch* service is the *Extensibility* directory of the 1E Client, and hence not, for example, an older standalone version of Nomad.	None

1.11.12.10.1.5 Trigger templates

The following table shows the trigger templates included in the Nomad Client Health Integrated Product Pack.

> **Note**
>
> The **Parameters** column in the following table shows the ranges and default values for the parameters. The default values are used when you create custom rules using these templates, unless you select alternative values.

Name	Readable Payload and summary	Parameters
TriggerTemplate-FileChange	**On change of file "<fileName>"** When a file changes (Windows only)	**File Name** • File path of file to be monitored, default is null.
TriggerTemplate-IntervalHours	**Every <intervalHours> hours** Periodic (hours)	**Interval Hours** • 0 to 999 hours (approximately 42

Name	Readable Payload and summary	Parameters
		days), default interval is 12 hours.
TriggerTemplate - IntervalMinutes	**Every <intervalMinutes> minutes** Periodic (minutes)	**Interval Minutes** • 0 to 99,999 minutes (approximately 69 days), default interval is 30 minutes.
TriggerTemplate -IntervalSeconds	**Every <intervalSeconds> seconds** Periodic (seconds)	**Interval Seconds** • 0 to 999,999 seconds (approximately 11 days), default interval is 3600 seconds (1 hour).

Name	Readable Payload and summary	Parameters
TriggerTemplate - ServiceStatusChange	**On change of running state of the "<serviceName>" service** When the state of the named Windows service changes **Note** You can determine the short name of a service using the PowerShell cmdlet `get-service -DisplayName "Network Location Awareness"` This will return **NlaSvc** in the above example. It is this short name you specify in the <ServiceName> parameter.	**Service Name** • Short name of service - for example Nomad Branch.
TriggerTemplate - WindowsRegistryChange	**On change of registry values in "<hive>\<subkey>" (include subkeys=<includeSubkeys>)** When the value of a Windows registry key changes.	**Hive**, which must be one of: • HKLM (default) • HKCR **Subkey** : free text string, default empty. **Include Sub Keys** : 1/0 default 0.

1.11.12.11 Windows Client Health integrated product pack

Integrated Product Pack used to create the **Windows Client Health** instruction set and **Windows Client Health** policy.

For more information, please refer to Windows Client Health Policy.

1.11.12.11.1 Windows Client Health integrated product pack

Integrated Product Pack used to create the **Windows Client Health** instruction set and **Windows Client Health** policy.

For more information, please refer to Windows Client Health Policy.

Over time Windows devices can develop performance problems related to device or service availability. This policy verifies the available storage capacity on devices, notifies of application crashes, monitors WMI health and service function, and also checks the behavior of core Windows services.

The Windows client health policy covers all of the following:

- Manages Windows devices and service availability performance problems
- Safeguards disk space integrity, ensuring sufficient storage capacity
- Ensures optimum performance of the Configuration Manager client and that WMI is active and integrated
- Notifies of application crashes and remediation assists. Investigates root cause for specific issues.

Note

This policy is intended for deployment to Windows devices only.

1.11.12.11.1.1 Instructions

The following table shows the instructions included in the Integrated Product Pack. Unless already uploaded, the following instructions are added to an Instruction set named:
Windows Client Health

Readable Payload	Type	Description	Name	Version
What applications have crashed?	Question	List application crashes. Returns an aggregated list of applications which have crashed and the number of times each of them crashed, including the application module which caused the crash, and application and module versions. The drill-down shows each device which suffered the crash, the file paths of the faulting application and module, the	**1E-Explorer-WindowsClientHealth-ApplicationCrashes**	3

Readable Payload	Type	Description	Name	Version
		exception code and offset, and the time of the crash.		
What crashes has <ApplicationName> suffered?	Question	List application crashes for a specific application.	**1E-Explorer-WindowsClientHealth-ApplicationCrashesFiltered**	3
What is the content of the Log located at <filepath>?	Question	Retrieve the content of a specified log file.	**1E-Explorer-WindowsClientHealth-GetLogFileContent**	3
Start the WMI service	Action	Start the Windows Management Instrumentation (WMI) service.	**1E-Explorer-WindowsClientHealth-StartWMIService**	3

1.11.12.11.1.2 Policies

The following table shows the policies included in the Integrated Product Pack.

Name	Description
Windows Client Health	The Windows Client Health policy ensures that the health of the Windows operating system is compliant with a reference baseline.

1.11.12.11.1.3 Rules

The following table shows the rules included in the Integrated Product Pack.

> **Note**
>
> Any parameter values shown in the **Check and Fix fragments**, **Triggers** and **Precondition fragment** columns are specifically set in the rules when the pack is uploaded. These may be different to the default values shown in the Windows Client Health Integrated Product Pack - Fragments table. You can modify these if required.

Name	Type	Description	Check and Fix fragments	Triggers	Precondition fragment
Check application	Check	Check that an application	1E-GuaranteedState-WindowsClientHealth-Check-ApplicationCrashes	TriggerTemplate-ProcessCrash	1E-GuaranteedState-General-

Name	Type	Description	Check and Fix fragments	Triggers	Precondition fragment
crash count (not assigned to any policy by default)		has not crashed excessively. **Note** By default, this check is not assigned to the	• ApplicationName=myApplication.exe • MaxCrashCount=1 • Days=7 **Note** ApplicationName is case insensitive but is required to be the filename of the executable for example unreliableapp.exe (without the path).	• Executable=myApplication.exe **Note** The Executable parameter must match the Application Name parameter in the associated Check fragment.	PreCondition-WindowsDevice • No parameters

Name	Type	Description	Check and Fix fragments	Triggers	Precondition fragment
		policy.			
Check free disk space	Check	Check that the system disk has at least 5 Gb of free space. (changed from 2 to 5 Gb in v5.0)	1E-GuaranteedState-WindowsClientHealth-Check-SystemDriveFreeSpace • ThresholdGb=5	TriggerTemplate-IntervalHours • Interval Hours=6	1E-GuaranteedState-General-PreCondition-WindowsDevice • No parameters
Check WMI repository health	Check	Check that the WMI repository is in a healthy state.	1E-GuaranteedState-WindowsClientHealth-Check-WmiBasicHealth • No parameters	TriggerTemplate-IntervalHours • Interval Hours=3	1E-GuaranteedState-General-PreCondition-WindowsDevice • No parameters
Ensure WMI service is running (not enabled and not assign	Fix	Ensure that the WMI service is running. **Note**	1E-GuaranteedState-General-Check-ServiceState • ServiceName=winmgmt • State=Running 1E-GuaranteedState-WindowsClientHealth-Fix-StartWMIService	TriggerTemplate-ServiceStatusChange • Service Name=winmgmt	1E-GuaranteedState-General-PreCondition-WindowsDevice • No par

Name	Type	Description	Check and Fix fragments	Triggers	Precondition fragment
ed to any policy by default)		By default, this fix is disabled, and not assigned to other p	• No parameters		ameters

Name	Type	Description	Check and Fix fragments	Triggers	Precondition fragment
		olicy.			

1.11.12.11.1.4 Fragments

The following table shows the fragments included in the Integrated Product Pack.

> **Note**
>
> The **Parameters** column in the following table shows the ranges and default values for the parameters. The default values are used when you create custom rules using these fragments, unless you select alternative values.

Name	Type	Readable Payload and summary	Parameters
1E-GuaranteedState-General-PreCondition-InstalledSoftware	Precondition	**Run if <SoftwareTitle> is installed** Uses the Software.GetInstallations to see if SoftwareTitle is installed. **Note** The Software Title parameter can be a partial string such as **SQL Server** which will match on the first SQL Server title that is found installed on the device. **Note** Not used by any policy rules by default.	**SoftwareTitle** • default empty
1E-GuaranteedState-General-PreCondition-MinWindowsVersion	Precondition	**Run if device is Windows <MinimumVersion>** Uses Agent.GetSummary method to get MinimumVersion, and passes if it matches the given parameter. • XP or greater (5.2) - also matches Server 2003 • Vista or greater (6.0) - also matches Server 2008 • 7 or greater (6.1) - also matches Server 2008 R2	**MinimumVersion** • XP or gr

Name	Type	Readable Payload and summary	Parameters
		• 8 or greater (6.2) - also matches Server 2012 • 8.1 or greater (6.3) - also matches Server 2012 R2 • 10 or greater (10.0) - also matches Server 2016 **Note** Not used by any policy rules by default.	• eater • Vistaorgreater • 7orgreater • 8orgreater

Name	Type	Readable Payload and summary	Parameters
			• 8.1 or greater • 10 or greater (default)
1E-GuaranteedState-General-PreCondition-OperatingSystem	Precondition	**Run if operating system is <OsText>** Uses the Agent.GetSummary method to get OsText, and passes if it matches the given parameter. **Note** Not used by any policy rules by default.	**OsText** • Andro

Name	Type	Readable Payload and summary	Parameters
			id • CentOS • Fedora • macOS • RedHat • SUSE • Ubuntu

Name	Type	Readable Payload and summary	Parameters
			• Windows 10 • Windows 7 • Windows 8.1 • WindowsServe

Name	Type	Readable Payload and summary	Parameters
			r2012 • WindowsServer2016 • WindowsVista • Window

Name	Type	Readable Payload and summary	Parameters
			sXP (default empty)
1E-GuaranteedState-General-PreCondition-OSAndSoftware	Precondition	**Run if operating system is <OsText> and <SoftwareTitle> is installed** Uses the Agent.GetSummary method to get OsText. Uses the Software.GetInstallations to see if SoftwareTitle is installed.	**OsText** • seeabove **SoftwareTitle** • default empty
1E-GuaranteedState-General-PreCondition-WindowsDevice	Precondition	**Determine if device is running Windows** Is Operating System type = Windows. Uses the Device.GetSummary method.	No parameters

Name	Type	Readable Payload and summary	Parameters
1E-GuaranteedState-General-Check-ServiceState	Check	**Check that service "<ServiceName>" is <State>** Uses the OperatingSystem.GetServiceInfo method to check the specified service is in the specified state. You specify the service by its short name. **Note** Service names are listed under registry HKLM\CurrentControlSet\Services. You can determine the short name of a service using the PowerShell cmdlet: *`get-service -DisplayName "Network Location Awareness"`* The above example will return **NlaSvc**, whch is the short name you specify in the **<ServiceName>** parameter. Another example is WindDefend, which is the short name of the Microsoft Defender Antivirus Service.	**ServiceName** • default empty **State** • Running • Stopped
1E-GuaranteedState-WindowsClientHealth-Check-ApplicationCrashes	Check	**Check that application <ApplicationName> has not suffered more than <MaxCrashCount> crashes for the last <Days> days** **<Days>** is Days back from now. **<ApplicationName>** is case insensitive but is required to be the filename of the executable, for example unreliableapp.exe (without the path).	**ApplicationName** • defau

Name	Type	Readable Payload and summary	Parameters
		This fragment queries the root\cimv2 WMI space with the query "SELECT * FROM Win32_NTLogEvent WHERE (logfile='Application') AND (type='Error') AND (EventCode=1000) AND (Message LIKE '%name: %ApplicationName%,%')" in order to retrieve the event log entries relating to application crashes for a specific application. If the count of events exceeds the parameter **<MaxCrashCount>** then compliance failure is returned.	lt e m p t y **MaxCrashCount** • d e f a u lt 1 **Days** • d e f a u lt 7
1E-GuaranteedState-WindowsClientHealth-Check-SystemDriveFreeSpace	Check	**Check that system drive has at least <ThresholdGb> Gb of free space** **<ThresholdGb>** is free space in gigabytes. This fragment runs the WMI query "Select DeviceId, FreeSpace from Win32_LogicalDisk" and filters the results to include just the system drive. It then determines whether the reported free space exceeds the **<ThresholdGb>** parameter and returns compliance failure if it does not.	**ThresholdGb** • 0 t o 9 9 9 , n o d e f

Name	Type	Readable Payload and summary	Parameters
			a u lt
1E-GuaranteedState-WindowsClientHealth-Check-WmiBasicHealth	Check	**Check that Windows WMI repository is consistent and can process basic query** This fragment first verifies repository integrity by issuing the command winmgmt /verifyrepository. If this reports that the repository is ok, the WMI query "Select Name from Win32_computerSystem" is issued against the root\cimv2 namespace. If this also succeeds, the fragment returns success, otherwise it returns failure, with the Data column containing one of the following depending on whether the consistent check or the subsequent query failed: • WMI repository is not consistent • WMI repository is consistent but failed to process basic query	No parameters
1E-GuaranteedState-WindowsClientHealth-Fix-StartWMIService	Fix	**Start the WMI service** This fragment uses the OperatingSystem.ControlService method to set the action of the **Winmgmt** (WMI) service to **Start**. It then enumerates running services and if the service is now running, it returns compliance success otherwise failure. The data column in the response always contains the value **winmgmt**.	No parameters

1.11.12.11.1.5 Trigger templates

The following table shows the trigger templates included in the Windows Client Health Integrated Product Pack.

> **Note**
>
> The **Parameters** column in the following table shows the ranges and default values for the parameters. The default values are used when you create custom rules using these templates, unless you select alternative values.

Name	Readable Payload and summary	Parameters
TriggerTemplate-IntervalHours	**Every <intervalHours> hours** Periodic (hours)	**Interval Hours** • 0 to 999 hours (approximately 42 days), default interval is 12 hours.
TriggerTemplate-IntervalMinutes	**Every <intervalMinutes> minutes** Periodic (minutes)	**Interval Minutes** • 0 to 99,999 minutes (approximately 69 days), default interval is 30 minutes.
TriggerTemplate-IntervalSeconds	**Every <intervalSeconds> seconds** Periodic (seconds)	**Interval Seconds** • 0 to 999,999 seconds (approximately 11

Name	Readable Payload and summary	Parameters
		days), default interval is 3600 seconds (1 hour).
TriggerTemplate-ProcessCrash	**On crash of process "<executable>"** When a process crashes (Windows only) Monitors the Windows Application Event Log for event 1000. **Note** Executable is case insensitive but is required to be the whole filename without the folder path, such as unreliableapp.exe A partial string such as unreliableapp will not trigger on a crash of unreliableapp.exe.	**Executable** • Filename of executable to be monitored, default is empty.
TriggerTemplate-ServiceStatusChange	**On change of running state of the "<serviceName>" service** When the state of the named Windows service changes **Note** You can determine the short name of a service using the PowerShell cmdlet `get-service -DisplayName "Network Location Awareness"` This will return **NlaSvc** in the above example. It is this short name you specify in the <ServiceName> parameter.	**Service Name** • Short name of service - for example Nomad Branch.
TriggerTemplate-WindowsEventLog	**On Windows"<channel>"; event log entry matching "<query>" (debounce for <debounce> seconds)** When an event log entry is created (Windows only) **Note** A **channel** is an event sink, example standard channel names are Application or Security.	**Channel** • Text string, default null. **Query**

Name	Readable Payload and summary	Parameters

	To determine the available event channels execute the following PowerShell command:
	`Get-WinEvent -ListLog *`
	Or to view the event channels on a remote computer:
	`Get-WinEvent -ListLog * -ComputerName <hostname>`
	Similarly to view event log entries for a given channel either use Event Viewer or from PowerShell for example:
	`Get-EventLog application | where {($_.EntryType -Match "Error")`
	`-or ($_.EntryType -Match "Warning")}`
	Or:
	`[dateTime]$oneWeekAgo = (get-date).addDays(-7) Get-EventLog -LogName Application`
	`-After $oneWeekAgo -computerName . \| ? {$_.EventID -eq 1000}`
	Note
	A **query** is used to filter the event log messages for a given channel. Examples can be found at https://docs.microsoft.com/en-us/windows/win32/wes/consuming-events.
	For example to query all OneNote application crashes error log messages:
	*[System[(Level=2) and (EventID=1000)]] and *[EventData[Data='onenote.exe']]
	Debounce is a settling period to ensure that in the case of multiple events, only a single event is registered within the space of a given time period.
		• Text string, default null.
		Debounce Time Seconds
		• 0 to 99 seconds, default 0.

TriggerTemplate-WindowsRegistryChange (added in 5.0)	**On change of registry values in "<hive>\<subkey>" (includesubkeys=<includeSubkeys>)** When the value of a Windows registry key changes.	**Hive**, which must be one of: • HKLM (default)

Name	Readable Payload and summary	Parameters
		• HKCR **Subkey** : free text string, default empty. **Include Sub Keys** : 1/0 default 0.

1.11.12.12 Tachyon Core integrated product pack

Reference for the policy objects contained in the Integrated Product Pack: Tachyon Core.

> **Note**
>
> This Integrated Product Pack does not include any Instructions, Policies or Rules. It contains only fragments (preconditions, checks and fixes) and trigger templates. These can be used to create your own custom rules and policies.

1.11.12.12.1 Instructions

No Instructions.

1.11.12.12.2 Policies

No Policies.

1.11.12.12.3 Rules

No Rules.

1.11.12.12.4 Fragments

The following fragments are not currently used in ready-made policies provided by 1E, but you can use them to create custom policies.

> **Note**
>
> The **Parameters** column in the following table shows the ranges and default values for the parameters. The default values are used when you create custom rules using these fragments, unless you select alternative values.

Name	Type	Readable Payload and summary	Parameters
1E-GuaranteedState-General-Check-RegistryValue	Check	**Check that registry key <Hive>\>Subkey>\<Name> has < ValueType> value of "<Value>"** Uses NativeServices.RegistryGetValue method to see if the specified registry entry exists, and compares its value with the specified value. This fragment is intended for Windows only devices.	**Hive** • HKLM (default) • HKCR **Subkey** - default empty **Name** - default empty **Value** - default empty **ValueType** • REG_SZ • REG_DWORD • REG_QWORD • REG_EXPAND_SZ
1E-GuaranteedState-General-Fix-RegistryValue	Fix	**Set registry key <Hive>\<Subkey>\<Name> to <ValueType> value of "<Value>"** Uses NativeServices.RegistrySetValue method to set the specified registry value. This fragment is intended for Windows only devices.	**Hive** • HKLM (default) • HKCR **Subkey** - default empty **Name** - default empty

Name	Type	Readable Payload and summary	Parameters
			Value - default empty **ValueType** • REG_SZ • REG_DWORD • REG_QWORD • REG_EXPAND_SZ
1E-GuaranteedState-General-Check-ServiceState	Check	**Check that service "<ServiceName>" is <State>** Uses Device.GetSummary method to see if the device is running Windows, and OperatingSystem.GetServiceInfo method to see if the specified service is installed, and compares its state with the specified state. ServiceName is the short name of the service. **Note** You can determine the short name of a service using the PowerShell cmdlet `get-service -DisplayName "Network Location Awareness"` This will return **NlaSvc** in the above example. It is this short name you specify in the **<ServiceName>** parameter.	**ServiceName** - default empty **State** • Running • Stopped
1E-GuaranteedState-General-Fix-ServiceState	Fix	**Request service "<serviceName>" to <action>** ServiceName is the short name of the service. Uses OperatingSystem.ControlService method to attempt to set the state of the specified service. The fragment does not change any dependencies (StopDependencies=false). Does not change the startup type.	**ServiceName** - default empty **Action** • Start • Stop

Name	Type	Readable Payload and summary	Parameters
		This fragment is intended for Windows only devices.	• Pause • Resume • Restart

Preconditions included in this pack are documented in the Trigger templates and preconditions reference page.

1.11.12.13 Trigger templates and preconditions reference

Reference for all the precondition fragments and trigger templates available in Integrated Product Packs included in the **Tachyon Platform** zip. These can be used to create your own custom rules and policies.

1.11.12.13.1 Trigger templates

Name	Readable Payload and summary	Parameters	Included in
TriggerTemplate-FileChange	**On change of file "<fileName>"** When a file changes (Windows only)	**File Name** • File path of file to be monitored, default is null.	• Nomad Client Health integrated product pack
TriggerTemplate-IntervalHours	**Every <intervalHours> hours** Periodic (hours)	**Interval Hours** • 0 to 999 hours	• Microsoft SCCM

Name	Readable Payload and summary	Parameters	Included in
		(approximately 42 days), default interval is 12 hours.	Client Health Integrated Product Pack • Nomad Client Health integrated product pack • Tachyon Core integrated pr

Name	Readable Payload and summary	Parameters	Included in
			oduct pack • Windows Endpoint Performance Integrated Product Pack • Windows Client Health integrated product

Name	Readable Payload and summary	Parameters	Included in
			pack
TriggerTemplate-IntervalMinutes	**Every <intervalMinutes> minutes** Periodic (minutes)	**Interval Minutes** • 0 to 99,999 minutes (approximately 69 days), default interval is 30 minutes.	• Microsoft SCCM Client Health Integrated Product Pack • Nomad Client Health integrated product pack

Name	Readable Payload and summary	Parameters	Included in
			• Tachyon Core integrated product pack • Windows Endpoint Performance Integrated Product Pack • Windows Client

Name	Readable Payload and summary	Parameters	Included in
			Health integrated product pack
TriggerTemplate-IntervalSeconds	**Every <intervalSeconds> seconds** Periodic (seconds)	**Interval Seconds** • 0 to 999,999 seconds (approximately 11 days), default interval is 3600 seconds (1 hour).	• Microsoft SCCM Client Health Integrated Product Pack • Nomad Client Health int

Name	Readable Payload and summary	Parameters	Included in
			egrated product pack • Tachyon Core integrated product pack • Windows Endpoint Performance Integrated Product

Name	Readable Payload and summary	Parameters	Included in
			Pack • Windows Client Health integrated product pack
TriggerTemplate-ProcessCrash	**On crash of process "<executable>"** When a process crashes (Windows only) Monitors the Windows Application Event Log for event 1000. **Note** Executable is case insensitive but is required to be the whole filename without the folder path, such as unreliableapp.exe A partial string such as unreliableapp will not trigger on a crash of unreliableapp.exe.	**Executable** • Filename of executable to be monitored, default is empty.	• Tachyon Core integrated product pack • Windows Client

Name	Readable Payload and summary	Parameters	Included in
			Health integrated product pack
TriggerTemplate-ProcessLaunch	**On launch of process "<executable>"** When a process starts (Windows only) Monitors the Windows Security Event Log for event 4688.	**Executable** • File path of executable to be monitored, default is empty.	• Tachyon Core integrated product pack • Windows Endpoint Performance Integrated

Name	Readable Payload and summary	Parameters	Included in
			Product Pack
TriggerTemplate-ServiceStatusChange	**On change of running state of the "<serviceName>" service** When the state of the named Windows service changes **Note** You can determine the short name of a service using the PowerShell cmdlet `get-service -DisplayName "Network Location Awareness"` This will return **NlaSvc** in the above example. It is this short name you specify in the <ServiceName> parameter.	**Service Name** • Short name of service - for example NomadBranch.	• Microsoft SCCM Client Health Integrated Product Pack • Nomad Client Health integrated product

Name	Readable Payload and summary	Parameters	Included in
			pack • Tachyon Core integrated product pack • Windows Client Health integrated product pack
TriggerTemplate-WindowsEventLog	**On Windows"<channel>"; event log entry matching "<query>" (debounce for <debounce> seconds)** When an event log entry is created (Windows only) **Note**	**Channel** • Text string, defau	• Tachyon Core int

Name	Readable Payload and summary	Parameters	Included in

	A **channel** is an event sink, example standard channel names are Application or Security.
	To determine the available event channels execute the following PowerShell command:
	`Get-WinEvent -ListLog *`
	Or to view the event channels on a remote computer:
	`Get-WinEvent -ListLog * -ComputerName <host name>`
	Similarly to view event log entries for a given channel either use Event Viewer or from PowerShell for example:
	`Get-EventLog application | where {($_.EntryType -Match "Error") -or ($_.EntryType -Match "Warning")}`
	Or:
	`[dateTime]$oneWeekAgo = (get-date).addDays(-7) Get-EventLog -LogName Application -After $oneWeekAgo -computerName . \| ? {$_.EventID -eq 1000}`
	Note
	A **query** is used to filter the event log messages for a given channel. Examples can be found at https://docs.microsoft.com/en-us/windows/win32/wes/consuming-events.
	For example to query all OneNote application crashes error log messages:
	*[System[(Level=2) and (EventID=1000)]] and *[EventData[Data='onenote.exe']]
	Debounce is a settling period to ensure that in the case of multiple events, only a single event is registered within the space of a given time period.
		lt null.
		Query
		• Text string, default null.
		Debounce Time Seconds
		• 0 to 99 seconds, default 0.
			egrated product pack
			• Windows Client Health integrated product pack

Name	Readable Payload and summary	Parameters	Included in
TriggerTemplate-WindowsRegistryChange	**On change of registry values in "<hive>\<subkey>" (include subkeys=<includeSubkeys>)** When the value of a Windows registry key changes.	**Hive**, which must be one of: • HKLM (default) • HKCR **Subkey** : free text string, default empty. **Include Sub Keys** : 1/0 default 0.	• Nomad Client Health integrated product pack • Tachyon Core integrated product pack

1.11.12.13.2 Precondition fragments

Name	Readable Payload and Description	Parameters	Included in
1E-GuaranteedState-ClientHealth-	**Run if the ConfigMgr client is installed** Uses the Device.GetSummary method to determine if the device is running Windows.	No parameters.	• MEMCM Client

Name	Readable Payload and Description	Parameters	Included in
PreCondition-ConfigMgrClient	Uses the OperatingSystem.GetServiceInfo method to determine if the ConfigMgr client service (ccmexec) is installed, although not necessarily running.		Health Integrated Product Pack
1E-GuaranteedState-General-PreCondition-InstalledSoftware	**Run if <SoftwareTitle> is installed** Uses the Software.GetInstallations to see if SoftwareTitle is installed. **Note** The Software Title parameter can be a partial string such as **SQL Server** which will match on the first SQL Server title that is found installed on the device.	**Software Title** • A product name as it appears in Programs and Features (Add Remove programs - ARP).	• Tachyon Core integrated product pack • Windows Client Health integrated product pack

Name	Readable Payload and Description	Parameters	Included in
1E-GuaranteedState-General-PreCondition-MinWindowsVersion	**Run if device is Windows <MinimumVersion>** Uses Agent.GetSummary method to get MinimumVersion, and passes if it matches the given parameter. • XP or greater (5.2) - also matches Server 2003 • Vista or greater (6.0) - also matches Server 2008 • 7 or greater (6.1) - also matches Server 2008 R2 • 8 or greater (6.2) - also matches Server 2012 • 8.1 or greater (6.3) - also matches Server 2012 R2 • 10 or greater (10.0) - also matches Server 2016	**Minimum Version** • XP or greater • Vista or greater • 7 or greater • 8 or greater • 8.1 or greater • 10 or greater (default)	• Tachyon Core integrated product pack • Windows Client Health integrated product pack
1E-GuaranteedState-General-PreCondition-MinWindowsVersionAndVariant	**Run if device is running <Variant> variant of Windows <MinimumVersion>** Uses the Agent.GetSummary method to get Variant and MinimumVersion, and passes if they match the given parameters. If the text Server is in OsVersionText then it's a Server, otherwise it's a Desktop. • XP/Server 2003 or greater (5.2)	**Minimum Version** • XP/Server 2003 or greater	• Tachyon Core integrated product

Name	Readable Payload and Description	Parameters	Included in
	• Vista/Server 2008 or greater (6.0) • 7/Server 2008 R2 or greater (6.1) • 8/Server 2012 or greater (6.2) • 8.1/Server 2012 R2 or greater (6.3) • 10/Server 2016 or greater (10.0)	• Vista/Server 2008 or greater • 7/Server 2008 R2 or greater • 8/Server 2012 or greater • 8.1/Server 2012 R2 or greater • 10/Server 2016 or greater (default) **Variant** Windows OS variant:	pack

Name	Readable Payload and Description	Parameters	Included in
		• Desktop (default) • Server	
1E-GuaranteedState-General-PreCondition-OperatingSystem	**Run if operating system is <OsText>** Uses the Agent.GetSummary method to get OsText, and passes if it matches the given parameter.	**OsText** • Android • CentOS • Fedora • macOS • Red Hat • SUSE • Ubuntu • Windows • Windows 10 • Windows 7 • Windows 8.1 • Windows	• Tachyon Core integrated product pack • Windows Client Health integrated product pack

Name	Readable Payload and Description	Parameters	Included in
		Server 2012 • Windows Server 2016 • Windows Vista • Windows XP	
1E-GuaranteedState-General-PreCondition-OSAndSoftware	**Run if operating system is <OsText> and <SoftwareTitle> is installed** Uses the Agent.GetSummary method to get OsText. Uses the Software.GetInstallations to see if SoftwareTitle is installed.	**OsText** • See: 1E-Guaranteed State-General-PreCondition-OperatingSystem **SoftwareTitle** • See: 1E-Guaranteed State-General-PreCondition	• Tachyon Core integrated product pack • Windows Client Health integrated pro

Name	Readable Payload and Description	Parameters	Included in
		n-InstalledSoftware	duct pack
1E-GuaranteedState-General-PreCondition-OsTypeAndArchitecture	**Check whether a device has an OS of <OsType > and an architecture of <Architecture>** Passes if the OsType agent enumeration and the Architecture match the given parameters. Uses the Device.GetSummary method.	**OsType** • – –	• Tachyon Core integrated product pack • Windows Endpoint Performance Integrated Product Pack
		–	
		–	

Name	Readable Payload and Description	Parameters	Included in
		–	
		Architecture •	
		–	
		–	
1E-GuaranteedState-General-PreCondition-Service	**Run if <ServiceName> service is installed** Uses the OperatingSystem.GetServiceInfo method to check the specified service is in the specified state. You specify the service by its short name. **Note** Service names are listed under registry HKLM\CurrentControlSet\Services.	**ServiceName** • Short name of the Windows Service, default	• Tachyon Core integrated product

Name	Readable Payload and Description	Parameters	Included in
	You can determine the short name of a service using the PowerShell cmdlet: *get-service -DisplayName "Network Location Awareness"* The above example will return **NlaSvc**, whch is the short name you specify in the **<ServiceName>** parameter. Another example is WindDefend, which is the short name of the Microsoft Defender Antivirus Service.	empty.	pack
1E-GuaranteedState-General-PreCondition-WindowsDevice	**Determine if device is running Windows** Is Operating System type = Windows. Uses the Device.GetSummary method.	No parameters.	• Tachyon Core integrated product pack • Windows Client Health integrated product

Name	Readable Payload and Description	Parameters	Included in
			pack
1E-GuaranteedState-Nomad-PreCondition-MultiTests	**Nomad client passes 3 standard tests plus any /all of the following tests if enabled** The precondition passes for all of the following standard tests: • The device is running a version of Windows - Nomad is only supported on Windows operating systems • The device is not running Windows XP - which is no longer supported by Nomad • The *NomadBranch* service is installed, although not necessarily running The precondition also tests for each of the following if it is enabled by changing its parameter from 0 to 1: • **hasCmClient** : The ConfigMgr client is installed • **sccmDp** : The device is a ConfigMgr Distribution Point (DP) • **smbEnabled** : SMB sharing of Nomad's cache is enabled. If **smbEnabled** test is set in the rule precondition then an additonal test is made to see if the device is a Domain Controller (DC). When installed on a DC Nomad must use its computer account instead of SMSNomadP2P& in order to share its cache. This requires registry value *HKLM\SOFTWARE\1E\NomadBranch\SpecialNetShare* to have its 0x80 bit set. If not set then Nomad does not share its cache on a DC and does not respond to elections.	• **hasCmClient** : 1/0 • **sccmDp** : 1/0 • **smbEnabled** : 1/0 Defaults are 0.	• Nomad Client Health integrated product pack

1.11.13 Tachyon release information

1.11.13.1 Tachyon release information

These notes contain information about Tachyon that you need to have to successfully install and use the product. You should read these release notes and the online documentation for Tachyon thoroughly before using the software.

1.11.13.1.1 New features in Tachyon 8.1

1.11.13.1.1.1 Tachyon 8.1 platform

- New supported platform components:
-
  - Switch now using C++17
  - Platform now using .NET Framework 4.8
- New Tachyon connector: OpenLM connector - in this version, the Inventory (SLA) is the only app capable of viewing this data

1.11.13.1.1.2 Consumer applications for v8.1

- **AppClarity 8.1:**
  - Works with Tachyon Platform 8.1
  - No features or feature changes added in this release, but includes any hotfixes from previous versions.
- **Application Migration 8.1:**
  - Works with Tachyon Platform 8.1
  - No features or feature changes added in this release, but includes any hotfixes from previous versions.
- **Guaranteed State 8.1:**
  - Works with Tachyon Platform 8.1
  - No features or feature changes added in this release, but includes any hotfixes from previous versions..
- **Nomad 8.1:**
  - Works with Tachyon Platform 8.1
  - **Insights on how Nomad enhances user experience** - with the rapid shift to a Work From Anywhere (WFA) workforce and an increased focus on the Digital End-User eXperience, Nomad on Tachyon Platform now provides insights into how it helps to ensure a great user eXperience. With the introduction of Nomad's Bandwidth Protection Reporting, you can now see how Nomad is preventing end-user disruption due to software and update deployments. Bandwidth Protection Reporting will allow you to see the positive impact Nomad is having across the organization, to individual sites, subnets, all the way down to a single client.

- Support for Cloud-based content in Task Sequences - cloud-based services to support Work From Anywhere (WFA) users are becoming more critical to the way enterprises work, there is an increased reliance on Cloud Distribution Points for distributing content.
- **Feature improvements** - as Configuration Manager evolves and new features are released, Nomad on Tachyon Platform is being continuously maintained to ensure it works seamlessly with new releases.
    - Content Distribution service no longer uses SQL Linked Server to connect to Microsoft Endpoint Configuration Manager.

- **Patch Success 8.1:**
    - Works with Tachyon Platform 8.1
    - No features or feature changes added in this release, but includes any hotfixes from previous versions.
- **Tachyon Explorer 8.1:**
    - Works with Tachyon Platform 8.1
    - No features or feature changes added in this release, but includes any hotfixes from previous versions.
- **Tachyon Experience 8.1:**
    - Works with Tachyon Platform 8.1
    - No longer requires SQL Server Analysis Server (SSAS)
    - On the Software page, the **Product**, **Executable**, **Version** and **Architecture** columns have been removed from the table that is displayed after clicking on a particular row. This is because the subsequent table is filtered on the selected Product, Executable, Version and Architecture values and will be the same for every row in the table. The values are displayed anyway in the heading for the page, and the columnscan be added back from the Column picker if needed
    - User Sentiment descriptions now highlight that User Sentiment is processed once a day, rather than real-time.

1.11.13.1.1.3Product Packs for v8.1

- **Classic Product Packs:**
    - 1E-ConfigMgrConsoleExtensions.zip
    - 1E-Experience.zip
    - 1E-Explorer-TachyonAgent.zip (new instruction: 1E-Explorer-Upgrade1EClient8.0macOS, updated instruction: Set1EClientAgentConfig)
    - 1E-Explorer-TachyonCore.zip
    - 1E-Inventory.zip

- 1E-Nomad.zip (new instructions: 1E-Nomad-CacheCleanerDeleteAll, 1E-Nomad-LocationDiscovery, 1E-Nomad-SetWorkRate)
- 1E-Patch-Success.zip
- 1E-Tachyon-Platform.zip (new instruction: 1E-TachyonPlatform-Device-ComparisonData)

- **Integrated Product Packs:**
  - MEMCM Client Health Integrated Product Pack (new preconditions: MEMCM-Client, Network-IPv4-PrimaryAddressInDNS, and some rules modified to use them)
  - NomadClientHealth.zip (minor changes)
  - TachyonCore.zip (minor changes)
  - WindowsClientHealth.zip (minor changes).
- Other Product Packs are available from the Tachyon Exchange: tachyonexchange.1e.com

1.11.13.1.1.4Enhancements in v8.1

- Platform:
  - Updated PowerShell scripts used to create direct-based management groups - see Management Groups page
  - Internal changes to support Tachyon SaaS
  - SCCM inventory connector now supports the Tachyon SaaS DataSync service
  - Support for future consumer applications
- **Tachyon Setup**
  - Support for future consumer applications
- **Tachyon Product Pack deployment tool**
  - No changes.

1.11.13.1.2 Troubleshooting

1.11.13.1.2.1Online help

Tachyon comes with online help that shows you how to install, configure and use the product. Click the following link to view the help:

- Introducing Tachyon

For support queries, please:

- Use https://support.1e.com/ where you can search the KB or submit a support case.
- Contact support@1e.com.

1.11.13.1.2.2Known issues

The current known issues related to the installation and running of Tachyon can be found on the Known issues page.

1.11.13.1.3 Tachyon release history

1.11.13.1.3.1Web Release-8.1 (14-Mar-2022)

1.11.13.1.3.1.1 Tachyon Server 8.1.2.102 - Tachyon Toolkit 8.1.2.102 - 1E Catalog 8.1.2.7 - Software Lifecycle Automation 8.1.2.22 - Business Intelligence 8.1.2.3 - ContentDistribution 8.1.2.59 - AppClarity 8.1.2.3 - ApplicationMigration 8.1.2.21

For new features please refer to the top of the page.

1.11.13.1.3.1.2 Enhancements for v8.1

1.11.13.1.3.1.2.1 Hotfixes rolled up into this release - Server (including Experience, Explorer, and Guaranteed State):

- Q22008 - Policy status is incorrectly updated when rule status events arrive out of order (TFS 244465)
- Q22006 - Experience - Device hyperlink goes missing when view is changed from one saved pre-set to another (TFS 245628)
- Q22004 - Experience - Device pillar view on low resolution screen (TFS 245878)
- Q22002 - Experience - Selecting instances of events does not filter by time (TFS 246428)
- Q22000 - User with permission 'Guaranteed State Policy Assigner' and 'Guaranteed State User' cannot assign policy (TFS 244646)
- Q21998 - Option to delete direct-based Management Groups (TFS 245958)
- Q21996 - Group membership resolution fails for some applications when nested group search is disabled. (TFS 245991)
- Q21902 - Sanitize Server Side Instruction parameters to prevent SQL injection (TFS 246156)
- Q21900 - Explorer - Coverage is being ignored during follow up question/action when additional result filters are applied (TFS 245874)
- Q21898 - Server Side Instructions - The "EvaluatingCondition" workflow state causes responses not to be retrievable (TFS 245352)
- Q21896 - Guaranteed State - Remediation page fails to load any data in large estate (TFS 245349)

1.11.13.1.3.1.2.2 Hotfixes rolled up into this release - SLA:

- Q22110 - Excessive tempdb data usage for ReportTag consolidation step (TFS 249162)
- Q22108 - Incorrect number of devices in Tachyon management group (TFS 246018)
- Q22106 - String or binary data truncated within Management Group data (TFS 247120)
- Q22104 - Machines are showing up in the wrong Management Group (TFS 247888)

- Q22102 - Hash conflict issue in Tachyon connector. (TFS 248544)
- Q22100 - Primary user details are not showing when another connector inventory date is ahead of Tachyon. (TFS 246199)
- Q22098 - Wrong Devices Returned From Management Group Member Retrieval api when Device and Patch consolidation report is in process (TFS 235368)

1.11.13.1.3.1.2.3 Hotfixes rolled up into this release - Catalog:

- Q21948 - Catalog - UpdateService - Base Url extraction algorithm is flawed (TFS 247265)

1.11.13.1.3.1.2.4 Hotfixes rolled up into this release - AppClarity:

- None

1.11.13.1.3.1.2.5 Hotfixes rolled up into this release - Application Migration:

- Q22078 - Direct Membership Based Management Group Support In Task Sequence API. (TFS 250710)

1.11.13.1.3.1.2.6 Hotfixes rolled up into this release - Toolkit

- Q22032 - Incorrect domain suffix is appended to a device name when using Tachyon Instruction Runner (TFS 247012)
- Q21848 - Tachyon Instruction Runner will not run against a collection with a comma in the name (TFS 246056)

1.11.13.1.3.1.2.7 Hotfixes rolled up into this release - Nomad and Content Distribution:

- Q22048 - An unhandled exception is thrown if Content Distribution is installed on a non-English server. (TFS 247999)
- Q22010 - Task sequence does not get synced if an entry of precached task sequence was created before the CMSync (TFS 247742)
- Q21984 - Multiple Task sequences with same name displayed on Nomad dashboard TaskSequence page. (TFS 246962)
- Q21982 - Nomad Sites page on Nomad dashboard displays 0 for “Unknown” category of site. (TFS 246477)
- Q21980 - NomadBranch Admin UI Extensions: "Pre-caching Jobs" view only shows 50 most recent jobs (TFS 246609)
- Q21978 - Device tab displays status as "Partially Downloaded" (TFS 247193)
- Q21976 - Subnet Drawer displays "Partially downloaded" status (TFS 247268)
- Q21974 - Selecting Subnet Drawer of TS content causes exception (TFS 247269)
- Q21972 - Precache jobs report incorrectly as “Partially Downloaded” (TFS 245156)
- Q21856 - Subnets counts on Nomad Site page gets changed by changing time filter. (TFS 245938)
- Q21854 - Subnet Drawers and Site Detail page shows null subnet (TFS 245937)
- Q21852 - Device Details page shows incorrect counts (TFS 245936)
- Q21850 - Content Details page never returns data. (TFS 245939)

1.11.13.1.3.1.2.8 Hotfixes rolled up into this release - Business Intelligence:

- None

1.11.13.1.3.2 Web Release-8.0 (29-Oct-2021)

1.11.13.1.3.2.1 Tachyon Server 8.0.4.237 - Tachyon Toolkit 8.0.4.237 - 1E Catalog 8.0.4.28 - Software Lifecycle Automation 8.0.4.135 - Business Intelligence 8.0.4.10 - ContentDistribution 8.0.4.323 - AppClarity 8.0.4.32 - ApplicationMigration 8.0.4.37

1.11.13.1.3.2.2 Platform v8.0

- Significant changes to **Permissions** (role-based access control)
  - Role name changes, listed in Roles page
  - Some roles can be delegated to users by assignment to Management Groups
  - Re-design of Permissions management
- **Custom properties** have been extended to enable the creation of Management Groups based on device and software tags
  - **Device Tags** (previously called Coverage Tags)
  - **Software Tags** (new in this version)
- **Management Groups** feature improvements make it easier to represent your existing management structure in Tachyon
  - Organize Management Groups into a hierarchy (new in this version)
  - Easily create complex Management Group definitions using the **Management Group Rule Builder** (new in this version)
  - **Additional Rule Attributes** - build Management Group rules based on **Device** and **Software** Tags
- **Software Tags** and **Notes** can be added to each VTVE in Software Inventory.

1.11.13.1.3.2.3 Consumer applications for v8.0

- **AppClarity 8.0:**
  - Works with Tachyon Platform 8.0
  - No features or feature changes added in this release, but includes any hotfixes from previous versions.
- **Application Migration 8.0:**
  - Works with Tachyon Platform 8.0
  - No features or feature changes added in this release, but includes any hotfixes from previous versions.
- **Explorer 8.0:**
  - Works with Tachyon Platform 8.0

- Coverage tags renamed as **Device tags**
- No features or feature changes added in this release, but includes any hotfixes from previous versions.

- **Experience 8.0:**
  - Works with Tachyon Platform 8.0
  - The user interface has been re-organized and provides several new pages and popups:
    - Experience Analytics:
      - The existing Overview, Categories, Stability, Responsiveness, Performance and Sentiment pages are now re-organized under Experience Analytics.
    - Advanced Analytics:
      - **Network**: includes scored and raw metrics for Bytes Sent/Received per Second, Outbound Packets Discarded, Packet Outbound Errors, Active TCP Connections, Network Retransmit Rates, Network Usage Overall, Network Bandwidth Utilization, Wireless Send and Receive Rate, Wireless Transmit Rate.
      - **Boot and Login**: includes scored and raw metrics for Policy Processing, Startup Apps Processing Time, Main Path Boot Time, Post Boot Time.
    - Inventory Management:
      - **Devices page** - displays device-centric metrics including details such as network configuration (IP, Gateway, Connection Type, OS Install Date)
      - **Software page** - displays software products with the software associated metrics and inventory details
      - **Users page** - displays information on the users known to Tachyon via the 1E Client.
    - User Engagements. The existing Surveys feature has been renamed and re-organized under User Engagements and extended
      - **Announcement Feature**: Engage users via announcements and urgent announcements/notifications.
      - User Sentiment Surveys are now called **Sentiment Surveys**.
      - General Purpose Surveys are now called **Info Surveys**.
    - Root Cause Analysis tools - two new popups have been added to the Devices page:
      - **Device comparison**: highlights the differences between two selected devices related to Operating System Details, Hardware Details, Usage Details, Installed Software, Services and Processes

    - **Scatter chart**: Quadrant placement of devices, plots devices on a chart with customizable X and Y axes (align on the grid based on metrics, scores etc.)

- A variety of data types are now available to add as columns in the table views:
    - Score - values that have been processed and normalized by Experience, this may include consolidation and combinations of other data
    - Raw - the unprocessed and un-normalized values retrieved from devices
    - Device Details - information related to devices, such as: IP Address, DHCP Server, Operating System etc.
    - Software Details - information related to software, such as: the Architecture supported by the software
    - Event - event information retrieved from devices, such as: Software uninstall, hang and crash events; Operating System boot and crash events, and many others
- Network related scores have been added to enhance the overall user experience score:
    - **Output queue length** - scores the network transmission backlog, based on the length of the output packet queue
    - **Wireless Signal Quality** - scores the signal quality of the wireless network connection on the device.

- **Guaranteed State 8.0:**
    - Works with Tachyon Platform 8.0
    - No features or feature changes added in this release, but includes any hotfixes from previous versions.
- **Nomad 8.0:**
    - Works with Tachyon Platform 8.0
    - **Integrating Nomad with WakeUp**
    - Enhancements:
        - Task Sequence support for Windows feature updates
        - Automatic grooming of the Content Distribution database
        - Support for Windows Authentication between Background Channel and Content Distribution API
        - Tachyon Setup: Nomad screen has improved authentication options
        - Improving performance of the dashboards
        - API versioning using Tachyon SDK.
- **Patch Success 8.0:**

- Works with Tachyon Platform 8.0
- No features or feature changes added in this release, but includes any hotfixes from previous versions.

1.11.13.1.3.2.4 Product Packs for v8.0

- **Classic Product Packs:**
  - 1E-ConfigMgrConsoleExtensions.zip
  - 1E-Experience.zip
  - 1E-Explorer-TachyonAgent.zip (new instruction: 1E-Explorer-Upgrade1EClient8.0macOS, updated instruction: Set1EClientAgentConfig)
  - 1E-Explorer-TachyonCore.zip
  - 1E-Inventory.zip
  - 1E-Nomad.zip (new instructions: 1E-Nomad-CacheCleanerDeleteAll, 1E-Nomad-LocationDiscovery, 1E-Nomad-SetWorkRate)
  - 1E-Patch-Success.zip
  - 1E-Tachyon-Platform.zip (new instruction: 1E-TachyonPlatform-Device-ComparisonData)
- **Integrated Product Packs:**
  - MEMCM Client Health Integrated Product Pack (new preconditions: MEMCM-Client, Network-IPv4-PrimaryAddressInDNS, and some rules modified to use them)
  - NomadClientHealth.zip (minor changes)
  - TachyonCore.zip (minor changes)
  - WindowsClientHealth.zip (minor changes).
- Other Product Packs are available from the Tachyon Exchange: tachyonexchange.1e.com

1.11.13.1.3.2.5 Enhancements in v8.0

- Platform:
  - Device Deduplication also includes Nomad
  - Ability to set the Experience Cube processing time (ExperienceSync) is also described on the Device Deduplication page.
  - New options for Switch Command Lines
  - AI Powered Auto-curation: Changing the AI Deployment path
- **Tachyon Setup**
  - Hotfix installer supports preconditions
  - Support for **mst** transform files

- Nomad screen has improved authentication options
- Maintenance feature includes support for updating Nomad proxy

- **Tachyon Product Pack deployment tool**
  - Supports alternative credentials.

1.11.13.1.3.2.6 Enhancements for v8.0

1.11.13.1.3.2.6.1 Hotfixes rolled up into this release - Server (including Experience, Explorer, and Guaranteed State):

- Q21760 - Cross Forest without trust DMZ switch trying to bind on manager port on NATed IP which fails and eventually kills the switch (TFS 244306)
- Q21758 - Wrong Devices Returned From Management Group Member Retrieval api when Device and Patch consolidation report is in process (TFS 235368)
- Q21756 - GS - Rules removed from all assigned policies (TFS 244253)
- Q21748 - Switch system health check is failing for some switches (TFS 240529)
- Q21688 - Nomad application - crash on the device details page when device does not exist in Tachyon (TFS 235249)
- Q21686 - Platform - Group membership resolution fails when nested group search is disabled (TFS 234348)
- Q21684 - Experience - What's Changed (last 7 days) - Not enough data to show deltas (TFS 234748)
- Q21682 - Experience - Timeouts occur during SQL partition processing for Experience (TFS 235469)
- Q21680 - Platform - Duplicate devices appear in Tachyon and Nomad dashboards (TFS 229352)
- Q21660 - Platform - Hotfix Utility - throws exception when a patch is applied on workgroup - DMZ Server (TFS 235801)
- Q21626 - Platform - Tachyon Setup.exe--Maintenance--Server Certificate option fails to update binding with selected certificate correctly (TFS 233846)
- Q21624 - Platform - Experience - Timeout errors when inserting offloaded experience data during cube processing (TFS 233425)
- Q21622 - Tachyon - Number of clients connected to switch drops (TFS 233339)
- Q21620 - Platform - Guaranteed State - TachyonResponses-PolicyRule_0 table is unable to manage partitions after it reaches 10 (TFS 234759)
- Q21618 - Background channel unable to load client certificate private keys behind the CNG API (TFS 234777)
- Q21616 - Switch - Erroneous 'Total Sent' counts. (TFS 235011)
- Q21564 - Experience - Experience is keeping master groomed devices for longer than it should (TFS 228555)

- Q21562 - Platform - CSV Export to UNC path should be more constrained (TFS 138387)
- Q21560 - Platform - Change to timing for Experience cube sync (TFS 227857)
- Q21558 - Platform - Instructions not receiving any responses (TFS 226038)
- Q21556 - Platform – Not all Switches come back online after a reboot (TFS 227933)
- Q21554 - Platform – Tachyon Switches went offline (TFS 228930)
- Q21552 - Switch - Number of Online machines differs across Tachyon Explorer (TFS 228154)
- Q21550 - Platform - Some Clients are not responding to Tachyon instructions (TFS 226839)
- Q21548 - Platform - Export All task failing due to SQL login timeout by bcp.exe (TFS 230869)
- Q21546 - Platform - Guaranteed State - Device/Rule History will take a long time to display with large amounts of data (TFS 231327)

1.11.13.1.3.2.6.2 Hotfixes rolled up into this release - SLA:

- Q21762 - Wrong Devices Returned From Management Group Member Retrieval api when Device and Patch consolidation report is in process. (TFS 244355)
- Q21746 - Management Group Sync with Powershell clashing causing empty Management Groups (TFS 241903)
- Q21744 - Management Group Evaluation is taking time in completing a cycle. (TFS 241990)
- Q21742 - Management Group Sync with Powershell clashing causing empty Management Groups. (TFS 241975)
- Q21740 - Clean Sync and Clear Data action failing with foreign key violation error. (TFS 237160)
- Q21738 - Duplicate entries in Management Group instance total. (TFS 241971)
- Q21736 - Correct device info is not picked up in case of device collision when same device is coming from 2 different connectors . (TFS 231155)
- Q21734 - Management Group not showing any device if rule is created on basis of installed software. (TFS 236925)
- Q21732 - OU information is not consolidated correctly in Basic Inventory Consolidation. (TFS 240608)
- Q21730 - IsCMClient value is not populating correctly for a device if device is reported from both Tachyon and CM connector. (TFS 231005)
- Q21728 - No OU information were consolidated for such devices which was reported from a single connector. (TFS 242259)
- Q21658 - Inventory - Clean Sync leaves orphan Attachment IDs in Attachment table. (TFS 235178)
- Q21656 - Inventory - The File Upload connector does not process device data when uploading a file that contains column OSManufacturer (TFS 234923)
- Q21654 - Inventory - Basic Inventory Consolidation takes too much time to complete (TFS 232513)

- Q21652 - SLA - Device and Patch consolidation fails with Arithmetic Overflow error. (TFS 231525)
- Q21650 - Inventory - Device Serial number is null in SLA-Data database (TFS 229622)
- Q21648 - Inventory - WSUS Connector device data is inflating the inventory with stale devices that no longer exist (TFS 228571)
- Q21646 - Inventory - Tempdb filling up causing BIC to fail (TFS 231526)
- Q21644 - Inventory - Tachyon Master device table OS information not correctly handled by BIC (TFS 227957)
- Q21642 - SLA: Tachyon is not properly processing the primary user data from the Tachyon connector (TFS 227750)
- Q21640 - SLA: Software Inventory not being reported correctly due to SCCM having multiple ResourceIDs for the same hostname (TFS 227755)
- Q21638 - SLA: Management Groups contain devices that don't match the rules (TFS 221910)
- Q21636 - SLA: Different usage categories between AppClarity versions (TFS 227142)
- Q21634 - SLA : Failure when editing policy. (TFS 218751)

1.11.13.1.3.2.6.3 Hotfixes rolled up into this release - Catalog:

- None

1.11.13.1.3.2.6.4 Hotfixes rolled up into this release - AppClarity:

- Q21722 - AppClarity - Total counts of Units Reclaimed and savings are dropping on Software Reclaim Summary and Savings pages (TFS 232667)
- Q21720 - AppClarity - Reclaim popup appears incorrectly on large number of devices as installations falls into unused category due to sync issue (TFS 240329)
- Q21718 - AppClarity - Filter not working on 'Price per unit' column on reclaim usage summary page (TFS 217531)
- Q21596 - AppClarity - Reclaimer Popup reappears after user has clicked "remove now" button (TFS 227253)
- Q21594 - AppClarity - Entitlements are not imported correctly for large number of entitlements in TSV file (TFS 234655).

1.11.13.1.3.2.6.5 Hotfixes rolled up into this release - Application Migration:

- Q21570 - AppMigration Role Based Application Set rules (TFS 233385)

1.11.13.1.3.2.6.6 Hotfixes rolled up into this release - Nomad and Content Distribution:

- Q21754 - CM Sync fails to sync content because of null SourceVersion (TFS 241994)
- Q21750 - Nomad clients are unable to communicate with ContentDistribution (TFS 244275)
- Q21702 - An error occurred whilst migrating legacy pre cache data. CM sync failed. (TFS 237645)
- Q21700 - Get Migration Settings TS action sets an incorrect PBAComputerName for restore (TFS 239635)

- Q21698 - Failed to register devices because Ip4SubnetAddr column does not allow nulls. (TFS 232498)
- Q21678 - Duplicate Devices in Tachyon and Nomad dashboards (TFS 229352)
- Q21612 - Support for feature updates in TS (TFS 233798)
- Q21610 - Known Subnets are showing under Unknown as well in Nomad Dashboard (TFS 234520)
- Q21608 - CM sync's failing in CD due to FOREIGN KEY constraint (TFS 234770)
- Q21598 - CM Sync's failing in Content Distribution (TFS 233608)

1.11.13.1.3.2.6.7 Hotfixes rolled up into this release - Business Intelligence:

- None

1.11.13.1.3.3 Web Release-5.2 (28-Apr-2021)

1.11.13.1.3.3.1 Tachyon Server 5.2.5.165 - Tachyon Toolkit 5.2.5.165 - 1E Catalog 2.1.100.28 - Software Lifecycle Automation 5.2.5.160 - Business Intelligence 3.4.5.18 - ContentDistribution 1.0.5.1068 - AppClarity 7.1.105.37 - AppMigration 3.1.105.10

1.11.13.1.3.3.2 Platform v5.2

- **Tachyon Platform:**
  - Support for **Content Distribution** and its **Nomad app**
  - Background Channel provides a reverse proxy (including devicesAuthentication options) to support communication between Nomad clients and Content Distribution
  - User Interface telemetry reports how the user interface is used
  - Device View provides a single page of details about any device with key information from and links to licensed Tachyon consumer applications
  - New feature that synchronously runs instructions on single device, with results briefly cached in memory instead of a database (used by the Device View feature)
- **Inventory application:**
  - Microsoft Office 365 connector - new
  - 24 hours sync cycle for Tachyon connector
  - Direct-based management groups and sample PowerShell scripts
- **Settings application:**
  - System health page - new
  - Deploy button on Consumers page to deploy all policies for all registered consumers, to support consumers that do not have their own Deploy button
- **Tachyon Setup:**
  - Installation of Nomad consumer application

        - ActiveEfficiency is replaced by Content Distribution when upgrading, with database backup, and a redirect provided for legacy Nomad clients
        - Configures the reverse proxy in the Background Channel for new Nomad clients
        - Setup deploys Nomad event policies after successful installation
    - Tachyon Setup's Nomad screen now uses SMS Provider to locate SQL database, and validates CM Site server during installation and upgrade
    - Two-stage automation of Implementing a Tachyon DMZ Server
    - New option for User Interface telemetry on Tachyon Setup's Telemetry screen
    - Support for multiple HTTPS bindings
        - Selection of existing certificate during upgrade when multiple bindings are encountered
        - Option to specify an alternate HTTPS binding on Tachyon Setup's Website configuration screen - required for DMZ Server

1.11.13.1.3.3.3 Consumer applications for v5.2

- **AppClarity 7.1.105:**

  The AppClarity 7.1.105 maintenance release contains a number of bug fixes:

  - Works with Tachyon Platform 5.2
  - No features or feature changes added in this maintenance release.

  The main AppClarity 7.1 release contained the following features:

  - Works with Tachyon 5.1
  - Windows Server OS LDC
    - New license demand for core based licensing of Windows Server OS (calculated with-in Microsoft Core LDC)
    - Compliance calculation is now based on new license demand
  - Support for Currency Conversion
    - When you can set a default currency (other than USD) AppClarity now renders all reporting and financial numbers (or graphs) only in that set currency
  - New UI controlsNew UI controls have been added to improve the usability:
    - Report refresh - ability to refresh reports on individual pages, and the ability to view the status of the last report refresh
    - UI Controls - ability to choose columns as either shown or hidden on individual screens
  - Installation mode change

- AppClarity installer is now included as an app with the Tachyon installer and can be installed and maintained this way
- Hotfixing capability

- Enhancements
  - Entitlement
    - New Active Entitlements Only toggle filter on Entitlement Summary page
    - The ability to export entitlement summary data
  - License Demand
    - Device names are now shown as hyperlinks on LDC reports
  - Compliance
    - Improved logic for rendering installs, and a new "Exempt" status on the compliance detailed table
    - Effective License Position (ELP) displayed for SQL Server components as it is for SQL Server entitlement
  - Reclaim
    - Reclaim product usage screen loading time is optimized for quick page load.

- **Application Migration 3.1.105:**

  Features in the Application Migration 3.1.105 maintenance release:

  - Works with Tachyon Platform 5.2
  - No new features in this maintenance release.

  Features in the main Application Migration 3.1 release:

  - Works with Tachyon 5.1
  - Improvements to upgrade rules to support scenarios where the currently installed software has a later version than the one listed in the upgrade rule - In versions prior to Application Migration 3.1, it was possible that upgrade rules had issues when the application they were trying to upgrade on the client devices were later versions than the ones they were trying to upgrade to. To remedy these unpredictable and unwanted results, now if an upgrade rule tries to downgrade an application then it will be ignored.
  - Application and Package installation success has been improved - this handles scenarios where the administrator has forgotten to check the **Allow this application to be installed from the Install Application task sequence action without being deployed** checkbox, which is a prerequisite for migrating an application. In practice, it was a common error for administrators to overlook this, which - in earlier versions - led to the Task Sequence failing. In Application Migration 3.1, if the administrator forgets to set the

checkbox, a warning is now displayed that lets the administrator continue and Application Migration sets the option automatically.

- Multiple exclusion of applications is now supported from the Installations page.

- **Explorer 5.2:**
  - Works with Tachyon Platform 5.2
  - Devices table and dashboard link through to Device View.
- **Experience 1.3:**
  - Works with Tachyon Platform 5.2
  - Deploy button on Surveys page now only deploys Experience policies
  - Devices page links through to Device View
  - 1E Experience product pack to support Experience features of the Device View
  - Users page "User session reactiveness" column has been renamed to "Application responsiveness"
- **Guaranteed State 1.5:**
  - Works with Tachyon Platform 5.2
  - Deploy button on Policies page now only deploys Guaranteed State policies
  - Integrated Product Packs:
    - MEMCM Client Health Integrated Product Pack (minor changes)
    - NomadClientHealth.zip (minor changes)
    - TachyonCore.zip (minor changes)
    - WindowsClientHealth.zip (minor changes).
  - Other Product Packs are available from the Tachyon Exchange: tachyonexchange.1e.com
- **Nomad 1.0 (New app in 5.2):**
  - Works with Tachyon Platform 5.2
  - **Modernized backend infrastructure** - Nomad requires a back-end server, which was previously the legacy ActiveEfficiency platform, this has been replaced by the Tachyon Platform to provide Single-Site download, Pre-caching and a new Dashboard. For customers moving to Modern Management, Nomad provides visibility and control of Delivery Optimization, which is used by Intune, MS store and MS update.
  - **Leverage the Tachyon Platform and 1E Client** - with the Tachyon Platform you can enable further features including Experience, User Sentiment, Guaranteed State and Patch Success, as well as opening up real-time management to any task by acquiring the appropriate license.

- **Content Distribution** - Content Distribution is a new component of the Tachyon Platform that provides control and visibility on content deployments and delivery in an organization
    - Replaces ActiveEfficiency features, maintaining support during upgrade for legacy Nomad clients (versions earlier than Nomad 7.1 in 1E Client 5.2)
    - Nomad 7.1 clients now connect to Tachyon Response Stack components (Switch and Background Channel) which act as a proxy for Content Distribution, and legacy clients continue to connect directly to Content Distribution.
- **Nomad app** - the user interface for Content Distribution, provides real-time visibility of what content is downloading or available in each location, subnet and client, see how much WAN traffic is being saved overall and each day
    - **Delivery Optimization (DO) Visibility** - visibility of Delivery Optimization downloads and content availability in each location, subnet and device
    - **Delivery Optimization (DO) and Windows Update Agent (WUA) monitoring** - track Windows download or Microsoft Endpoint Configuration Manager deployments on clients being downloaded via Delivery Optimization in real time, their peer to peer downloads efficiency, sources of the downloaded content and see this reported in the Nomad app dashboards
    - **Overview page** - gives a high-level view of the current status of content throughout the entire network
    - **Content page** - provides a Content-centric view of content distributed throughout your network
    - **Task Sequences page** - provides that visibility by grouping the reference content for each Task Sequence into a single view, so you can see which content is cached and which is not
    - **Devices page** - lists all Devices that have sent Nomad device registration events and have sent download events within a selected time period, links through to Device View
    - **Nomad Sites page** - shows how the network is being used for content distribution in different locations
    - **Client Health page** - shows information from two Integrated Product Packs provided with the Tachyon Platform.

- **Patch Success 1.3:**
    - Works with Tachyon Platform 5.2
    - Devices page and Patch Success Overview page link through to Device View
    - Unidentified patch publish dates show 'Not available' instead of 1970-01-01.

1.11.13.1.3.3.4 Product Packs for v5.2

- **Classic Product Packs:**
    - 1E-ConfigMgrConsoleExtensions.zip (minor changes)

- 1E-Experience.zip (**new** pack in 5.2, with instructions to support Device View)
- 1E-Explorer-TachyonAgent.zip (minor changes)
- 1E-Explorer-TachyonCore.zip (minor changes, additional instructions to support Device View)
- 1E-Inventory.zip (1E-Inventory-Device-GetProcessors improved, 1E-PatchSuccess-PatchStatus now only runs on Windows)
- 1E-Nomad.zip (**new** pack in 5.2, previously provided with Nomad, includes additional instructions to support Device View)
- 1E-Patch-Success.zip (minor changes)
- 1E-Tachyon-Platform.zip (minor changes, additional instructions to support Device View).

· **Integrated Product Packs:**

- MEMCM Client Health Integrated Product Pack (minor changes)
- NomadClientHealth.zip (minor changes)
- TachyonCore.zip (minor changes)
- WindowsClientHealth.zip (minor changes).

· Other Product Packs are available from the Tachyon Exchange: tachyonexchange.1e.com

1.11.13.1.3.3.5 Enhancements in v5.2

· Platform:

- Additional details in device online messages "OsLocale" and "OSInstallUtc" visible in Device View
- Support for each consumer independently deploying its own policies
- Support for dynamic Coordinator Module registration
- Switch Performance Counters now support multiple switches
- Switch denial-of-service protection is now set to off by default
- Business Intelligence - credentials no longer stored in encrypted configuration file.
- Support for SCCM2006 and SCCM2010
- Support for Windows Server 2012 R2 dropped

· Inventory application

- Upgrade Improvements
- Handling of unicode char of Vendor in Processor_cr and Device_cr during Catalog sync
- The check has been extended for those Versions which have a long numeric value in the Product_cr and will not insert this kind of records in the 1ECatalog

- Catalog product creation procedure has been modified to not attempt creating “Product” without corresponding "Vendor"
- Check has been extended in case of Windows and Windows Server to include three-part version (10.0.x) in the Auto-curation, which will return the unique colloquial version.

- Tachyon Setup
  - Consumer-specific policy deployment during upgrade/installation
  - Support to patch Tachyon Server successfully in SQL High-Availability Setup
  - Support to disable SQL scan during installation.

1.11.13.1.3.3.6 Enhancements for v5.2

1.11.13.1.3.3.6.1 Hotfixes rolled up into this release - Server (including Experience, Explorer, and Guaranteed State):

- Q21426 - Platform - Guaranteed State policy changes are deployed without using Deploy button. (TFS 226416)
- Q21424 - Platform - Infrastructure log error - StateMachine Initialise failed. Check for wrong XML in the workflow definition. (TFS 221269)
- Q21422 - Platform - Mismatch between number of devices returned for Management Group and the count in the header (TFS 226897)
- Q21420 - Platform - Some Clients are not responding to Tachyon instructions (TFS 226839)
- Q21418 - Platform - Instructions not receiving any responses (TFS 226038)
- Q21404 - Platform - Tachyon Switch crash when logging 'Session raw writes' (TFS 222683)
- Q21342 - Platform - Experience Database growing at a steady pace filling up drive space (TFS 218297)
- Q21340 - Platform - Devices being groomed from Tachyon database when the LastConnUtc being reset to time (zero) (TFS 220090)
- Q21338 - Platform - Management Group membership synchronization from Platform to Experience is failing (TFS 220175)
- Q21326 - Platform - Switch device upload thread stalled waiting for a HTTP response that never comes (TFS 219898)
- Q21322 - Platform - DBNULL errors in Core API log (TFS 218336)
- Q21320 - Platform - Number of clients shown online in console not matching connections (TFS 219164)
- Q21316 - UI - Experience – Metrics hyperlinks do not work in What’s Changed (last 7 days) charts after applying hotfix Q21198 (TFS 218801)
- Q21314 - Platform - Tachyon switch will crash on empty Management groups (TFS 218673)
- Q21312 - Platform - Tachyon may fail to process experience data synchronization and cube processing (TFS 218349)

- Q21310 - Platform – Scheduled UTC time for sync firing off at the wrong local time (TFS 218552)
- Q21276 - Platform – Switch – Switch does not start (TFS 216338)
- Q21274 - Platform - Switch - Tachyon shows 0 devices connected (TFS 211468)
- Q21272 - Platform - Tachyon Switch does not send GS Policy until 1E Client restarts (TFS 217028)
- Q21270 - Platform - Certain localization settings cause no data to appear in the Experience UI (TFS 217171)
- Q21248 - UI - Experience - Experience Numbers don't add up (TFS 214589)
- Q21246 - Platform - Licensing - Tachyon.lic filesize is larger than current limit (TFS 216700)
- Q21244 - Platform - Tachyon Core API is exhausting ephemeral ports while offloading events (TFS 216403)
- Q21242 - Platform - Tachyon Coordinator service seems to get stuck and email notifications are not sent to the Tachyon admin (TFS 212094)
- Q21240 - Platform – Switch - Guaranteed State showing unknown state for certain rules. (TFS 216386)
- Q21212 - Platform - Experience - SQL query fails with uncaught exception when trying to fetch events for selected device (TFS 214865)
- Q21210 - Platform - Cube processing put a lock on UserSurveyPerformanceMetric table (TFS 214436)
- Q21208 - UI - Guaranteed State - Not possible to apply filter when the windows size is not full screen (TFS 213722)
- Q21206 - UI - Guaranteed State - Reports->Devices->View Details link - Not possible to view more than 100 records (scroll bar not available) (TFS 214207)
- Q21204 - UI - Guaranteed State - Unauthorised error message is displayed for Guaranteed State Viewers user (TFS 215201)
- Q21202 - UI - Experience - User Sentiment->Score calculation text indicates no survey is available, even though surveys are present (TFS 212676)
- Q21200 - Platform - Experience - Description for overall experience score doesn't mention user sentiment (TFS 212609)
- Q21198 - Platform - Experience - 'What's changed' chart on the Overview screen doesn't work if you add a filter when you have surveys. (TFS 213260)
- Q21196 - UI - Experience - Devices page - sort order is not indicated when sorting with any column header except FQDN (TFS 212592)
- Q21194 - UI - Experience - UI displays empty screen with 'An error ocurred' if a survey is deleted that's used by a preset. (TFS 213200)
- Q21192 - Platform - Second is not a supported unit for date/time-based visualizations (TFS 213337)
- Q21190 - Platform - Experience - Performance page -> Information icon missing for Network tile (TFS 212737)

- Q21188 - UI - Experience - Sentiment->User Sentiment->View Detailed Data->sorting Matching devices is not working (TFS 212732)
- Q21186 - UI - Experience - Surveys Page -> The selected survey responses cannot be sorted against Date column. (TFS 212678)
- Q21184 - Platform - Experience - Devices page-> Cannot filter events against Description column on selected device event log (TFS 214215)
- Q21182 - Platform - Experience - Users page incorrectly displays/sorts metrics if the name clashes with a 'User Sentiment' survey (TFS 212604)
- Q21180 - UI - Experience - Breakdown By drop down-> Others Filter -> Should not be allowed to drill into (TFS 214859)
- Q21178 - Platform - Guaranteed State - Reports->Devices->View Details link lists the records in ASC order, by default instead of DESC (TFS 214204)
- Q21176 - Platform - Duplicate non-metric survey can be created by Clone Survey action (TFS 215348)
- Q21174 - Platform - Certain regional settings break device performance scoring (TFS 214980)
- Q21164 - AppClarity upgrade is failing due to HTTP request timeout while uploading the ACS file from Portal API to SLA Platform API (TFS 214950)

1.11.13.1.3.3.6.2 Hotfixes rolled up into this release - SLA:

- Q21392 - SLA: Virtual machines categorized into the “Unknown” category (TFS 220815)
- Q21390 - SLA: AppClarity loading individual entitlements takes 50 seconds (TFS 217118)
- Q21344 - SLA : Failure when editing policy. (TFS 218751)
- Q21318 - SLA - SCCM Connector sync fails when a device is reported as having 0 processor cores (TFS 218609)
- Q21157 - SLA: Upgraded schedules can not be edited for some cases (TFS 213456)
- Q21155 - SLA - Data type conversion error occurs during the Basic Inventory Consolidation if the date is older than epoch date (TFS 211476)

1.11.13.1.3.3.6.3 Hotfixes rolled up into this release - Catalog:

- Q21234 - Patch Success doesn't show specific information regarding the Operating System
- Q21168 - SLA - Tachyon Sync Failing (BIC) with Rollback Transaction Error

1.11.13.1.3.3.6.4 Hotfixes rolled up into this release - AppClarity:

- Q21308 - AppClarity - Reclaim action results are not saved for optional reclaim policies on certain products (TFS 211745)
- Q21306 - AppClarity – Missing costs affect calculation of Effective License Position (TFS 193527)
- Q21304 - AppClarity – Perpetual entitlements with future dates are included with 'Active Entitlements Only' filter (TFS 213388)
- Q21302 - AppClarity – Entitlement import increases the Quantity of licenses (TFS 212841)

- Q21300 - AppClarity – Reclaim Usage page does not load in Internet Explorer browser (TFS 208574)
- Q21298 - AppClarity – While creating a New License entitlement, certain characters in the Product SKU field cause an error (TFS 208968)
- Q21296 - AppClarity – A duplicate entitlement is created when an existing entitlement with SKU is edited and saved as draft (TFS 197392)
- Q21294 - AppClarity – Entitlement import incorrectly saves Version as .* (TFS 186415)
- Q21292 - AppClarity – When a Reclaim policy is cancelled, the Provider log does not show "Completed On" time in UTC (TFS 211766)
- Q21290 - AppClarity – The Top 10 Saving Opportunities chart incorrectly filters the Reclaim Usage table (TFS 211166)
- Q21288 - AppClarity – Entitlements created as Colloquial version are converted to DotFormat version (TFS 211159)
- Q21238 - AppClarity – Pagination not working in Entitlements Contracts page (TFS 213990)

1.11.13.1.3.3.6.5 Hotfixes rolled up into this release - Application Migration:

- Q21410 - Broken association API improvement to handle large application migration rules count (TFS 222660)
- Q21286 - Application Migration – allow use of OU Path rule (TFS 213954)

1.11.13.1.3.3.6.6 Hotfixes rolled up into this release - Business Intelligence:

- Q21428 - BI - Cube having a slow refresh time with SQL views (TFS 222048)

1.11.13.1.3.4Web Release-5.1 (03-Sep-2020)

1.11.13.1.3.4.1 Tachyon Server 5.1.0.663 - Tachyon Toolkit 5.1.0.663 - 1E Catalog 2.1.0.140 - Software Lifecycle Automation 5.1.0.755 - Business Intelligence 3.3.0.61 - ActiveEfficiency Server 1.10.100.10 - AppClarity 7.1.0.95 - AppMigration 3.1.0.172

1.11.13.1.3.4.2 Platform v5.1

- **Tachyon:**
  - Improved support for multi-forest and multi-domain Active Directory environments. Multiple domains can be set during setup.
  - Telemetry gathering on Tachyon usage statistics to help with 1E's continued product improvement initiative.
  - Tachyon Portal and emails can be customized with your company logo and branding.
  - Support withdrawn for Internet Explorer 11 and Legacy Microsoft Edge.
  - Switch Performance Counters.
  - Enhancements:
    - RBAC naming has been improved by changing the permissions name from **Instrumentation** to **Infrastructure**.

- Support for Microsoft System Center Configuration Manager CB 2002.
- Tachyon platform instrumentation data is now exposed as Windows Performance Counters.
- Platform installation and deployment has been simplified by eliminating the Tachyon CoreInternal component.

- **Inventory application:**
  - The Inventory application has some additional pages that provide information on your system, as gathered by inventory connectors:
    - The **Software Inventory** section provides **Dashboard**, **Aggregate** and **Product Usage** pages to help you understand the software that is installed in your enterprise
    - The **Hardware** section lets you investigate the virtual machines and physical devices present in your enterprise by using its **Hardware Inventory**, **Virtual Summary** and **Device** pages
  - Export option now available on the **Inventory→Hardware→Hardware Inventory** page.
  - Sync actions for Connectors allow you select which data categories you want to sync, and if you want to run **AI Powered Auto-curation** as part of Basic Inventory Consolidation (BIC) process that runs after each sync.
  - 1E Catalog:
    - Improved hotfix capability.
    - Catalog documentation merged with Tachyon.
- **Settings application:**
  - Tachyon connector optimization - the duration of inventory instructions has been reduced from 7 days to 15 minutes to allow them to be run more frequently
  - Other Connector optimizations:
    - Ability to request selected data when scheduling a sync. For example, Device, Software, User, Patch etc. This has been added to the Tachyon, Configuration Manager and ServiceNow connectors
    - The Device and Patch Consolidation reports have been split from the Basic Inventory Consolidation action. Patch Success users can now just execute the Device and Patch consolidation reports rather than running a complete Basic Inventory Consolidation.
    - AI actions have been decoupled from the Inventory synchronization cycles.
  - A new **Provider log** page has been added that provides the status of Provider related operations
  - **AI Powered Auto-curation** can be turned on or off from the Components page.

- **Intune connector** - device, software and user data can now be retrieved from your Intune infrastructure.

- **Tachyon Setup enhancements:**
  - Maintenance screen Hotfixing feature to upload and apply a 1E Hotfix bundle.
  - Installation of AppClarity 7.1 and Application Migration 3.1 (using their installers).

1.11.13.1.3.4.3 Consumer applications for v5.1

- **AppClarity 7.1:**
  - Windows Server OS LDC
    - New license demand for core based licensing of Windows Server OS (calculated with-in Microsoft Core LDC)
    - Compliance calculation is now based on new license demand
  - Support for Currency Conversion
    - When you can set a default currency (other than USD) AppClarity now renders all reporting and financial numbers (or graphs) only in that set currency
  - New UI controls have been added to improve the usability:
    - Report refresh - ability to refresh reports on individual pages, and the ability to view the status of the last report refresh
    - UI Controls - ability to choose columns as either shown or hidden on individual screens
  - Installation mode change
    - AppClarity installer is now included as an app with the Tachyon installer and can be installed and maintained this way
    - Hotfixing capability
  - Enhancements
    - Entitlement
      - New Active Entitlements Only toggle filter on Entitlement Summary page
      - The ability to export entitlement summary data
    - License Demand
      - Device names are now shown as hyperlinks on LDC reports
    - Compliance
      - Improved logic for rendering installs, and a new "Exempt" status on the compliance detailed table

  - Effective License Position (ELP) displayed for SQL Server components as it is for SQL Server entitlement

- Reclaim
  - Reclaim product usage screen loading time is optimized for quick page load.

- **Application Migration 3.1:**
  - Improvements to upgrade rules to support scenarios where the currently installed software has a later version than the one listed in the upgrade rule - In versions prior to Application Migration 3.1, it was possible that upgrade rules had issues when the application they were trying to upgrade on the client devices were later versions than the ones they were trying to upgrade to. To remedy these unpredictable and unwanted results, now if an upgrade rule tries to downgrade an application then it will be ignored.
  - Application and Package installation success has been improved - this handles scenarios where the administrator has forgotten to check the **Allow this application to be installed from the Install Application task sequence action without being deployed** checkbox, which is a prerequisite for migrating an application. In practice, it was a common error for administrators to overlook this, which - in earlier versions - led to the Task Sequence failing. In Application Migration 3.1, if the administrator forgets to set the checkbox, a warning is now displayed that lets the administrator continue and Application Migration sets the option automatically.
  - Multiple exclusion of applications is now supported from the Installations page.
- **Experience 1.2:**
  - The Tachyon Experience score has been greatly enhanced to include User Sentiment - this means that, not only can you monitor the stability, responsiveness, and performance of the devices on your network to deduce your end-users satisfaction with their IT services, you can send out surveys and incorporate your end-users actual feedback directly into the picture.
    - The Tachyon Experience score displayed on the Overview page includes user sentiment values, please refer to The Scores for more information.
    - The Categories page includes a Sentiment tile showing the current User Sentiment score.
    - The Sentiment page lets you view the User Sentiment score on its own and drill down to view users and monitor their feedback and pain points.
  - End-User Surveys - two types of survey are supported: User Sentiment and General Purpose. User Sentiment Surveys contribute towards the Tachyon Experience score, General Purpose Surveys can be used to ask one-off questions of your end-users and get their feedback on any issue. The Surveys page is where you can create, enable and deploy surveys.
  - A Users page is provided that lets you get information on the end-users on the devices in your network.
  - Customize the Tachyon Experience pages to view the interactive charts you want to focus on - including the display of the results from your User Sentiment surveys on the Sentiment page.

- **Explorer 5.1:**
  - No changes
- **Guaranteed State 1.4:**
  - The workflow on the rule creation page has been improved, so that all the information you need to enter is presented on a single page, making it easier to create rules.
  - Support for digital signing, versioning and licensing of Guaranteed State policy fragments. This requires that upgrading to Tachyon 5.1 has a new license.
- **Patch Success 1.2.104:**
  - No changes to this application for this maintenance release.

1.11.13.1.3.4.4 Product Packs for v5.1

- **Classic Product Packs:**
  - 1E-ConfigMgrConsoleExtensions.zip (minor changes)
  - 1E-Explorer-TachyonAgent.zip (minor changes, new 1E-Explorer-TachyonAgent-Set1EClientAgentConfig)
  - 1E-Explorer-TachyonCore.zip (minor changes)
  - 1E-Inventory.zip (1E-Inventory-Device-GetProcessors improved, 1E-PatchSuccess-PatchStatus now only runs on Windows)
  - 1E-Patch-Success.zip (minor changes)
  - 1E-Tachyon-Platform.zip (minor changes).
- **Integrated Product Packs:**
  - All fragments are now signed, and have InstructionType defined
  - MEMCM Client Health Integrated Product Pack - (**new** improved replacement for *Microsoft SCCM Client Health Integrated Product Pack)*
  - Microsoft SCCM Client Health Integrated Product Pack

    (**removed**)
  - NomadClientHealth.zip (minor changes)
  - TachyonCore.zip (minor changes)
  - WindowsClientHealth.zip (minor changes).
- Other Product Packs are available from the Tachyon Exchange: tachyonexchange.1e.com

1.11.13.1.3.4.5 Enhancements for v5.1

1.11.13.1.3.4.5.1 Hotfixes rolled up into this release - Server:

- Q21118 - Tachyon Clients machines unable to receive instructions (TFS 209695)

- Q21100 - Platform - Coordinator - Delay in sending email causing approval to fail (TFS 198224)
- Q21098 - Platform - Tachyon Instructions - Approvals taking multiple times to get approved whilst email addresses are being resolved (TFS 201850)
- Q21058 - UI - Explorer - Schedule instruction scheduler presents unclear time setting for non UTC sites. (TFS 203430)
- Q21056 - Platform - Tachyon does not resolve group membership correctly (TFS 201849)
- Q21054 - Platform - AD group membership update causes time out in Tachyon portal (TFS 203074)
- Q21052 - Platform - Tachyon unable to perform scheduled sync (TFS 204203)
- Q20994 - Platform - Experience - Tachyon Platform installed against SQL Server Evaluation edition fails to support partitioning (TFS 200801)
- Q20992 - Platform - Configurable authentication dialog before sending action in Explorer (TFS 195947)
- Q20990 - Platform - Experience - UDP Send time, Disk Random AccessTime, Disk Sequential Access time and Registry Write HKLM values are being scored as 0 (TFS 200770)
- Q20988 - UI - Experience - Devices screen needs to report more digits for experience values (TFS 199506)
- Q20986 - Platform - Coordinator is not loading the entire license upon flat license request (TFS 199897)
- Q20984 - Platform - Experience - Memory Hard page faults - scoring is wrong (TFS 199843)

1.11.13.1.3.4.5.2 Hotfixes rolled up into this release - SLA:

- Q21108 - Views have been introduced to view inventory data under 'SLA-Data'database (TFS 208158)
- Q21106 - Mapping between Product and a SCCM package/application didn't persist after clean sync/clear (TFS 210042)
- Q21104 - Tachyon connector sync should not delete the sync schedule if sync fails and retry again in next sync. (TFS 204587)
- Q21102 - Performance improvements in clean sync and clear data actions. (TFS 210045)
- Q21090 - SLA - Management group evaluation and ETL cube processing fail with Arithmetic Overflow error (TFS 206524)
- Q20924 - Clear Data action was clearing the data from SLA Reports (TFS 198458)
- Q20922 - Reclaim API changes to support multiple command lines (TFS 199059)
- Q20920 - Support Disabling Remote Access option in Product (TFS 190817)
- Q20918 - No option was present in Tachyon connector to separate the actions for "Consolidation Reports" from the "Sync Data" action. (TFS 198649)
- Q20916 - Products with special character like "uTorrent" were not getting normalized with Catalog even though match rules existed. (TFS 197516)
- Q20914 - Data disappears on sorting on Product to CM Association Tab (TFS 197878)

- Q20912 - The number of devices in Patch Success was reset and had to repopulate (TFS 194114)
- Q20910 - The new OU Path in Management Group rules is not working correctly with contains (TFS 197293)

1.11.13.1.3.4.5.3 Hotfixes rolled up into this release - 1E Catalog:

- Added "Not Remove" and "Not Patch" condition for SetfolderPermission custom action to support catalog hotfix (TFS 208305)
- Sync is failing in case only TLS 1.2 is enabled on client (TFS 206213)
- Creation of entitlements in AppClarity resulted in merged entitlements for different release of windows server for example, Windows 2019 and 2016 (TFS -204034)
- Deletion of records in case of Incremental Sync from Prediction Results (TFS 203575)
- Performance improvement in AI Engine (TFS 201562)
- XML Wrapper SP for SurrogateKey Feature (TFS 200529)
- Provided grant permission in stored procedure "EntitlementProductversionEditionExpensionMD5_se“ (TFS 200452)
- Handling of Unicode values for vendor in Devices and Processors stored procedures (TFS 199898)

1.11.13.1.3.4.5.4 Hotfixes rolled up into this release - AppClarity:

- Q20962 - Incorrect license demand calculations for VM cluster in case of Oracle LDC (TFS 200689)
- Q20960 - Oracle installations not visible on compliance summary by title & ELP report when product installed on VMs and demand computed on physical clusters (TFS 198809)
- Q20958 - Software can be reclaimed from any device, and will not depend on Device Type anymore, in fact considers only Operating System of device (TFS 200632)
- Q20956 - After upgrade to v7.0, entitlement summary screen and/or license / maintenances screen displays null error (TFS 199952)
- Q20954 - After upgrade, on reclaim usage summary screen, Saving Opportunity graph is crashing due IsLicenseRequired null value error (TFS 199953)
- Q20952 - Multiple Uninstall command lines in a reclaim policy are not supported (TFS 199947)
- Q20950 - Reclaim policy cannot be Save draft/publish as disabled (TFS 199754)
- Q20948 - All software installations under 'License Exemption' management group not exempting from compliance (TFS 199980)
- Q20946 - Display changes for compliance details of LDC products (TFS 199954)

1.11.13.1.3.4.5.5 Hotfixes rolled up into this release - Application Migration:

<None>

1.11.13.1.3.4.5.6 Hotfixes rolled up into this release - Business Intelligence:

- Q21078 - Patch Success - 400 year old patch causes cube process failure

- Q21076 - ETL sync is taking an excessive amount of time to complete

1.11.13.1.3.5 Web Release-5.0 (18-MAR-2020)

1.11.13.1.3.5.1 Tachyon Server 5.0.0.592 - Tachyon Toolkit 5.0.0.592 - 1E Catalog 2.0.0.296 - Software Lifecycle Automation 5.0.0.20 - Business Intelligence 3.2.0.303 - ActiveEfficiency Server 1.10.100.10

1.11.13.1.3.5.2 Platform v5.0

- **Tachyon:**
  - Switch now supports Windows Certificate Store (instead of Switch certificate files)
  - Eventing mechanism allows propagation of live events in real-time from 1E Client to consumers
- **SLA:**
  - Support for Microsoft System Center Configuration Manager CB1910 and Microsoft SQL Server 2019
- **1E Catalog:**
  - Hotfix capability
  - Support for EXE file mapping to multiple products
  - Surrogate keys - used in tracking changes to 1E Catalog - allows for example, details of the original vendor to be retained when a product is acquired by a new vendor
  - Catalog UI should set the "Customer" as submission source instead of "1E" for customer curated data
  - UNSPSC Software Category must be available to user in human-readable format on the SLA UI
  - Changes to support "Latest Version" field in SLA - Extra column will be returned during SLA normalization with Catalog
  - AI Auto-curated entries are not deleted after a sync/resync/upgrade
  - Installer enhancements:
    - AI model file download switch (Installer and DB setting); default off
    - Catalog installer changes to support TLS 1.2 using ADO.NET SQLClient
    - Support for Network Service account
    - Remove sysadmin requirement in installation
    - Custom user entries in Web.config file need to be parsed and added back to the new config file during Catalog upgrade
- **Settings application:**
  - Permissions->Add User search has changed from search-as-you-type to search on demand. This can be done against Users or Groups or Both, by clicking search icon available

  - Provider Configuration->New option called "Test" has been added which is only enabled when SCCM Connector exists. Otherwise the option is disabled, even for Provider Configuration Administrator and Global Administrator. Required for AppMigration/AppClarity

- **Inventory application (new in v5.0):**
  - AI Powered Auto-curation
  - Software Inventory, including aggregation
  - Hardware Inventory, including summaries for devices and virtual hosts
  - Manage associations between inventoried products and Configuration Manager applications and packages
- **Tachyon Setup:**
  - When upgrading from SLA Platform 3.3 its SLA users are migrated to become Tachyon users with no roles assigned
  - Network Service is used for the 1E Catalog Update Service instead of a domain account
  - "Business Intelligence" option to allow independent installation of BI
  - Maintenance page provides Server Certificate option to update certificate bindings, that also provides better troubleshooting experience
  - Installation of new Experience application
  - Option to enable the AI Powered Auto-curation feature
  - Extends db_ddladmin permission on Tachyon Master database, in addition to existing db_datareader and db_datawriter
  - Supports backup of all installed components and their respective databases during upgrade
  - Clickable link to download missing pre-requisite Visual C++ 2013 redistributable
  - The 'License File' step now occurs before "Select components" to validate the allowed components/features in license file

1.11.13.1.3.5.3 Consumer applications for v5.0

- **AppClarity 7.0**(available separately from the 1E Support Portal, not included in Tachyon Setup)
- **Application Migration 3.0**(available separately from the 1E Support Portal, not included in Tachyon Setup)
- **Experience 1.0 (new application in v5.0)**
- **Explorer 5.0:**
  - The Response page has a new option to show raw data when an aggregated instruction is asked
- **Guaranteed State 1.3:**

- Overview dashboard has been rearranged as a result of field feedback
- The term "Policy" has been removed from all the tiles on Overview dashboard
- The Rule type filter does not contain "Event" any longer. Only Check and Fix types are supported
- Cosmetic casing changes - View History now reads "View history" and View Details" now reads "View details"
- The dashboard header statistics have been improved
- Guaranteed State now supports table partitioning (SQL Server feature for better performance)

· **Patch Success 1.2:**

- The Patch and Device details screens now allow Updating of all devices and patches for a given patch or a device respectively
- Performance improvements

1.11.13.1.3.5.4 Product Packs for v5.0

· Product Packs listed below are now included in the Tachyon Platform zip, previously they were in a separate Tachyon Product Packs zip

· Tachyon.ProductPackDeploymentTool.exe
(tool relocated from the Integrated folder to the root folder, so it can be used to upload Classic and Integrated packs, and be started by Tachyon Setup)

· **Classic Product Packs:**

- 1E-ConfigMgrConsoleExtensions.zip (minor changes to instructions)
- 1E-Explorer-TachyonAgent.zip (minor changes to instructions plus **new instructions for location**)
- 1E-Explorer-TachyonCore.zip (minor changes to instructions plus **new instructions for firewalls**)
- 1E-Inventory.zip (**new, renamed from 1E-Inventory-ProductPacks.zip previously included in the SLA installer**)
- 1E-Patch-Success.zip (**updated instructions and renamed zip**)
- 1E-Tachyon-Platform.zip (**renamed zip**)

· **Integrated Product Packs:**

- MSSCCMClientHealth.zip (**1 new rule**)
- NomadClientHealth.zip (minor changes)
- TachyonCore.zip (minor changes)
- WindowsClientHealth.zip (minor changes)

- EndpointPerformance.zip

  (**removed**)

- Other Product Packs are available from the Tachyon Exchange: tachyonexchange.1e.com

1.11.13.1.3.5.5 Enhancements for v5.0

1.11.13.1.3.5.5.1 Hotfixes rolled up into this release - Server:

- Q20709 - Platform - Unable to Stop Tachyon Actions/Questions (TFS 189888)
- Q20652 - Platform - Switch is discarding the policy status message from 1E client if it receives both policy and instruction response from same device on same worker thread (TFS 189178)
- Q20642 - Platform - GS- Overview dashboard is not reflecting the Device and policy rule status change correctly (TFS 188870)
- Q20640 - Platform - Server - Multiseries response visualization has wrong count (TFS 187380)
- Q20638 - Platform - Tachyon Coordinator Service fails to start up successfully (TFS 187750)
- Q20578 - Platform - Management group sync is failing when a MG assigned to Guaranteed state policy is deleted (TFS 184629)
- Q20576 - Platform - Implement solution for switch certificate without device FQDN (TFS 184623)
- Q20552 - Platform - Instruction sent to all devices when Switch fails to download list of targeted devices from Core (TFS 182945)
- Q20550 - Platform - Policy Caching issue on status changes (TFS 178541)
- Q20548 - Platform - GS Policies report displaying compliant devices as unknown incorrectly (TFS 180742)
- Q20546 - Platform - GS - Broken filtering on Policy and rule reports (TFS 180313)
- Q20544 - Platform - Core discards policy-catchups with exceed max length (TFS 182324)
- Q20542 - Platform - GS - Remediations report (and maybe elsewhere) not returning data when orphaned policy data exists (TFS 182338)
- Q20540 - Platform - Cannot deploy an empty policy (TFS 182235)

1.11.13.1.3.5.5.2 Hotfixes rolled up into this release - SLA:

- Q20713 - Generate Report - ETL is taking too long (TFS 192684)
- Q20703 - The Clean Sync box, in the Schedules UI, is showing the opposite setting to the actual setting in the database (TFS 189942)
- Q20701 - Software Reclaim shows Unreported for most of the products (TFS 185935)
- Q20699 - Patch Success does not show all the available Inventory repositories in the dashboards (TFS 190699)
- Q20697 - Consumer installation fails for remote SQL Server and named instance (TFS 175916)

- Q20604 - Web - ETL performance at scale (TFS 180087)
- Q20602 - Patch Success Dashboard is not showing all Endpoint Patch data (TFS 180018)

1.11.13.1.3.5.5.3 Hotfixes rolled up into this release - 1E Catalog:

- Catalog UI: While editing processor match rule only Source Family, Source Model and Source Name field (TFS 182917)
- Catalog Sync/Resync: For fresh Installation there is Error in recreating indexes after Sync (TFS 182597)
- WebUI- Data curated by the client have the submission source = 1E instead of the customer (TFS 178528)
- Site defined records are not getting processed, if they are in the queue table of Staging database (TFS 169408)
- ENABLETLS12=0 shows check marked in installer (TFS 156106)
- Catalog Installer Preference for site defined vendor alias in case duplicate vendor alias exist in catalog (TFS 155362)
- Resync fails to insert site defined [EntitlementProductProductMatchs] (TFS 154327)
- DROPOLDDB=0 enables the Drop old database option in the Database Server installer screen (TFS 154299)
- Resync fails to insert site defined [EntitlementProductSet] (TFS 154193)

1.11.13.1.3.6 Web Release-4.1 (24-JUN-2019)

1.11.13.1.3.6.1 Tachyon Server 4.1.0.169 - Tachyon Toolkit 4.1.0.169 - 1E Catalog 1.2.0.303 - Software Lifecycle Automation 4.1.0.47 - Business Intelligence 3.1.0.51 - ActiveEfficiency Server 1.10.0.62

1.11.13.1.3.6.2 Platform v4.1

- **Tachyon Setup has been expanded to include ActiveEfficiency Server:** this is in order to support the Nomad Dashboard and Nomad download pause features.
- Tachyon Setup has also been extended with the following features:
  - Uninstallation, and also inclusion of MSPs at install-time
  - Re(registration) of applications from Maintenance page
  - Consumer-level workflow override (e.g. for ServiceNow integration)
  - Support for partial upgrades
  - Ability to run Tachyon Product Pack Deployment Tool to upload Product Packs
- Tachyon toolkit consumers are registered automatically during installation
- Improvement on Action processing
- Improvements to Explorer:

  - A new **Instruction Detail** dialog has been added to the **Instruction History** page that shows information on the selected instruction
  - Improvements have been made to the **Device Detail** dialog on the **Devices** page
- Improvements to Guaranteed State
  - The **Rule Status** tile and corresponding drill-downs have been improved
  - Rule editing is now supported
  - A **Device Detail** dialog has been added
  - A **Remediation** report is now available that shows what remediations have been applied
  - The dashboard header statistics have been improved
  - Performance improvements
- Improvements to Patch Success:
  - The **Patch performance** dashboard tile can now be used to interactively filter the page
  - A new **Monitoring** menu has been added that displays the history and responses for the Patch Success instructions
  - Performance improvements
- Support has been confirmed for:
  - Microsoft System Center Configuration Manager CB1902

1.11.13.1.3.6.3 Product Packs for v4.1

- **Classic Product Packs (updated for 4.1):**
  - 1E-ConfigMgrConsoleExtensions.zip
  - 1E-Explorer-TachyonAgent.zip
  - 1E-Explorer-TachyonCore.zip
  - 1E-PatchSuccess.zip
  - 1E-TachyonPlatform.zip
- **Integrated Product Packs (new for 4.1):**
  - EndpointPerformance.zip
  - MSSCCMClientHealth.zip
  - NomadClientHealth.zip
  - TachyonCore.zip
  - WindowsClientHealth.zip

- Tachyon.ProductPackDeploymentTool.exe (new)
- Other Product Packs are available from the Tachyon Exchange: tachyonexchange.1e.com

1.11.13.1.3.6.4 Enhancements for v4.1

1.11.13.1.3.6.4.1 Hotfixes rolled up into this release - Server:

- Q20520 - Platform - Instruction sent to all devices when Switch fails to download list of targeted devices from Core (TFS 182945)
- Q20486 - Tachyon Guaranteed State dashboard is reporting the device compliance status incorrectly as “unknown”. (TFS 176304)
- Q20484 - Tachyon Switch failing to honour the log roll over setting (TFS 178311)
- Q20470 - 1E Tachyon Switch Host service fails to start after upgrading to Tachyon server 4.0 (TFS 175839)

1.11.13.1.4 Tachyon Platform features by release

A list of features of the Tachyon platform and features organized by the release they were implemented in. Links through to the features have been provided for convenience.

1.11.13.1.4.1New features in Tachyon 8.1

1.11.13.1.4.2Tachyon Platform 8.0

1.11.13.1.4.3Tachyon 5.2

1.11.13.1.4.4Tachyon 5.1

1.11.13.1.4.5Tachyon 5.0

1.11.13.1.4.6Tachyon 4.1

1.11.13.2 Tachyon Platform zip

The Tachyon Platform zip file can be downloaded from the 1E Support Portal https://support.1e.com/. Extracting the zip will create a folder structure containing the following, where the files highlighted in bold are required by Tachyon Setup.

- Licenses.txt
- Tachyon Release Information.html
- **Tachyon.Setup.exe**

Please refer to:

- Tachyon Setup, for detailed information about each screen in Tachyon Setup
- Quick Start if you want a brief overview of installing Tachyon.

Warning

Tachyon Setup is the only supported method of installing, upgrading, and patching a Tachyon server.

Installation using standalone **msi** or **msp** files is not supported unless advised by 1E, which may be necessary in complex installations, using non-interactive (quiet/silent) command-lines, and may require further post-install configuration steps.

- Installers**1ECatalog.msi**
- Installers**AppClarity.msi**
- Installers**ApplicationMigration.msi**
- Installers**ContentDistribution.msi**
- Installers**SLA.BI.Installer.msi**
- Installers**SLA.Platform.Installer.msi**
- Installers**TachyonServer.msi**
- Installers\TachyonToolkit.msi

This folder contains **msi installer files** for Tachyon components and applications that will be installed by Tachyon Setup if their prerequisites are met.

- Installers\Apps\Experience**Experience.zip**
- Installers\Apps\Experience**metadata.json**
- Installers\Apps\Explorer**Explorer.zip**
- Installers\Apps\Explorer**metadata.json**
- Installers\Apps\GuaranteedState**GuaranteedState.zip**
- Installers\Apps\GuaranteedState**metadata.json**
- Installers\Apps\Inventory**Inventory.zip**

This folder contains **apps folders** for Tachyon consumer applications that will be installed by Tachyon Setup if their prerequisites are met.

If you do not want to install a Tachyon consumer application, then delete the folder before running Tachyon Setup.

Later, if you need to install the Tachyon consumer application, then you can reinstate the folder and install the app using Tachyon Setup as described in Applications maintenance.

Note

Some consumer applications are installed using their msi instead of an apps folder, for example AppClarity and Application Migration.

- Installers\Apps\Inventory**metadata.json**
- Installers\Apps\Nomad**metadata.json**
- Installers\Apps\Nomad**Nomad.zip**
- Installers\Apps\PatchSuccess**metadata.json**
- Installers\Apps\PatchSuccess**PatchSuccess.zip**
- Installers\Apps\Settings**metadata.json**
- Installers\Apps\Settings**Platform.zip**
- ProductPacks\Newtonsoft.Json.dll
- ProductPacks\Tachyon.ProductPackDeploymentTool.exe
- ProductPacks\Tachyon.ProductPackDeploymentTool.exe.config
- ProductPacks\Tachyon.SDK.Consumer.dll
- ProductPacks\Classic\1E-ConfigMgrConsoleExtensions.zip
- ProductPacks\Classic\1E-Experience.zip
- ProductPacks\Classic\1E-Explorer-TachyonAgent.zip
- ProductPacks\Classic\1E-Explorer-TachyonCore.zip
- ProductPacks\Classic\1E-Inventory.zip
- ProductPacks\Classic\1E-Nomad.zip
- ProductPacks\Classic\1E-Patch-Success.zip

These Product Packs are required to support various Tachyon features, for more detail please refer to Tachyon Product Packs reference.If your license permits, you can use additional Product Packs available from Tachyon Exchange 1E Exchange to meet specific use-cases.

Classic Product Packs	Contain instructions, for use in Explorer and other Tachyon applications. They can be uploaded using the **Tachyon Product Pack deployment tool**, or using **Settings→Instructions→Instruction sets** page in the Tachyon Portal.
Integrated Product Packs	Contain policies, rules and fragments for use by Guaranteed State, and may also include instructions. They can only be uploaded using the

- ProductPacks\Classic\1E-Tachyon-Platform.zip
- ProductPacks\Integrated\MEMCMClientHealth.zip
- ProductPacks\Integrated\NomadClientHealth.zip
- ProductPacks\Integrated\TachyonCore.zip
- ProductPacks\Integrated\WindowsClientHealth.zip

Tachyon Product Pack deployment tool.

Tip

The **Tachyon Product Pack Deployment Tool** can be started independently, or at the end of the **Tachyon Setup** process via the Uploading with the Tachyon Product Pack Deployment Tool screen, where the screen contains a link that launches the tool. The **Tachyon Setup** method of starting the tool is recommended because setup ensures you have the correct permissions to upload the Product Packs.

1.11.14 Glossary

A glossary of Tachyon terminology.

1.11.14.1 Tachyon alphabetical glossary

Term	Definition
1E Client	1E Client provides client features and modules for 1E products including Tachyon. It replaces the Tachyon Agent.
Action	An Action is a specific type of instruction that is sent to client devices which can be used to modify the state of the target device. For example, setting a registry key, killing a process, deleting a file. Whereas a Question is an instruction that requests information from the target device, but does not change its state. Generally an Action needs to undergo an approval process before it is sent.
Agent	Agent is the old name for the client. The Agent has been replaced by the 1E Client which provides client features and modules for 1E products including Tachyon.
All Instructions Approver	This is a Tachyon system role which allows assigned users to approve actions for all Instruction Sets . Users can approve unless the action was requested by themselves.

Term	Definition
All Instructions Questioner	This is a Tachyon system role which allows assigned users to ask questions and view responses for all Instruction Sets; use custom properties.
All Instructions Viewer	This is a Tachyon system role which allows assigned users to view instructions and responses for all Instruction Sets.
Audit information log	The Audit information log page displays audit information related to installation, permissions, instruction set and consumer related operations carried out using the Explorer and Settings applications. See Audit information log page
Historic Data Capture	The old name for Tachyon Activity Record.
Agent Language	The Agent language is an interpretive programming language that is executed by the client in the form of an **instruction payload**. Instructions, and their payload, are based on instruction definitions which are stored in the TachyonMaster database. Definitions are uploaded into the database from the Administrator console by dragging and dropping one or more Instruction Definition files, a Product Pack or ZIP file containing Instruction Definition files. The language, called SCALE, uses Agent modules and methods and is documented in the SDK.
Agent Provider	A plug-in component for the 1E Client which communicates with an external component, such as an operating system facility (for example Windows registry) or a service-provider application (for example Content Distribution). 1E Client modules use Providers to get their work done. Examples: • WMI provider • Registry provider • Nomad provider • BASH provider

Term	Definition
Auto-curation	Auto-curation is a Catalog function and refers to the automated process of creating match rules in 1E Catalog. These match rules are neither created by the customer not by the 1E curation team. The rules are created in the customer's local 1E Catalog copy using automated logic built by 1E.
Background Channel	The Background Channel is a mechanism by which the Tachyon client can download resources via HTTPS without loading the Switch. Since this traffic does not go through the Switch, the client is still able to receive and process instructions instructions while performing these downloads. From v2.0 onwards, the client is able to download resources via Content Distribution. The Background Channel is a web application on the Tachyon Server Website and provides the following: • Stores Tachyon content from the Consumer API in the Background Channel for clients to retrieve • Responds to clients retrieving Tachyon content from the Background Channel See Tachyon Architecture and Communication Ports.
Client module	A plug-in component for the 1E Client which encapsulates business logic. Modules contain Methods, which can be invoked by SCALE. Modules (and their methods) effectively provide a platform independent API. To that end, Modules and their Methods do not (generally) talk about anything platform specific (Windows, Linux, Android etc). Examples: • FileSystem • OperatingSystem • Network • Software
Column filters	Some tables contain a column filter that lets you easily filter the information displayed in the table.**Using column filters**The picture opposite shows an example taken from AppClarity. In our example we

Term	Definition
	want to filter the table to show only those items where the **Edition** contains the text **Prof**.To filter the table on the **Edition** column:Click on the filter iconjust beneath the header row in the **Edition** column.The filter popup is displayed.Now select the operator. In our example this will be **contains**.Then type the text **Prof** into the text field.Click **Apply** and a new filter will be added to the table.The table will be filtered to just those items whose **Edition** contains the text **Prof**.**Adding another filter**You can add another filter by clicking on the filter icon for any of the columns. The picture opposite shows another filter added selecting table rows where the **Type** also contains the text **License**. The table will also be filtered accordingly.**Removing filters**You can remove filters by clicking on the filter close icon at the end of the filter.
Column Picker	**Using column picker**Where the column picker control is shown you can choose which columns are displayed. In the following example on the **Microsoft Core License Demand** page we hide the **Unknown Installs** column and move the **License Demand** column to the left of the page.To pick the displayed columns:Click on the Choose columns iconto the right of the header row to view the visible columns.To exclude **Unknown Installs**, select the Unknown Installs row and click **Exclude columns** button.The **Unknown Installs** column is now hidden.To move the **License Demand** column to the top of the list, hover your mouse over **License Demand** and using the direction control drag it to the top of the list.The Microsoft Core License Demand page has now been automatically updated with our changes.
Column sorts	Some tables contain column sorts that let you easily re-order the information displayed in the table.**Using column sorts**The picture opposite shows an example taken from AppClarity. In our example we want to sort the table on the **Cost** column from the highest cost at the top to the lowest at the bottom. To sort the table on the **Cost** column:Click on the sort iconjust beneath the header row in the **Cost** column.The sort popup is displayed.Now select the sort direction. In our example this will be **Sort descending**.After selecting this the data in the table is now sorted on the **Cost** column from highest to lowest and the sort icon has changed to a sort descending icon**Clearing the sort**You can clear the sort by clicking on the sort icon again and selecting the **Clear sorting** menu item from the sorting popup.
Configuration Manager Extensions	The Configuration Manager Extensions currently include.

Term	Definition
	• Configuration Manager Agent emergency stop and resume actions • Configuration Manager Agent actions • Client Health Check • Tachyon Run Instruction utility (used by the each of the above right-click actions to request Tachyon to run an instruction) • Tachyon Instruction Runner (a mini UI version of the Tachyon Explorer) This feature is included in the Tachyon Toolkit. Documentation for installing and using the Configuration Manager Extensions will be available soon.
Consumer	A Consumer is any application that connects to and uses the Consumer API. An example is the Explorer application.
Consumer API	The Consumer API is a documented set of API endpoints provided by a web application on the Tachyon Web Server called Consumer. It is referred to as the Consumer API in order to avoid confusion with Tachyon Consumers, which are 'consumers' of the API. The Consumer API is a web application on the Tachyon Server Website, actually named Consumer, and provides the following: • Processes the consumer requests from the Explorer and other Consumers • Publishes Tachyon content to the Background Channel • Forwards requests for instrumentation data from the Explorer to the Tachyon Instrumentation component • Forwards workflow commands from the Explorer to the Tachyon Workflow component See Tachyon Architecture and Communication Ports.
Consumer requests	A Consumer sends requests to the Consumer API.
Coordinator Service	The Coordinator Service has two modules:

Term	Definition
	• Instrumentation module • Workflow module See Tachyon Architecture and Communication Ports.
Coordinator Instrumentation module	The Coordinator Instrumentation module is part of the Coordinator Service on the Tachyon Server which processes instrumentation data from the following components: • Core • Coordinator Workflow module • Switch And responds to requests for instrumentation data from the Consumer API. See Tachyon Architecture and Communication Ports.
Coordinator Workflow module	The Coordinator Workflow module is part of the Coordinator Service on the Tachyon Server that provides the following: • Forwards workflow commands from the Consumer API to the Core • Stores workflow in SQL • Connects to remote SMTP to send emails used in the approval process for actions See Tachyon Architecture and Communication Ports.
Core	The Core is a Tachyon Server web component that does the following: • Forwards workflow commands from the Coordinator workflow module to the Switch • Forwards responses from the Switch to the Responses database (this task requires high throughput) • Generates and sends instrumentation data to the Instrumentation service See Tachyon Architecture and Communication Ports.

Term	Definition
Core Internal	Core Internal is the part of the Core which allows fast internal communication with the Switch using HTTP instead of HTTPS, restricted to the Switch server's local IP Address only. See Tachyon Architecture and Communication Ports.
Custom Role	Tachyon roles that define which Users have access to which Instruction Set. These roles can be modified in the Administration pages by users assigned to the Full Administrator role.
Custom Properties	Full Administrator can manage the custom properties using the Properties page in Explorer. The only custom property type available after installing the Tachyon server is Coverage tags, further types may be added during installation of other Consumers.
Device tags	Device tags can be used when setting the coverage for a particular question so that only client devices with a particular tag name and value get the question. The names and values of Device tags must be pre-configured by a Full Administrator before setting them on a client device using Device tag actions. Device tags can also be queried directly by Device tag questions. Device tags were previously known as Coverage tags. In 1E Client log files, Device tags are also referenced as scopable tags. Please also see Freeform tags.
DNS Name	DNS Name FQDN is the term used in this documentation to represent the name of a Tachyon Server. Typically a Tachyon Server will have only one DNS Name, which will be the CNAME or an (A) Host record that uniquely represents a server's IP Address. 1E normally recommends using an CNAME record. In a Tachyon system, each Tachyon Server will have a DNS Name FQDN. In a single-Switch installation the Switch is on the same server and uses the same DNS Name. When a Response Stack has more than one Switch, each Switch has its own IP Address, so you can choose if the will share

Term	Definition

	the same DNS Name, or if each will have its own DNS Name. The Tachyon Server certificate must have all
	
	`NAME TYPE VALUE`
	`----------`
	`tachyon.acme.com. CNAME tachyon.acme.local.`
	`tachyon.acme.local. CNAME foo.example.com.`
	`foo.example.com. A 192.0.2.23`
	
	`tachyon.acme.com is an Alias record`
	
	`tachyon.acme.local is a CNAME record`
	
	`foo.example.com is a (A) Host record`

Event Subscription	A type of instruction that can be sent to the client. An Event Subscription tells the client to monitor an arbitrary event source for a period of time (defined by the Instruction's TTL), to capture events as they occur and to report them back via the Switch.
Guaranteed State application	The Explorer application is the web portal used by users and administrators. It is an example of a Consumer application. **Note** Explorer can be reached directly using the following URL: `https://<tachyon DNS Name FQDN>/Tachyon/App/#/explorer/` where <tachyon DNS Name FQDN> is the one set up during the preparation phase, as described under the heading DNS Names. It is a web application on the Tachyon Server Website and provides the following: • Browser connection providing the Explorer and Administration pages • Sends consumer requests to the Consumer API See Tachyon Architecture and Communication Ports.
Filters	There are two kinds of filter: Question filters are used to reduce the responses from the clients; View filters reduce the information displayed in Explorer on the Responses page.

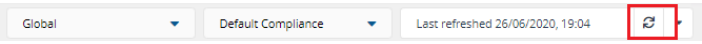
Term	Definition
Freeform tags	Freeform tags may be used to set properties on client devices that can subsequently be used in Freeform tag questions. They cannot be used when defining the coverage for a question. Freeform tags can be set with arbitrary names and values that are defined only when running a Freeform tag action. In Tachyon log files, Freeform tags are also known a non-scopable tags. Please also see Device tags.
FQDN	Fully Qualified Domain Name. This is the complete domain name for a specific IP-connected device, and is unique within the network and unambiguous. The FQDN consists of two parts: the hostname and the domain name. For example tachyon.acme.com.
Full Administrator	This is a Tachyon system role which has the combined rights of all the other system roles.
Group Administrator	This is a Tachyon system role which allows assigned users to create, modify and delete Management groups and modify their membership.
Guaranteed State application	Guaranteed State application is used to ensure endpoint compliance to enterprise IT policies. It is an example of a Consumer application. **Note** Guaranteed State can be reached directly using the following URL: `https://<tachyon DNS Name FQDN>/Tachyon/App/#/guaranteedstate/` where <tachyon DNS Name FQDN> is the one set up during the preparation phase, as described in DNS Names.
Instruction	Instruction is the generic term used to describe: • Questions • Actions An Instruction is sent to one or more clients, and will yield one or more responses.

Term	Definition
Instruction Definitions	Instruction Definitions are retrieved from the Core by the Switch. They define the type and functionality of the instructions and are used to control the clients to respond in the appropriate way.
Instruction Definition Files	Instruction Definition files are XML format files that contain definitions for Instructions and any associated resources.
Instruction Sets	Instruction Sets provide a way of organizing instructions and setting permissions on those instructions. They can be created, modified and deleted from the Tachyon Administration console.
Instrumentation data	Each of the Tachyon components creates instrumentation data that can be used to display how the Tachyon system is performing.
JSON Provider	This is an internal provider within the Tachyon agent library, used to deserialize and return a JSON string as a data table. Analogous to the Windows specific PowerShell Provider.
Legacy OS	In this documentation, Windows XP, Vista and Windows Server 2003 are referred to as legacy OS. Microsoft has withdrawn support for Windows XP and Windows Server 2003, but 1E includes Vista in this list because it is not significantly used by business organizations. For details of limitations and additional considerations for these OS, please see Supported Platforms.
License file	1E will provide you with a **Tachyon.lic** license file that defines the applications, tools, and features your Tachyon System is able to use, for how long, and how many devices it supports, this may be an evaluation or subscription license. • The license must be activated. Once activated, it may be used only by the Tachyon System that activated it. • Licenses can be renewed or updated, but if allowed to expire, then the affected products or features will not be usable. • For a new installation, the Tachyon Setup program will let you select the license file from any folder on disk.

Term	Definition
	• For an existing installation, the license file is copied into the folder: %PROGRAMDATA%\1E\Licensing on your Tachyon Server. Ensure the following URL is whitelisted: • https://license-v1.1e.com This URL must be accessible from the Tachyon Server during setup and running of Tachyon. The Tachyon license must be validated on a regular basis via internet contact with the 1E license service. The regular validation period is set when the license is requested. For whitelisting purposes, the Tachyon Server (specifically the Coordinator Workflow module in the Master Stack) requires an Internet connection to the 1E license service, as defined in the license file itself. If activation fails, then the system will install but not be usable until activation is completed. **Upgrading** When upgrading, you are recommended to get a new license file and update your whitelist with the new URL. The old URL (https://license.1e.com) is suitable only for 8.0 and earlier. However, if you are upgrading and your license file has the old URL then you should also whitelist the old URL.
License Service	The License Service is hosted in the cloud by 1E, and accessible via an internet connection.
Method	Methods are documented in the SDK.
Normalization	Normalization is a Platform function that refers to the process of finding (or not finding) a match rule in 1E Catalog, then deduplicating and rationalizing the information using Platform logic, and publishing the information on the 1E Catalog UI. Partial Matching for example does not have a match rule in 1E Catalog but it's still normalized and published on the UI using Platform logic.
Patch Success application	Patch Success application is used to report on and ensure successful patching of your enterprise. **Note**

Term	Definition
	Patch Success can be reached directly using the following URL: `https://<tachyon DNS Name FQDN>/Tachyon/App/#/patchsuccess/` where <tachyon DNS Name FQDN> is the one set up during the preparation phase, as described under the heading DNS Names
Permissions	How the Role-Based Access Control feature assigns Users to Roles, providing access to Instruction Sets and Administration pages.
Persistent Storage	The client stores information in Persistent Storage which it needs each time it starts. For example the last processed instruction. A hash value of each item of information is stored in the registry, which the client uses to ensure it trusts each item. Persistent storage includes a local database that is compressed and encrypted in a way that ensures a very low impact on device performance and security. This database is used to store data for the Tachyon Activity Record feature.
PowerShell Provider	This is a Windows specific internal provider within the Tachyon agent library. It provides functionality to execute powershell.exe from a fixed location (System32\WindowsPowerShell\v1.0) on a PowerShell (.sp1) script and return the result. Some earlier versions of Windows (such as Windows XP) do not support PowerShell.
Product Pack	Product Packs contain instructions or other things which extend the capabilities of Tachyon. Product Packs which are required to support Tachyon features out-of-the-box are provided in the Tachyon Platform zip downloaded from the 1E Support Portal. Other Product Packs are available for download from the 1E Exchange. There are two types of Product Packs described in the following table. **Classic Product Packs** — Classic Product Packs contain instructions (actually Instruction Definition files) for use in Explorer and other Tachyon applications.

Term	Definition
	Classic Product Packs can be uploaded into Tachyon using either of the following methods: • Tachyon Product Pack Deployment Tool - which will upload the instructions in the pack and create an Instruction Set for them based on the name of the zip (with hyphens converted into spaces) • the Tachyon Portal Settings app→ Instructions → Instruction Sets, described in Instructions Menu. This method requires instructions to be organized into Instruction Sets by an Instruction Set Administrator. Settings can also be used to export instructions. Either method requires an Instruction Set Administrator to configure permissions for accessing the instructions.
Integrated Product Packs	Integrated Product Packs contain policies, rules and fragments for use by Guaranteed State, and may also include instructions. If the Integrated Product Pack contains instructions associated with the policies, the tool creates an Instruction Set using the name in its manifest file. Integrated Product Packs are uploaded using the PPDT.
Tachyon Product Pack Deployment Tool	A tool for uploading Classic and Integrated Product Packs. Please see Tachyon Product Pack Deployment Tool.
Providers	Providers can be used by applications to leverage external tools to perform specific operations. For example the reclaim provider enables

Term	Definition
	software to be uninstalled, thereby extending the functionality of the platform to include uninstallation.
Question	In Tachyon a Question is a specific type of instruction that requests information from client devices. The information is returned to Tachyon as responses.
Report Refresh	You can refresh reports from individual AppClarity screens as well as using the Settings App. Where this is available you can do this by using the refresh icon next to the **Last Refreshed** box: 
Response	The data resulting from a client executing an instruction.
Role-Based Access Control	Also known as RBAC. This is a general term for assigning users to roles which allow them access specific features of Tachyon. Roles can be assigned to AD users and groups added in the Administration Security page. A role can be either of the following: • System role • Custom role
SCALE	The Agent Language.
SDK	The Tachyon SDK describes the following and is available here: /document/preview/736743#UUID-33c212b3-863e-21bc-bc5d-52e41a0492b3 • Agent Language (SCALE) • Agent modules and methods
Securable	Refers to an item that may be secured by Tachyon using RBAC.
Server installation account	This is the account used to run Tachyon Setup (and the MSI installer) when installing or upgrading a Tachyon Server. The account is automatically defined as a Tachyon admin user with limited rights which cannot be edited (called a system principal). The installation account only has sufficient rights to add other users, assign them to roles, and install Tachyon applications. The users and roles created by the

Term	Definition
	installation account are then used for ongoing use and management of Tachyon. If you need the installation account to have additional roles or be a Full Administrator, then the recommended approach is: • First create a role-based AD Security group, and add the installation and other accounts to this group • Then, the installation account: – Logs into Tachyon and navigates to Settings → Permissions → Users and Groups – Creates a new user for the role-based AD Security Group – Assigns the relevant system role(s) to the new user - this can be Full Administrator. When installing a Tachyon Server, the account must be an Active Directory domain account with various rights on the Tachyon Server and the SQL Server instance. For more detail see Tachyon Server Installation Account. For a new installation, only the Server installation account is able to use the Explorer and assign user rights to other users and groups. Once these other users or groups have been assigned, then the Server installation account can be optionally disabled in AD pending future updates and upgrades. The Server installation account is a system principal and cannot be deleted or granted additional rights; it is able to manage additional users and groups, create and edit custom roles, which are then used for ongoing use and management of the system. However, the account may be included in any AD security group assigned to a Tachyon system or custom role.
Server instructions	A special type of instruction, which cannot be run in Explorer. They are for internal use only, run on the server, and used to carry out on-demand or scheduled processing of data across various datasources, such as SQL databases. For example, the Dashboards app uses them to populate tiles and charts with data from the TachyonMaster and Experience databases.

Term	Definition
	They are also called server-side instructions, to differentiate them from client-side instructions which run on client devices.
Settings application	Settings application is used to configure Tachyon system and application settings. It is an example of a Tachyon Consumer application. **Note** Settings can be reached directly using the following URL: `https://<tachyon DNS Name FQDN>/Tachyon/App/#/platform/` where <tachyon DNS Name FQDN> is the one set up during the preparation phase, as described under the heading DNS Names.
Single-Switch installation	A **single-Switch installation** is a type of single-server installation which has only one Switch. This is the simplest Tachyon Server configuration.
Single-server installation	A **single-server installation** is where all Tachyon Server components are installed on the same Web Server, with one to five Switches, and SQL Server either local or remote. A single-Switch installation is the simplest configuration. More than one Switch requires additional hardware resources. If SQL Server is remote then it is also referred to as a **split-server configuration**. Best performance is achieved using a local SQL Server installation. See Tachyon Architecture and Communication Ports.
SMTP gateway	Systems such as the Tachyon Server connect to the gateway in order to send emails. Also known as SMTP relay.
Switch	The Switch component on the Tachyon Server provides the following: • Sends instructions to and retrieves responses from the clients • Forwards responses to the Core component • Receives workflow commands from the Core component • Retrieves instruction definitions from the Core component • Sends instrumentation data to the Instrumentation component

Term	Definition
	On the Tachyon Server, the Switch Host service is responsible for managing all the local Switches The Switch configuration is stored in the SwitchConfiguration table of the TachyonMaster database. This includes the number of slots and workers used by the Switch which controls the maximum number of devices that can be managed by each Switch. A Switch restart will fail if the Switch failed to de-register itself, therefore the registration entry in the TachyonMaster database will need to be manually removed after troubleshooting. See Tachyon Architecture and Communication Ports.
Switch Host	The Switch Host service • is a Windows service that manages local Switches • automatically starts each Switch and if a Switch stops, the Switch Host analyses the reason and attempt to restart it • has a configuration file contains entries for one or more Switches • has its own log file See Tachyon Architecture and Communication Ports.
System Principal	A system principal is a Tachyon user which cannot be modified in the Administration pages, and is assigned to a system role. The Server installation account is a system principal which is assigned to the Consumer Administrator, Security Administrator and Instruction Set Administrator system roles.
System Role	Tachyon roles which cannot be modified in the Administration pages. Tachyon users can be assigned to these roles. For more information about System and Custom roles, please refer to Roles and Securables. The following are built-in system roles. • All Instructions Actioner • All Instructions Approver • All Instructions Questioner

Term	Definition
	• All Instructions Viewer • Full Administrator • Group Administrator • Guaranteed State Administrator • Guaranteed State Policy Assigner • Guaranteed State User • Installer • Inventory Administrator • Inventory User • Tachyon System
Tachyon Activity Record	This is a client feature, also known as inventory, previously known as Historic Data Capture. This feature captures data from a number of sources on the client device, encrypts and stores in compressed form on the client device. Raw and summarized (aggregated) data is stored and can be queried using instructions. See Tachyon client settings.
Tachyon client	Client features are provided by the 1E Client. The 1E Client includes client features and modules for other 1E products including Tachyon. Tachyon enables rapid response to instructions using the client, which supports the retrieval of information, running actions and device tagging. The client can also be extended to support additional features. The client connects to the Switch and the Background Channel. See Tachyon Architecture and Communication Ports.
Tachyon content	Tachyon content is: • files (such as scripts) associated with a particular instruction via their which the client will download when it performs that instruction.

Term	Definition
	• extensibles (normally in the form of DLLs on Windows), which the client will download when it self-updates. This allows additional client functionality to be deployed. Tachyon content is downloaded on demand via the Background Channel.
1E Exchange	The 1E Exchange is a community platform and library of automation modules (Product Packs) for systems management created by 1E. Our goal for this community is to democratize the development and optimization of automation processes to simplify work. Leveraging SCALE, Tachyon's native language, and the Tachyon Platform we wish to grow into a community that builds powerful modules to serve each other's needs. https://tachyonexchange.1e.com/ You can browse the 1E Exchange but you will need a 1E Support login to download.
Tachyon Instruction Management Studio (TIMS)	This feature is included in the Tachyon Toolkit. TIMS provides a user interface for developing and testing instructions using SCALE. It includes an isolated copy of the 1E Client so that you can develop instructions for that client version, independent of the 1E Client version that may be installed on your computer. By default TIMS and its Tachyon client run under the security context of the user that started it. To use the context of **Local System**, as used by a normal Tachyon client, you can start TIMS using PSexec. More information about TIMS is available in the Tachyon Community on the 1E Support Portal. TIMS should be used to edit and save Instruction Definition files.
Tachyon Instruction Runner	This feature is the graphical user interface part of the Configuration Manager Extensions which is included in the Tachyon Toolkit. It is a mini UI version of Explorer. It is an example of a Tachyon Consumer. It should not to be confused with the Tachyon Run Instruction utility available in the Tachyon Toolkit.

Term	Definition
TachyonMaster database	The SQL Server database which contains: • Configuration details of the Tachyon System • instruction definitions and Instruction Sets • Users (Principals) • Permissions • Roles • Devices • Audit log The configuration files for the following components contain SQL Connection strings for the TachyonMaster database. • Core • Coordinator Workflow module • Consumer API
Tachyon Master Stack	A Tachyon Master Stack is part of a Tachyon System. There is one Tachyon Master Stack that all the Tachyon Response Stacks communicate with. A Tachyon Master Stack contains the following components: • SQL Server instance with TachyonMaster Database (local or remote/split) • Consumer API • Coordinator • Explorer • Authentication • Registration
Tachyon Portal	The Tachyon Portal is the home page for Tachyon applications, which can be reached using the following URL: `https://<tachyon DNS Name FQDN>/Tachyon`

Term	Definition
	where <tachyon DNS Name FQDN> is the one set up during the preparation phase, as described under the heading DNS Names. The following buttons appear on all application pages of the Tachyon Portal. The refresh button is used to refresh the contents of the page. The expand button toggles the size of the page inside the browser by hiding or showing the menu and main title bar.
TachyonResponses database	The SQL Server database which contains: • Responses
Tachyon Response Stacks	A Response Stack is part of a Tachyon System. This is where one or more Response Stacks talk back to a single Tachyon Master Stack. Multiple Response Stacks are necessary when additional Switches are required for scale, security or for geographic or other network reasons. Each Switch can handle 50000 devices, so each Response Stack can handle a maximum of 250000 devices. Each Response Stack has the following components: • Switch Host • Switches (up to 5, local or remote/split) • Core • SQL Server instance with Tachyon Responses database (local or remote/split) • Background Channel A Response Stack will typically host Switches and Background Channel using the same DNS Alias.

Term	Definition
Tachyon Role	Tachyon roles are used to implement Role-base access control (RBAC) and assign permissions to users and restrict access to areas of Explorer and ability to use instructions in Instruction Sets .The roles may be system roles or custom roles related to specific Instruction Sets .
Tachyon Run Instruction utility	This command-line utility is included in the Tachyon Toolkit and is targeted at 3rd party integration, and can be used by scripts. It is an example of a Tachyon Consumer. It is used by the Configuration Manager Extensions which is also available in the Tachyon Toolkit. More information about the Tachyon Run Instruction utility is available in the Tachyon Community on the 1E Support Portal.
Tachyon Server	A Tachyon Server is any server on which a Tachyon Server component is installed. The following are Tachyon Server components. • Coordinator service (Instrumentation and Workflow modules) • Switch Host • Switches • Website (including Explorer and Core) A Tachyon Server can have one or more Switches. See also single-server installation and single-Switch installation. See Tachyon Architecture and Communication Ports.
Tachyon Stack	There are two types of Stack: Master Stack and Response Stack. Every Tachyon system has a single **Master Stack**, which provides web services for Tachyon applications. Master Stack components are typically all installed on a single **Master Server**. Tachyon real-time features require **Response Stacks**, which are made up of one or more **Response Servers**. A **DMZ Server** is an example of a Response Server. Each Response Stack has at least one **Background Channel** for sharing resources, and a single **Core** component that supports an associated set of up to five **Switches**. Switches are the primary mechanism for rapidly requesting and retrieving responses from the **clients**. As each Switch can handle up to

Term	Definition
	50,000 devices there is a limit of 250,000 devices per Response Stack. Higher numbers can be achieved if you contact 1E for guidance. Switches may be local or remote to the other components in the Response Stack. **Databases** for Tachyon, Catalog, Content Distribution, Experience, SLA and BI, are installed on SQL Server database instance(s) that may also be local or remote to their respective Master and Response servers. It is also possible for multiple Response Stacks to share the same Responses database. The **Cube** used by Patch Success (SLA-BI) is installed on a local or remote SQL Server Analysis Services (SSAS) instance. For more details about architecture and components, please see Tachyon Architecture. Also see Architectural requirements.
Tachyon System	At the top-most level, a Tachyon System consists of Tachyon Server components, grouped into Tachyon Stacks, and a set of clients that are deployed onto the devices that you want to manage. In addition, a system can have one or more Consumers (the built-in Consumer is Explorer). See Tachyon Architecture and Communication Ports. Tachyon System is also a system role, used by Tachyon for service an equivalent account to perform Tachyon system operations.
Tachyon Toolkit	The Tachyon Toolkit is a collection of the following tools, which can be installed on a Windows computer for use by a User who has appropriate permissions. • Configuration Manager Extensions - this can be installed only on a computer that has already installed a Supported Platforms • Tachyon Instruction Management Studio. • .Tachyon Run Instruction utility The toolkit is available for download from the Tachyon Community in the 1E Support Portal. Documentation for installing and using the Toolkit will be available soon.
Tachyon User	A domain account that is authorized to access Explorer portal and/or the Tachyon Administration pages.

Term	Definition
	Authorization is achieved by adding the AD account or group and assigning it to a role.
Tags	There are two types of tag: coverage tags and freeform tags. In Tachyon log files, these tags are also known a scopable and non-scopable tags.
Two-factor authentication	Also known as 2FA. See Two-factor authentication.
Website	The Tachyon Website hosts the following web applications: Master: • Admin • Consumer - Consumer API • CoreExternal • Platform • Tachyon Response and DMZ: • Background - Background Channel • Core Optional applications on Master: • ContentDistrbution • Experience The Website has an HTTP binding and HTTPS binding. • The HTTP binding uses the server's hostname FQDN as a host header, and is used only by SLA components - please refer to Removing the HTTP binding from the Tachyon website • One or more HTTPS bindings - these use the Tachyon Web Server certificate, the server's DNS Alias as the host name, and has SNI enabled.

Term	Definition
	See Tachyon Architecture and Communication Ports.
Workflow commands	Workflow commands determine how the Coordinator Workflow module processes an instruction, particularly in terms of the permissions required to run the instruction.

1.12 Increasing Azure SQL Server Performance

The latest Azure Ev5 series VMs provides up to three times an increase in remote storage performance compared with previous generations: https://azure.microsoft.com/en-us/blog/increase-remote-storage-performance-with-azure-ebsv5-vms-now-generally-available/.

For larger scale Tachyon environments, achieving the best storage throughput provides the best performance for long running data consolidation operations.

In addition, the latest Ev5 Series VMs support disk busting which provides the ability to boost disk storage IOPS and MB/s performance: https://learn.microsoft.com/en-us/azure/virtual-machines/disk-bursting

On-demand disk bursting in Azure is only available for premium disks of 1TB in size or greater (P30), but by enabling this on SQL data disk(s), allows you to achieve the maximum storage throughput available to the VM on high-intensity operations: https://learn.microsoft.com/en-us/azure/virtual-machines/disks-enable-bursting.

2 1E Client

Here, we describe all aspects of installing and configuring 1E Client.

2.1 Introducing 1E Client

An overview of 1E Client features and modules. The 1E Client provides client functionality for Shopping, WakeUp, Nomad, and Tachyon.

The picture below shows the evolution of the 1E Client from a combination of other 1E Agents.

Note

On non-Windows devices, 1E Client provides only Tachyon client features.

In response to customer demand to reduce the number of agents required, 1E have unified the client functionality for Nomad, PXE Everywhere, Shopping, WakeUp, and Tachyon into a single 1E Client.

On Windows devices, 1E Client provides the following:

- Tachyon client features - see below
- User surveys and notifications, and notification area icon. This is used by Experience to enable User Sentiment and Info Surveys to be presented to end-users.
- Tachyon Telemetry. This information enables 1E to improve its product capabilities and features. It can be configured during Tachyon Setup and information on the data that is sent to 1E is provided in the Tachyon platform documentation.
- Nomad client module - supports content distribution for Configuration Manager and Tachyon
- PXE Everywhere client module - also known as PXE Everywhere Agent - which allows computers to automatically boot up into Windows PE, which then allows a Windows Operating System to be installed
- Shopping client module - supports access to a self-service software portal (which integrates with Configuration Manager) and includes the Windows Servicing Assistant (WSA) to support OS deployment
- WakeUp client module - integrates with Configuration Manager, NightWatchman and/or Nomad.

On non-Windows devices, 1E Client provides only Tachyon client features.

Tachyon client features:

- Real-time response to instructions, which supports the retrieval of information using questions, and running actions
- Tags (freeform and device/coverage)
- Criticality and Location
- 1E Client UI to support the Real-Time Control Center, Announcements, Surveys, and Sentiment features of the Experience application #
- Inventory, including process usage, to support:
  - The Tachyon Activity Record feature
  - The Inventory and other consumer applications.
- Performance metrics features to support the Experience application #
- Policy feature to support consumer applications: Guaranteed State ##, Experience #, and Nomad #
- Modules to support:
  - The Patch Success application #
  - Command and script execution

- Content distribution
- Device criticality
- Manipulation of files and processes
- Manipulation of registry and WMI #
- Security #
- Software uninstallation
- User sessions, including Primary User.

not supported on non-Windows, ## partially supported on non-Windows.

Many features and modules are optionally enabled and configured. The 1E Client can also be extended to support additional features and client modules.

1E Client does not include modules for 1E NightWatchman Agent, which is available as a separate agent. However, NightWatchman Management Center optionally integrates with Tachyon to provide online status of its clients.

On Windows devices, the 1E Client is installed as a Windows service, with a small footprint, with some client modules having their own service if enabled. On non-Windows devices, the 1E Client is installed as a background daemon, also referred to as a service on macOS.

2.1.1 Deployment

The Introducing 1E Client Deployment Assistant can be used with Microsoft System Center Configuration Manager to deploy 1E Client to Windows computers, and also 1E NightWatchman Agent.

1E Client may be deployed independently using alternative software distribution methods.

For further detail, please refer to:

- Deploying 1E Client on Windows
- Deploying 1E Client on macOS
- Deploying 1E Client on Linux
- Deploying 1E Client on Solaris
- Reconfiguring 1E Client
- Verifying

2.1.2 Supported Platforms

All 1E Client features are supported on the following Windows OS:

Windows

- Windows Server 2022

- Windows Server 2019
- Windows Server 2016
- Windows 11 CB 21H2
- Windows 10 CB 21H2
- Windows 10 CB 21H1
- Windows 10 CB 20H2

The zip for 1E Client for Windows is available for download from the 1E Support Portal.

Professional and Enterprise editions are supported for Windows 10 and Wndows 11.

All versions are provided with 32-bit & 64-installers, and can be installed on physical and virtual computers.

> **Note**
>
> This list shows only those OS versions in mainstream support by Microsoft, and therefore supported by 1E, and by 1E Client 8.1.
>
> For Microsoft product lifecycle details, please refer to https://support.microsoft.com/en-us/lifecycle/search.
>
> Please refer to https://support.1e.com/ for details of which Current Branch versions are supported by 1E products, and known issues regarding specific versions.

The Tachyon client features of 1E Client are supported on the following non-Windows OS:

macOS

- macOS Monterey 12.0
- macOS Big Sur 11.0
- macOS Catalina 10.15
- macOS Mojave 10.14

Linux

- CentOS Stream 8
- Debian 10.4
- Fedora 34
- Red Hat Enterprise Linux 7.9
- Red Hat Enterprise Linux 8.5
- SUSE Linux Enterprise 15.2
- Ubuntu 18.04

Solaris

- Please use 1E Client 5.2

Other versions of these non-Windows OS should work but have not been tested by 1E.

1E Client packages for other Linux distributions can be requested, including Raspbian for Raspberry Pi.

The 1E Client for Linux supports the following architectures:

- Linux variations on Intel 64-bit platforms

1E Client packages for Linux are included in the non-Windows zip available for download from the 1E Support Portal.

1E Client supports only Tachyon features on non-Windows devices.

1E Client 8.1 is ***not*** available for Solaris, please use 1E Client 5.2 instead.

The 1E Client 5.2 for Solaris supports the following architectures:

- Solaris on Intel 64-bit and SPARC platforms

1E Client 5.2 package for Solaris is included in the non-Windows zip and available for download from the 1E Support Portal.

1E Client supports only Tachyon features on non-Windows devices.

Additional information on Supported Platforms can be found on the Supported Platforms page.

2.1.3 Constraints of Legacy OS

In this documentation, the following are referred to as legacy OS. Below are described some known issues for these OS.

1E does not provide support for 1E products on the following OS unless the OS is explicitly listed as being supported for a specific 1E product or product feature. This is because Microsoft has ended mainstream support for these OS or they are not significantly used by business organizations.

- **Windows XP ***
- **Windows Vista**
- **Windows 7**
- **Windows 8.0**
- **Windows 8.1**
- **Windows Server 2003 ***
- **Windows Server 2008**
- **Windows Server 2008 R2**
- **Windows Server 2012**
- **Windows Server 2012 R2**

Note

1E Client 8.1 and later will not install on Windows XP and Windows Server 2003. Please contact 1E if you intend to continue using any of the other legacy OS. If you experience an issue, then please try replicating the issue on a supported OS.

For Microsoft product lifecycle details, please refer to https://support.microsoft.com/en-us/lifecycle/search.

2.2 Planning for 1E Client

1E Client is deployed as part of one or more 1E Solutions. You should review documentation for whichever 1E Solutions you are licensed to use, to help you decide which 1E Client features to configure, determined by which server systems are used.

Tip

1E Client contains client features and modules for Tachyon, Shopping/WSA, WakeUp, Nomad and PXE Everywhere clients. You can optionally enable and configure clients during and after installation.

You will need to decide which client features and modules to enable and configure. Unless otherwise stated, modules are only available on Windows computers. Please refer to Supported Platforms for details of supported OS platforms.

All modules including the Tachyon client feature can be optionally enabled during deployment of the 1E Client or after deployment by enabling features in its configuration file.

Feature/module	Description	Infrastructure dependencies
1E Client	This is the main service that determines which features and modules are enabled, including uninstallation of legacy versions of the 1E Client listed below. Please refer to 1E Client settings for details of configurable options.	See Common client requirements.
Tachyon client	Must be enabled on each end-user device to provide Real-time and Inventory features to support the following Tachyon platform applications: Explorer,	Full Tachyon infrastructure,

Feature/module	Description	Infrastructure dependencies
	Experience (including User Sensitivity), Guaranteed State, Patch Success, Application Migration, and AppClarity. Also required to support integration with NightWatchman and Nomad. Supports Windows and non-Windows devices. Please refer to Platform features of the 1E Client for details of configurable options.	including Master and Response Stacks. See infrastructure section in Tachyon platform client requirements.
Nomad client	1E Client module which replaces the NomadBranch client to support Nomad 7.0 and later, as well as Tachyon client's use of the Nomad content download feature. Must be enabled on each end-user device to provide bandwidth-efficient download of content for Tachyon clients, as well as Configuration Manager clients. It is optionally used by PXE Everywhere. Please refer to Content Distribution client settings for details of configurable options.	Tachyon infrastructure, including Master and Response Stacks. See the infrastructure section in Nomad client requirements
PXE Everywhere Agent	1E Client module which replaces the PXE Everywhere Agent to support PXE Everywhere 4.0 and later. Enabled on as may end-user devices as possible to provide a lightweight PXE service that responds to PXE requests on their local subnet. Please refer to /document/preview/647626#UUID-07a4d117-b2a9-8325-0e8e-1d3649997dc4 for details of configurable options.	PXE Everywhere Central must be installed. See the infrastructure section in PXE Everywhere client requirements. You can also configure PXE Everywhere to support environments that use DHCP Snooping.
Shopping client	Must be enabled on each end-user device to support access to the Shopping web portal, and WSA features to support OS rebuilds and upgrades.	Shopping Central website and

Feature/module	Description	Infrastructure dependencies
	Please refer to Shopping client settings for details of configurable options.	Shopping Receiver services are required. See the infrastructure section in Shopping client requirements.
WakeUp client	1E Client module which replaces WakeUp Agent to support WakeUp Server 7.2.500 and later. This version contains hotfixes. Must be enabled on each end-user device to support Wake-on-LAN and Configuration Manager policy refresh. Also integrates with Shopping policy refresh, and with 1E NightWatchman Agent for power management. Please refer to /document/preview/647736#UUID-b588cdab-ae07-3331-ceb1-c8c6ed63aa1e for details of configurable options.	NightWatchman Management Center server and at least one WakeUp Server are required. See the infrastructure section in WakeUp client requirements.

2.2.1 Common client requirements

Prerequisites and dependencies that are common to all client features and modules of the 1E Client.

Tip

1E Client contains client features and modules for Tachyon, Shopping/WSA, WakeUp, Nomad and PXE Everywhere clients. You can optionally enable and configure clients during and after installation.

2.2.1.1 Installation account for Windows

The 1E Client installer installs a service as local system, therefore the installation account for Windows clients must be capable of being elevated in order to run the installer. The simplest way of achieving this is for the account to have full local administrator rights (as a member of the localgroup administrators, either directly or indirectly).

2.2.1.2 Installation account for non-Windows

To install the 1E Client on a non-Windows client the installation account must have privileges to run the **sudo** command.

1E Client supports only Tachyon platform client features on non-Windows devices.

2.2.1.3 Supported Platforms

A list of all the platforms supported by **1E Client**, and the software required to allow **1E Client** to be installed or to work.

2.2.1.3.1 Windows client

Category	Product	Notes
Operating System	• Windows Server 2022 • Windows Server 2019 • Windows Server 2016 • Windows 11 CB 22H2 • Windows 11 CB 21H2 • Windows 10 CB 22H2 • Windows 10 CB 21H2	The zip for 1E Client for Windows is available for download from the support.1e.com/. Professional and Enterprise editions are supported for Windows 10 and Windows 11. All versions are provided with 32-bit & 64-installers, and can be installed on physical and virtual computers. **Note** This list shows only those OS versions in mainstream support by Microsoft, and therefore supported by Tachyon, and by 1E Client 8.1. Please refer to Constraints of Legacy OS regarding the end of mainstream support. For Microsoft product lifecycle details, please refer to https://support.microsoft.com/en-us/lifecycle/search. Refer to Support for Microsoft Rapid-Release Cycle on https://support.1e.com/ for details of which Current Branch versions are supported by 1E products, and known issues regarding specific versions. For installation guidance on Windows, please refer to Deploying 1E Client on Windows. The following 1E Client features and modules are supported on Windows OS: • Real-time features (for example instructions, experience, interaction)

Category	Product	Notes
		• Nomad client • PXE Everywhere Agent client • Shopping client • Windows Servicing Assistant (WSA) client (workstation OS only, not server OS) • WakeUp client
Runtime libraries	• .NET Framework 4.8 • Visual C++ 2015-2019 Redistributable	.NET Framework is required only for the following features of 1E Client: • The Real-Time Control Center feature of the 1E Client (also known as 1E Client UI and Interaction module) supports Experience Engagements (Announcements and Surveys), and ITSM Support Tickets • Windows Servicing Assistant (WSA) is a feature of the Shopping/WSA client module, which supports OS deployment, upgrades and migrations. **Note** This list shows only those .NET Framework versions in mainstream support by Microsoft, and therefore supported by 1E, and by 1E Client 8.1. For Microsoft product lifecycle details, please refer to https://support.microsoft.com/en-us/lifecycle/search. 1E Client installer includes the Visual C++ 2015-2019 Redistributable package.
Other Windows Software	• Nomad 8.0 (or later) • PowerShell 3.0 (or later)	1E Client provides real-time client features. It also includes the Nomad client module. Real-time client features can optionally use Nomad to download content (feature enabled by default) if the Nomad client module in 1E Client is enabled (module

Category	Product	Notes
		disabled by default) or Nomad 7.0 or later is running. For more details please refer to Nomad client requirements. PowerShell is not a prerequisite for installation of the 1E Client. PowerShell is used by some Tachyon instructions (that have PowerShell commands embedded or scripts that are downloaded) and some of these require PowerShell 3.0 or later.
Microsoft Endpoint Configuration Manager Client	• MECM CB 2211 • MECM CB 2207 • MECM CB 2203 • MECM CB 2111 • MECM CB 2107	The following client features work with these versions of Configuration Manager on Windows computers: • Real-time client - instructions used by Tachyon Configuration Manager Console extensions • Nomad client • PXE Everywhere Agent • Shopping/WSA client • WakeUp client - including Policy Refresh and REFRESHONSUBNETCHANGE features Configuration Manager is not a prerequisite for installation of the 1E Client, and except for above features, the 1E Client, its features and modules, have no dependency on Configuration Manager. Tachyon, Nomad, WakeUp, and Application Migration have Configuration Manager Console extensions which are available separately. **Note** This list shows only those Configuration Manager versions in mainstream support by Microsoft, and therefore supported by 1E, and by 1E Client 8.1.

Category	Product	Notes
		For Microsoft product lifecycle details, please refer to https://support.microsoft.com/en-us/lifecycle/search. Please refer to the Support for the Microsoft Rapid-Release Cycle on https://support.1e.com/ for details of which Current Branch versions are supported by 1E products, and known issues regarding specific versions. (Microsoft Endpoint Configuration Manager - MECM - is also known as Configuration Manager, ConfigMgr, Config Man, CM, and SCCM among other names. Version names include 2012 and Current Branch or CB.)

2.2.1.3.2 macOS clients

Category	Product	Notes
Operating System	• macOS Monterey 12.0 • macOS Big Sur 11.6 • macOS Big Sur 11.0 • macOS Catalina 10.15 • macOS Mojave 10.14	Other versions of these non-Windows OS should work but have not been tested by 1E. 1E Client package for macOS is included in the non-Windows zip available for download from the support.1e.com/. **Note** 1E Client for macOS is written for Intel and supported on Apple devices using Intel processors. It is also supported on Apple devices using the M1 chip, provided you have installed Rosetta 2, which is included with Big Sur. 1E Client is a daemon (not an app), therefore, during installation or running it will *not* prompt for Rosetta 2, which does not get installed on-demand. You only need to install Rosetta 2 once, using one of the following commands, but repeating the command will safely reinstall it. The second version of the command requires root permission. Attempting to install on an Intel device will issue a harmless "unrecognized option" usage message.

Category	Product	Notes

		`/usr/sbin/softwareupdate --install-rosetta`
		`/usr/sbin/softwareupdate --install-rosetta --agree-to-license`
		
		For installation guidance, please refer to Deploying 1E Client on macOS.

Other Software	• Bash • Perl • Rosetta 2 (on non-Intel)	Bash and perl are required for installation of 1E Client on all non-Windows OS. Tachyon instructions support the use of Bash scripts on all supported non-Windows OS. To see if an Instruction requires a Bash script, look in its Instruction Definition XML file for Bash script resources defined under the <Resources> tag. Bash is the preferred choice when developing custom instructions for non-Windows OS. There are slight differences between OS implementations of Bash, particularly on the Mac. Therefore, 1E recommends testing custom Bash scripts on each supported OS. Rosetta 2 must be installed before installing 1E Client for macOS on an Apple device using a non-Intel processor such as M1 chip. Please see note above about installing Rosetta 2.

2.2.1.3.3 Linux clients

Category	Product	Notes
Operating System	• CentOS Stream 8 • Debian 10.4 • Fedora 34 • openSUSE Leap 15.2 • Red Hat Enterprise Linux 7.9	Other versions of these non-Windows OS should work but have not been tested by 1E. • 1E Client packages for other Linux distributions can be requested, including Raspberry Pi. • 1E Client for Linux supports Linux variations on Intel 64-bit platforms. • 1E Client packages for Linux are included in the non-Windows zip available for download from support.1e.com/.

Category	Product	Notes
	• Red Hat Enterprise Linux 8.5 • SUSE Linux Enterprise 15.2 • Ubuntu 18.04	• 1E Client supports features on non-Windows devices. For installation guidance on the following OS, please refer to Deploying 1E Client on Linux.
Other Software	• Bash • Perl	Bash and perl are required for installation of 1E Client on all non-Windows OS. Tachyon instructions support the use of Bash scripts on all supported non-Windows OS. To see if an Instruction requires a Bash script, look in its Instruction Definition XML file for Bash script resources defined under the <Resources> tag. Bash is the preferred choice when developing custom instructions for non-Windows OS. There are slight differences between OS implementations of Bash, particularly on the Mac. Therefore, 1E recommends testing custom Bash scripts on each supported OS.

2.2.1.3.4 Solaris clients

Category	Product	Notes
Operating System	• Withdrawn	**Note** 1E Client is no longer available for Solaris, but 1E may reintroduce it, if there is sufficient demand.

2.2.1.4 Feature dependencies

Products and Features with dependencies on the 1E Client.

Supported versions of 1E companion products with features that depend on 1E Client 8.1.

Products and features that depend on 1E Client	Supported versions of companion products	
Tachyon	Tachyon requires the 1E Client (with 1E Client platform features enabled) to be installed on all client computers. This replaces the legacy Tachyon Agent. Tachyon platform features: • Real-time response to instructions, which supports the retrieval of information using questions, and running actions • Tags (freeform and device/coverage) • Criticality and Location • 1E Client UI to support the Real-Time Control Center, Announcements, Surveys, and Sentiment features of the Experience application # • Inventory, including process usage, to support the: – Tachyon Activity Record feature – Inventory and other consumer applications. • Performance metrics features to support the Experience application # • Policy feature to support consumer applications: Guaranteed State ##, Experience #, and Nomad # – Patch Success application # – Command and script execution – Nomad – Device criticality – Manipulation of files and processes	• Tachyon 8.1 • Tachyon 8.0 • Tachyon 5.2 • Tachyon 5.1

Products and features that depend on 1E Client	Supported versions of companion products
	– Manipulation of the registry and WMI # – Security # – Software uninstallation – User sessions, including Primary User. • Modules to support: # not supported on non-Windows, ## partially supported on non-Windows Clients can optionally use the Nomad client module of 1E Client to more efficiently download content.
Nomad	Nomad requires the 1E Client (with Nomad client module enabled) to be installed on all client computers, and on Distribution Points if Configuration Manager is used.	• Nomad 8.1 • Nomad 8.0 • Nomad 7.1
Nomad	Nomad Download Pause is an optional feature of Nomad. It requires the 1E Client (with Nomad client module enabled) to be installed on all client computers, and a Tachyon server infrastructure.	• Tachyon 8.1 • Tachyon 8.0 • Tachyon 5.2 • Tachyon 5.1 • Nomad 8.0 • Nomad 7.1
PXE Everywhere	PXE Everywhere requires the 1E Client (with PXE Everywhere Agent client module enabled) to be installed on all client computers.	• PXE Everywhere 8.1 • PXE Everywhere 8.0

Products and features that depend on 1E Client	Supported versions of companion products
	• PXE Everywhere 4.0
Shopping	Shopping requires the 1E Client (with Shopping client module enabled) to be installed on all client computers. This replaces the legacy Shopping Agent.	• Shopping 6.1 • Shopping 6.0
Shopping	Windows Servicing Assistant (WSA) is an optional feature of Shopping that supports OS Deployment. Please refer to Shopping 6.1 - Preparation: Windows Servicing Assistant (WSA) for WSA features in different versions of 1E Client.	• Nomad 8.1 • Nomad 8.0 • Nomad 7.1 • Shopping 6.1 • Shopping 6.0
WakeUp	WakeUp requires the 1E Client (with WakeUp client module enabled) to be installed on all client computers, and WakeUp Servers. This replaces the WakeUp component of the 1E Agent.	• WakeUp 7.3

Supported versions of 1E companion products that 1E Client 8.1 features depend on.

Products and features that 1E Client depends on	Supported versions of companion products
Tachyon	Tachyon real-time and other features require a full Tachyon infrastructure including a Tachyon Server and a Tachyon license.	• Tachyon 8.1 • Tachyon 8.0 • Tachyon 5.2 • Tachyon 5.1
Nomad	Tachyon platform clients can optionally use Nomad (1E Client with Nomad client features enabled) to provide more efficient downloading of content.	• 1E Client 8.1 (with Nomad client module enabled)

Products and features that 1E Client depends on	Supported versions of companion products
	• 1E Client 8.0 (with Nomad client module enabled) • 1E Client 5.2 (with Nomad client module enabled) • 1E Client 5.1 (with Nomad client module enabled)

2.2.1.5 Firewall ports

1E does not provide a combined diagram showing all components and features. Please refer to the communications reference page for each product:

- Tachyon platform Communication Ports.
- Nomad Communication ports — Diagrams and tables with lists of all the Nomad communication ports.
- PXE Everywhere communication ports — A list of communication ports used by PXE Everywhere. Useful, if needed, for network and device firewalls.
- Shopping communication ports — A diagram and a table with a list of all the Shopping communication ports.
- NightWatchman Enterprise communication ports — Tables with lists of all the NightWatchman Enterprise components and their communication ports.

2.2.1.6 Anti-Virus and Malware

The following should be excluded from scans to prevent file locking and resource deletion.

- 1E log files. See Log files.
- The 1E Client temporary directory. We recommend modifying the TemporaryDirectory 1E Client configuration setting to **%programdata%\1E\Client\Temp** and excluding that directory. See 1E Client settings.

  Note

  TemporaryDirectory must be specified as an absolute path. The directory is not automatically created by 1E Client. It must be created before being set otherwise 1E Client will use its default.

2.2.1.7 Digital signing certificates

On Windows computers, the installation MSIs, executables and DLLs of the 1E software are digitally signed by 1E using the **1E Limited** SHA1 and SHA256 signature certificates.

These signing certificates are issued by the **Symantec Class 3 SHA256 Code Signing CA**, which in turn is issued by the root CA **VeriSign Class 3 Public Primary Certification Authority - G5**.

The SHA1 and SHA256 signature certificates are each countersigned with the same Timestamp signature certificate **Starfield Timestamp Authority - G2**, itself issued by **Starfield Secure Certificate Authority - G2**, in turn issued by the root CA **Starfield Root Certificate Authority – G2**.

The root CA certificates (for signing and countersigning) must exist in the **Third-Party Root Certification Authorities** store (which is replicated in the Trusted Root Certification Authorities store). These root CA certificates are normally automatically provided by Microsoft's Update Root Certificates feature, however for legacy OS computers in a lab environment that are not connected to the Internet, see Common client requirements.

2.2.1.8 Constraints of Legacy OS

1E does not provide support for 1E products on the following OS unless the OS is explicitly listed as being supported for a specific 1E product or product feature. This is because Microsoft has ended mainstream support for these OS or they are not significantly used by business organizations. For details, refer to Supported Platforms

2.2.2 Tachyon platform client requirements

Information that will help you design and plan the implementation of Tachyon in your organization. This includes all the prerequisites and dependencies, which are necessary to install 1E Client with Tachyon platform features enabled.

For a full understanding of Tachyon features and their configuration, please refer to Introducing Tachyon documentation.

Tip

Tachyon platform client features are not required if the 1E Client is being installed only to support PXE Everywhere, Shopping, or WakeUp.

Tachyon platform client features are required if you are using any of the following:

- Experience
- Explorer
- Guaranteed State
- Patch Success
- Nomad - if using Nomad features of the Tachyon platform. Also requires Nomad client to be enabled
- AppClarity - if using Tachyon as an inventory data source
- Application Migration - if using Tachyon as an inventory data source.

2.2.2.1 Public Key Infrastructure

Tachyon features require a PKI and certificates on client devices and servers. Please see below for client requirements, and Certificate requirements for server requirements.

You need to have a PKI in your environment with at least one Issuing CA.

Tachyon requires each Issuing CA has:

- A **Certificate Revocation List** (CRL) **Distribution Point** (CDP) that uses HTTP/S
- This HTTP/S CDP information is included in certificates issued to Tachyon Server and client devices.

PKI notes

If you have an existing PKI and have just added a new CDP to support HTTP/S then you will need to re-issue certificates to your servers and devices.

Tachyon deliberately does not work with self-signed certificates for security reasons. Therefore, Tachyon client or Server cannot be installed on the same server as a Root CA, because its certificate is self-signed.

Tachyon uses TLSv1.2. If your PKI is using SHA512, then please ensure that your environment has relevant updates applied, as described in KB2973337. See Client issues.

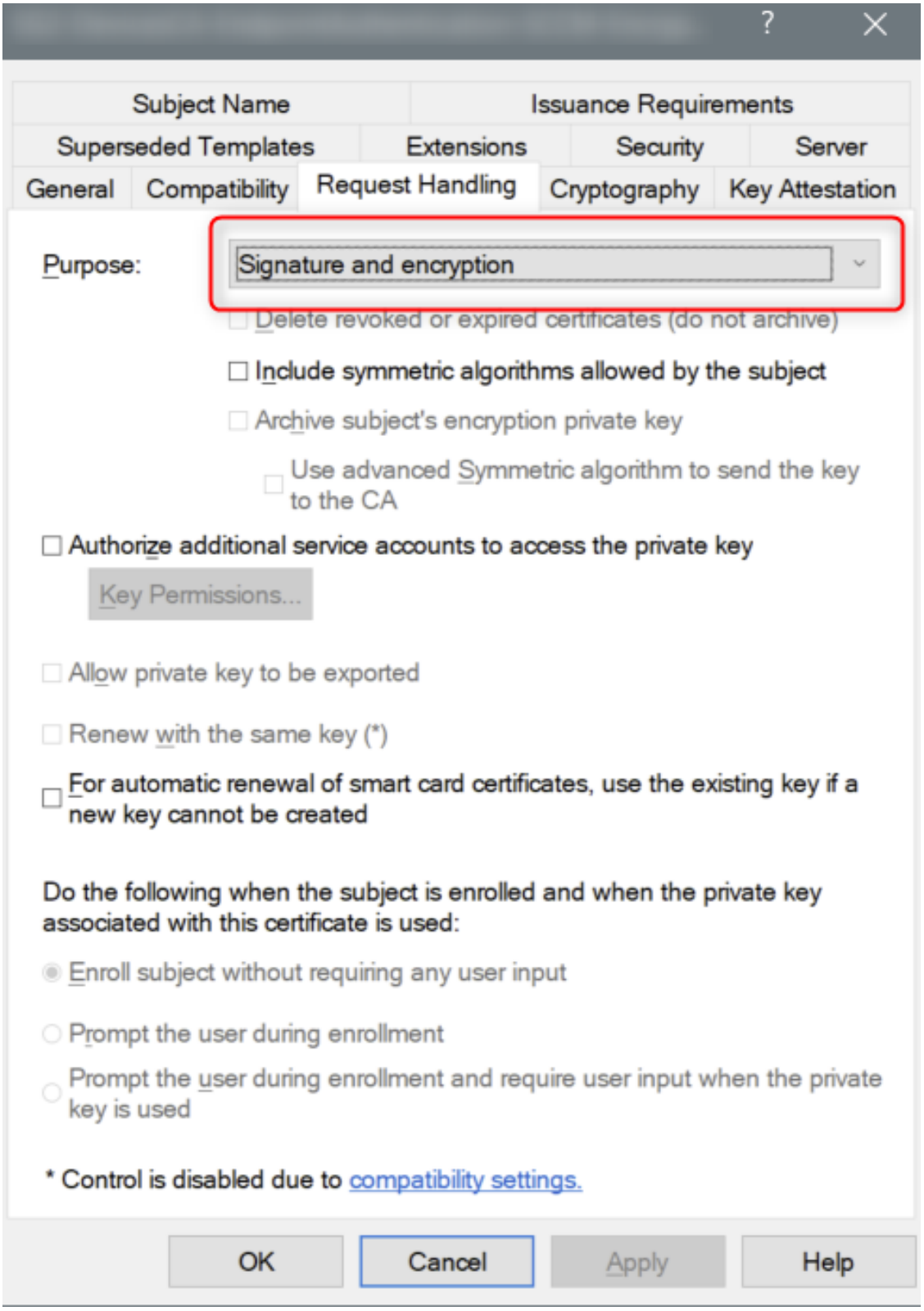
If you want Tachyon to manage legacy OS that Microsoft no longer supports, there may be issues with encrypted certificates described in Common client requirements.

2.2.2.2 Client Certificates

If you have configured Tachyon Server to require client certificates (Client certificates) then each device requires a certificate with the following properties, so the Tachyon platform client can be authenticated by the Tachyon Switch.

Note

The 1E Client requires that the client certificate it presents to the platform has both the **Signature** and **Encryption** request handling options. These options are the defaults if provisioning using a Computer Certificate template from a Microsoft Windows Certificate Authority. If you are using a custom template, or an alternative certificate authority, you should confirm that both these options are enabled.



- Issued by a trusted Certificate Authority (CA):
  - The certificate for the Root CA in the Certification Path must exist in the Trusted Root CA store of the client.

  - If the issuing CA is not the Root CA then the certificate for the issuing CA and any intermediate CA in the Certification Path must exist in the Intermediate CA store of the client.
  - If either of these CA certificates is different from those used by the Tachyon Web Server, they will need to be exported and imported on the Tachyon Web Server.
  - Most organizations have automated distribution of these CA certificates to clients and servers, using Group Policy for example.
- Has at least the following Enhanced Key Usage:
  - Client Authentication.
- Has at least the following Key Usage:
  - Digital Signature.
  - Key encipherment.
- Has a private key:
  - For workgroup and non-Windows devices, the **private key must be exportable**
- Revocation information is included:
  - References at least one CRL Distribution point that uses HTTP.
- Has a Subject Name of type Common Name (**CN=<computername>**) or Subject Alternative Name (**DNS Name=<computername>**) where <computername> depends on the type of device:
  - On domain-joined Windows PCs this must be the **computername FQDN** of the computer, for example **W701.ACME.LOCAL**.
  - On workgroup Windows PCs and non-Windows devices, this must be the computername of the computer - as returned by the **hostname** command, for example on Windows PC this could be **W701**, and on a Mac this could be **MAC01.local**.

Note

Tachyon clients and Switches use OpenSSL and its validation process to verify certificates.

The client device's certificate is stored differently depending on the type of OS:

- For Windows devices, the certificate is stored in the Windows Local Computer personal certificates store.
- For non-Windows devices, except for the Mac, the client does not use proprietary certificate stores. Instead, the client requires the certificate to exist as a **.pfx** file in the client installation folder structure, refer to Client certificates.
- For macOS, you have a choice of storing the client certificate in the macOS Key Store or using the **.pfx** file approach required by other non-Windows devices, refer to Client certificates.

The following need to be considered when requesting this type of certificate:

- The certificate can be used only on the server it was intended, that has the correct computername FQDN and DNS Alias FQDN.
- It is not possible to use the **Create Certificate Request** method in IIS Manager Server Certificates, because it does not support all the above requirements.
- If you have a Microsoft CA, and a suitable **Web Server** template has been issued and enabled in the **Directory Enrollment Policy**, then it is possible to **Request New Certificate** in the **Certificates (Local Computer)** mmc snap-in and use the **Certificate Enrollment wizard**.
- Many organizations have their own process for submitting a Certificate Signing Request (CSR). Please ensure all the above requirements are specified. Security administrators sometimes have difficulty providing a certificate with one or more Subject Alternative Names (SAN), and it helps to explain these are type DNS.

2.2.2.3 Other infrastructure requirements

In addition to PKI and network requirements, other infrastructure dependencies are:

- **DNS** - each Tachyon Server requires at least one DNS Name
- **Active Directory** - for installation and user accounts and groups; Tachyon supports multi-domain, multi-forest environments that have two-way trusts
- **IIS** - a standard configuration required on each Tachyon Server
- **SQL Server** - databases for Tachyon Master and Response Stacks, 1E Catalog, SLA, BI, Experience and Nomad
- **SQL Analysis Services** - must be installed in multi-dimensional mode, if you are installing Business Intelligence (required by Patch Success)
- **Email** - optional for approval and notification emails, but required if using two-factor authentication (2FA)
- **Internet access** - Master Stack requires access to the 1E license service via the Internet in order to keep the Tachyon license activated, and 1E Catalog requires access to the 1E Catalog Cloud service to download Catalog updates.

These are explained in Planning for Tachyon.

2.2.2.4 Tachyon platform client integration with Nomad

Tachyon platform client integration with Nomad allows clients to make use of Nomad features for more efficient downloading of content from different HTTP sources, including the Tachyon Background Channel. Using this feature needs the following settings enabled, you can do this during the 1E Client installation:

- Nomad client module - enabled (off by default)
- Tachyon integration with Nomad - enabled (on by default).

With the Tachyon integration setting enabled, the client will automatically detect if the Nomad client module is enabled and use it to download content from HTTP sources when requested.

Tachyon use of Nomad works irrespective of whether Nomad is integrated with Microsoft Configuration Manager, or using 1E ActiveEfficiency or Content Distribution features.

The Nomad client is included in 1E Client 8.1 and later requires Tachyon platform with Nomad features enabled. Nomad is the replacement for ActiveEfficiency.

Configuration Manager is not a prerequisite for Tachyon integration with Nomad, but you will need to consider the following:

Configuration Manager client present	You do not need to make any configuration changes to Nomad for it to integrate with Tachyon, other than enable the Nomad client module in the 1E Client, or have a legacy version of the Nomad client installed. Please refer to Introducing Nomad documentation for guidance on designing and deploying Nomad.
Configuration Manager client not present	You must ensure the following bits are enabled in the relevant Nomad installer properties and their corresponding registry values. These are enabled by default in the Nomad client module of the 1E Client, but if you modify the following properties for any other purposes, then you must ensure these bits are set: • CompatibilityFlags bit 1 - enable long hashes • SpecialNetShare bit 13 - enable HTTP(S)

Note

If you have any configuration baselines or other policies that control Nomad settings, then these will need to be reviewed. Review is especially important if you have upgraded from legacy Nomad Branch 6.x where these bits were disabled by default.

2.2.2.5 Tachyon scripting requirements

Tachyon real-time instructions are written in the Tachyon native language SCALE, which is very like SQL but with additional logic, functions, and methods. Scripts can be downloaded when an instruction runs or actual command text is embedded in the instruction. You will very probably want to use scripts in the instructions you download from 1E or instructions you write yourself. Therefore, you must ensure the appropriate scripting environment is present on Agent devices.

Windows Tachyon clients can use PowerShell scripts. Ensure your client devices have an appropriate version of PowerShell installed to support any custom scripts you may develop. See PowerShell on Windows OS.

Non-Windows clients can use bash as their scripting medium. This should be present on all non-Windows client devices.

For more information about SCALE and writing your own instructions, please refer to:

- Installing TIMS

- /document/preview/736871#UUID-66857689-bfb0-8dbc-ae8d-1de40c66fad9
- /document/preview/738566#UUID-88a06651-3aab-3a4b-7c4d-36010c23c8a6.

2.2.2.5.1 PowerShell

PowerShell is used by some instructions (that have PowerShell commands embedded or scripts that are downloaded) and some of these require PowerShell 3.0 or later, although some scripts will support PowerShell 2.0. PowerShell scripts are supported only on Windows OS.

If installing or upgrading PowerShell, it is best to install the latest version available. However, do not expect full forward or backward compatibility between PowerShell versions.

> **Tip**
>
> To determine the version of PowerShell on a computer, start PowerShell (command prompt or ISE) and enter one of the following commands: **$PSVersionTable.PSVersion** or **$PSVersionTable** for more detail.

The table below shows which versions of PowerShell are supported on each OS version and Service Pack, and if it is built-in or needs to be installed.

OS Version	PowerShell Version				Notes
Windows Server 2022				RTM (Notes 12, 13)	Note 4
Windows 11				RTM (built-in)	
Windows Server 2016, 2019, 2022			RTM (Note 9)	RTM (Notes 12, 13)	Note 4
Windows 10			RTM (built-in)	Anniversary Update (built-in)	
Windows Server 2012 R2 *		RTM (built-in)	RTM (Note 9)	RTM (Note 12)	Note 4
Windows 8.1 *		RTM (built-in)	RTM (Note 9)	RTM (Note 12)	

OS Version	PowerShell Version	Notes					
Windows Server 2012 *			RTM (built-in)	RTM (Note 7)	RTM (Note 9)	RTM (Note 12)	Note 4
Windows 8 *			RTM (built-in)				
Windows Server 2008 R2 *		RTM (built-in)	SP1 (Note 6)	SP1 (Note 7)	SP1 (Note 8)	SP1 (Note 10)	Note 4
Windows 7		RTM (built-in)	SP1 (Note 6)	SP1 (Note 7)	SP1 (Note 8)	SP1 (Note 10)	
Windows Server 2008 *	RTM (built-in)		SP1 & SP2 (Note 2)				
Windows Server 2003 *	RTM & SP1	R2 & SP2					Notes 1, 2
Windows Vista *	RTM	SP1 & SP2					Notes 1, 2
Windows XP *	RTM, SP1 & SP2	SP3					Notes 1, 2

* These OS are regarded as legacy OS:

1. PowerShell is not built-in for these OS. These OS do not support 3.0 or later. See Constraints of Legacy OS
2. If PowerShell 1.0 is installed it must be removed in order to install a later version.
3. Support for PowerShell 2.0 is included in PowerShell 3.0 and later.
4. PowerShell is not installed by default on these OS but is an optional feature that should be enabled using Server Manager.
5. PowerShell 2.0 is part of WMF Core package (KB968930) with prerequisite of .NET Framework 3.51 (which includes .NET 2.0 SP1).

6. PowerShell 3.0 is part of WMF 3.0 with prerequisite of .NET Framework 4.0 or later. Refer https://www.microsoft.com/en-us/download/details.aspx?id=34595

7. PowerShell 4.0 is part of WMF 4.0 with prerequisite of .NET Framework 4.5 or later. Refer https://www.microsoft.com/en-us/download/details.aspx?id=40855

8. PowerShell 5.0 is part of WMF 5.0 with prerequisites of .NET Framework 4.5 or later and WMF 4.0. Refer https://www.microsoft.com/en-us/download/details.aspx?id=50395

9. PowerShell 5.0 is part of WMF 5.0 without any other prerequisites. Refer https://www.microsoft.com/en-us/download/details.aspx?id=50395

10. PowerShell 5.1 is part of WMF 5.1 with prerequisites of .NET Framework 4.6 or later, WMF 4.0 and SHA-2 Code Signing. Refer https://msdn.microsoft.com/en-us/powershell/wmf/5.1/install-configure

11. PowerShell 5.1 is part of WMF 5.1 with prerequisites of .NET Framework 4.6 or later and WMF 4.0. Refer https://msdn.microsoft.com/en-us/powershell/wmf/5.1/install-configure

12. PowerShell 5.1 is part of WMF 5.1 with prerequisite of .NET Framework 4.6 or later. Refer https://msdn.microsoft.com/en-us/powershell/wmf/5.1/install-configure

13. In these Server OS, PowerShell 5.1 is referred to as the Desktop Experience. You can use the PowerShell Core version if you prefer.

Please refer tohttps://support.microsoft.com/en-gb/help/17455/lifecycle-faq-net-framework for details of Microsoft support for .NET Framework.

- Support for 4, 4.5, and 4.5.1 ended on January 12, 2016
- Support for 4.5.2, 4.6 and 4.6.1 ended on April 26, 2022

2.2.2.5.2 Bash and Perl

Bash and Perl are required for the installation of all non-Windows 1E Client.

Tachyon instructions support the use of Bash scripts on all supported non-Windows OS.

To see if an Instruction requires a Bash script, look in its Instruction Definition XML file for the Scripting. Run method. Bash is the preferred choice when developing custom Instructions for non-Windows OS.

There are slight differences between OS implementations of Bash, particularly on the Mac. Therefore, 1E recommends testing custom Bash scripts on each supported OS.

2.2.2.6 Requirements for verifying the Tachyon installation

The Verifying page provides detailed steps for verifying a new or upgraded infrastructure, including the first steps for uploading and running instructions. Below is a list of requirements to perform verification testing.

1. Tachyon Server installed.
2. Remote workstation with a Supported Platforms.
3. The name and password for the **server installation account**.

a. The AD account must be enabled.

b. The account may already be assigned to other Tachyon roles either directly or via membership of an AD group role.

4. Two AD User accounts, **Test User 1** and **2**.

   a. Must not be existing Tachyon users because they will be assigned specific roles for the purpose of these tests.

   b. Must have email addresses and be able to read emails.

5. The **1E Tachyon Platform** instruction set with two Verification instructions.

   a. The verification steps describe how to create this instruction set by uploading the Tachyon Platform Product Pack.

   b. You may have already uploaded this Product Pack using the Tachyon Product Pack Deployment Tool, either during Setup or after.

   c. The Tachyon Platform Product Pack is included in the **Tachyon Platform** file that you can download from the 1E Exchange.

6. At least one test device on which the 1E Client will be installed.

7. 1E Client installation source files and configuration details required by your Tachyon implementation.

2.2.2.7 Firewall ports

Please refer to urn:resource:component:647599.

2.2.3 Nomad client requirements

Information that will help you design and plan the implementation of **Nomad** in your organization. This includes all the prerequisites and dependencies, which are necessary to install 1E Client with Nomad client enabled.

> **Tip**
>
> Nomad client features are not required if the 1E Client is being installed only to support Tachyon, Shopping, or WakeUp. However, Nomad can be used to help platform clients download content from the Background Channel and other sources. For more detail, please refer to Tachyon platform client integration with Nomad.

2.2.3.1 Nomad infrastructure dependencies

For a full understanding of Nomad features and their configuration, please refer to Introducing Nomad documentation.

In addition to deploying 1E Client (with Nomad client module enabled) on all computers and on Configuration Manager Distribution Points, the following are also required:

- Nomad tools installed on Configuration Manager sites and SMS Providers

- Nomad Configuration Manager Console extensions on Configuration Manager site servers, any other computer that has the Configuration Manager Console installed.

Nomad can be used for downloading content for platform clients, as well as Configuration Manager clients.

2.2.3.2 Downloading client content and Nomad integration

1E Client downloads content from the Tachyon Background Channel. Content is mainly scripts and other files required by instructions. It also includes client resources such as extensible modules, providers, and other dependencies to maintain the 1E Client. In most cases, client resources are version controlled to prevent repeated downloads. Tachyon instructions always request a download even if they have run an instruction before, unless the content for that instruction has been cached in memory.

You may need to consider the impact on the network if there is a large amount of content included in an instruction. This is more of an operational consideration instead of a design consideration.

Nomad is an optionally licensed component of the 1E Client. It makes software deployment, patching and downloading content more efficient and reduces the impact on the network. It removes the need for remote Distribution Point servers in Microsoft System Center Configuration Manager systems. When Nomad is installed on computers, it automatically elects a peer to download content from a server over the WAN and then peer-shares the content with other PCs at the same location. The downloaded content is cached locally on each PC in case it is needed again.

Tachyon can optionally use Nomad to download content from servers irrespective of whether Nomad is integrated with Configuration Manager or not, and also uses advanced Nomad features.

2.2.3.2.1 Tachyon platform client integration with Nomad disabled

If Nomad integration is not used, the following applies:

- Tachyon platform client waits a randomized stagger period defined by its DefaultStaggerRangeSeconds (refer to #UUID24ef0cf654c33163e98e9dc427464c32_id_Deploying1EClientonWindowsDEFAULTSTAGGERRANGESECONDSDEFAULTSTAGGERRANGESECONDS for details) setting, and then downloads content from the specified **Background Channel**.
- Tachyon platform client retains modules and extensible that it has downloaded but does not retain instruction scripts after they have been run. Any instruction that requires a script or other file will download the latest version each time the instruction is run.

2.2.3.2.2 1E Client integration with Content Distributionenabled

Content Distribution integration is available on Windows PC devices and is enabled by default, but can be disabled during installation of the 1E Client.

With the Content Distribution integration feature enabled, 1E Client will detect if a supported version of Content Distribution is running on the device.

- 1E Client immediately requests Content Distribution to download content from the specified HTTP source, such as the **Background Channel**. Content Distribution behaves in the same way as it does with

Configuration Manager by ensuring the latest version of content is obtained and electing a master to perform the actual download.

- Content Distribution maintains its own cache of downloaded content which avoids the need for repeat downloads over the WAN, and provides content to peers that require the same resources which avoids peer devices having to download over the WAN.
- If the Content Distribution integration feature is enabled, and requested content is not provided within the timeout period, the 1E Client will fall back to downloading directly from the HTTP source. The most likely reason for a timeout is if Content Distribution is busy downloading other content.

To use Content Distribution, there is no special configuration of Tachyon Servers unless you want to use server-based features provided by the Content Distribution and Content Distribution, which requires the reverse proxy feature to be configured on Background Channels.

The Background Channel is a web application on the Tachyon Server which uses HTTPS and default port is 443. The URL for the Background Channel is defined in the 1E Client configuration file and is specified during installation of the 1E Client if Tachyon features are enabled. The 1E Client passes this URL to Content Distribution when it requests content to be downloaded. Instructions can also specify other HTTP sources.

Content Distribution does not need to be configured to use certificates in order to communicate with the Background Channel (the Content Distribution CertIssuer and CertSubject settings are used only with Configuration Manager Distribution Points that are configured to validate device certificates).

The **Nomad Single-Site Download (SSD)** feature, which uses **Content Distribution**, further reduces the impact of downloading content over the WAN.

2.2.3.3 Firewall ports

Refer to Firewall ports.

2.2.4 PXE Everywhere client requirements

Information that will help you design and plan the implementation of **PXE Everywhere** in your organization. This includes all the prerequisites and dependencies, which are necessary to install 1E Client with the PXE Everywhere Agent client module enabled.

For a full understanding of PXE Everywhere features and their configuration, please refer to Introducing PXE Everywhere documentation.

2.2.4.1 PXE Everywhere infrastructure dependencies

PXE Everywhere helps with OS Deployment. The PXE Everywhere Agent is a lightweight PXE service deployed throughout the network, responding to PXE requests on local subnets. Local Agents elect which one will respond to the original PXE request, and communicate with PXE Everywhere Central to determine what to do next, by asking Configuration Manager. If the original PXE client has been assigned a Task Sequence, then the Agent provides the associated boot image to the local PXE client, which can then start the Task Sequence. Boot images will have been previously deployed to Agents, providing the reassurance there will always be a local Agent capable of quickly responding with the relevant boot image. It also means you can deploy a PXE solution

without needing to configure routers to support DHCP forwarding to a central PXE server. Please refer to Introducing PXE Everywhere documentation for more details.

PXE Everywhere does not depend on Nomad but is often used with Nomad, which helps with the distribution of PXE boot images via Configuration Manager, which further reduces the impact of network traffic on the WAN.

Introducing 1E Client Deployment Assistant is the recommended method of using Configuration Manager to deploy 1E Client to client computers. CDA is necessary if you want to include a boot image in the same deployment as the 1E Client.

PXE Everywhere also works in environments that use DHCP Snooping, as described in DHCP Snooping. This requires the following configuration changes:

- Install one or more PXE Everywhere Responders, typically on server OS in the central network - Responders only communicate with Agents, they do not communicate with the PXE Everywhere Central server or with Configuration Manager.
- Authorize the Responders to respond to PXE requests.
- Configure DHCP Relays (IP helpers) on routers to forward DHCP/PXE request packets to the PXE Everywhere Responder(s) in addition to any DHCP Relays you already have configured for the DHCP server(s).
- Configure PXE Everywhere Agents to listen on port 2067 (default) instead of port 67.

2.2.4.2 Firewall ports

Please refer to Communication Ports.

2.2.5 Shopping client requirements

Information that will help you design and plan the implementation of **Shopping** in your organization. This includes all the prerequisites and dependencies, which are necessary to install 1E Client with Shopping client enabled.

For a full understanding of Shopping and WSA features and their configuration please refer to Shopping 6.1 documentation.

> **Tip**
>
> Shopping client features are not required if the 1E Client is being installed only to support Tachyon, Nomad, or WakeUp.

2.2.5.1 Shopping infrastructure dependencies

Please refer to Shopping 6.1 documentation for more details.

Shopping requires an ActiveEfficiency Server, and ActiveEfficiency Scout to import data from Configuration Manager into ActiveEfficiency.

A Shopping solution requires a Shopping Central server on a web server, and a Shopping Receiver installed on each Configuration Manager Site server that has a client reporting to it, and on a CAS if using Shopping for OS Deployment.

2.2.5.2 Loopback feature

If users are using Edge or Metro browsers, then you must enable the loopback feature. This feature implements a mechanism for passing information between the Shopping client, the browser's secure sandboxed environment and the local machine. This mechanism affects these browsers as a whole and is not just restricted for use by Shopping.

> **Note**
>
> Before enabling the loopback feature, check your security policy on enabling loopback and be aware of the implications of allowing access between browsers and the local machine.

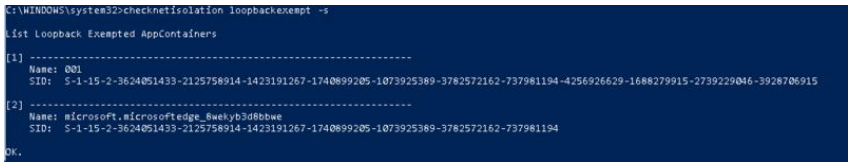
2.2.5.2.1 Checking loopback exemption on Microsoft Edge and Metro Internet Explorer browsers

The following is valid only for Windows 8.1 and Windows 10.

Open a **command-prompt as administrator** on the computer you want to check, then run the following command to verify that loopback exemption was enabled during the installation of the 1E Client.

```
CheckNetIsolation LoopbackExempt -s
```

Output should be:



If either of these items is missing, you can manually add them by executing the following commands. Quotes may be required around the name of the app.

For IE:

```
CheckNetIsolation LoopbackExempt -a -n=windows_ie_ac_001
```

For Edge:

```
CheckNetIsolation LoopbackExempt -a -n=Microsoft.MicrosoftEdge_8wekyb3d8bbwe
```

Removing

The exemption from loopback restrictions can also be removed for all apps installed by using the following command:

```
CheckNetIsolation LoopbackExempt –c
```

More information

For more information from Microsoft about CheckNetIsolation please refer to: https://docs.microsoft.com/en-us/previous-versions/windows/apps/hh780593(v=win.10).

2.2.5.3 Information provided by the Shopping client

The following details are provided by the Shopping client, when a user browses to the Shopping Web Portal, and the website uses the loopback feature to query the local computer.

Attribute	Description	Example
UniqueId	Configuration Manager client GUID	GUID:04804aed-922c-4a4b-9f41-eab6592e7d83
AssignedSite	Configuration Manager client Site code	CM1
MacAddress	Computer's MAC Address	20-68-9D-5B-EB-73
HostName	Computername	1EUKCOL1184
HostDomainName	Computer's NetBIOS Domain Name	1E
OSVersion	OS Version	6.3.9600
OSArchitecture	OS Architecture	64-bit
OSRole	Workstation or Server	1
SccmVersion	Configuration Manager client version	5.00.8239.1203

You can confirm Shopping is able to get these "Probe details" via your browser by going to the Shopping portal and navigating to **Preferences** → **Diagnostics** page, or using the URL **https://<shopping>/Shopping/context**

The diagnostics page also displays the **Timezone** of the browser (as minutes ahead of UTC), and does not display the **SccmVersion**. It also shows Identity details stored in the Shopping database that Shopping has obtained from Active Directory about your user account and machine details.

2.2.5.4 Firewall ports

Please refer to /document/preview/717111#UUID-9c22bc2f-ae28-7668-9b8b-64706f16e1e2.

2.2.6 WakeUp client requirements

Information that will help you design and plan the implementation of **WakeUp client** in your organization. This includes all the prerequisites and dependencies, which are necessary to install 1E Client with WakeUp client enabled.

Tip

WakeUp client features are not required if the 1E Client is being installed only to support Tachyon, Nomad, or Shopping.

2.2.6.1 NightWatchman and WakeUp infrastructure dependencies

For a full understanding of WakeUp and NightWatchman features and their configuration, please refer to NightWatchman Enterprise 7.3 documentation.

If implementing WakeUp, or Nomad integration with WakeUp, then you require at least one WakeUp Server. If you have Configuration Manager, you require a WakeUp Server on each Site server that has clients reporting to it. If you do not have Configuration Manager, you require one or more independent WakeUp Servers.

A NightWatchman Management Center server is required when implementing a WakeUp solution. Your 1E Account Team will explain whether your license also includes NightWatchman client features. 1E NightWatchman Agent is a separately installed client agent, that can optionally be used to help with power management of computers. It is not included in 1E Client, but is included in the Introducing 1E Client Deployment Assistantwhich assists with deploying Windows versions of 1E Client via Configuration Manager. As well as providing power management features, when 1E NightWatchman Agent is installed alongside the WakeUp client, it will optionally manage the computer returning to its original power state after being woken using 1E WakeUp and the computer is not busy, for example, installing patches.

Web WakeUp is an optional server component that is typically installed on the NightWatchman Management Center server. It is a web portal for users and administrators to search for computers to wake. It optionally provides a remote desktop link to the woken computer.

2.2.6.2 Client hardware requirements for WoL

To utilize Wake-On-LAN (WoL) technology, you need the following hardware configurations:

Hardware	Configuration
Network card	A network card that can support Wake-On-LAN. Your network card vendor can tell you if your network adapter supports Wake-On-LAN. If it does, it must be configured to enable remote wake-up. Some adapter drivers are disabled by default within the operating system.
System BIOS	Wake-On-LAN must be enabled in the system BIOS. This option can usually be found in the Boot menu of the BIOS configuration program. Some BIOS have a 'Maximum Power Savings' or 'Low Power S5' option, which should be disabled in order to allow some power to the network card.
Power management	APM or ACPI should be enabled, otherwise, the user of the machine should ensure that it is powered off by hitting the off button after shutdown.

A quick way to tell if a system is Wake-On-LAN ready is to power down the system and then look at the network adapter display LED's. If the lights are still on, then chances are that the system is OK. Windows must have been powered down gracefully (either off or asleep) in order for it to prepare the network card for WOL.

Tip

Please contact 1E if you require guidance with WoL configuration on Windows operating systems and enterprise vendor hardware including Dell, HP and Lenovo computers.

2.2.6.3 1E NightWatchman Agent

If you are deploying WakeUp as part of a NightWatchman Enterprise power management solution then you will also need to consider 1E NightWatchman Agent requirements.

2.2.6.4 Firewall Ports

Please refer to NightWatchman Enterprise communication ports.

2.3 Installing 1E Client

How to deploy 1E Client..

1E Client provides Tachyon features and modules for Nomad, PXE Everywhere, Shopping/WSA, and WakeUp.

2.3.1 Deploying 1E Client on Windows

Guidance for deploying 1E Client onto **Windows** computers, including installation and uninstallation.

If you are upgrading Tachyon Agent or other 1E Client agents to 1E Client, then please consult Upgrading 1E Client.

If you are reconfiguring 1E Client, then please refer to Reconfiguring 1E Client.

2.3.1.1 Requirements

Please review Planning for 1E Client pages. After installation, please review the Verifying page.

For details of supported OS platforms, please refer to Common client requirements page.

The guidance below is for deployment on Windows devices. For other platforms, please refer to Deploying 1E Client on macOS and Deploying 1E Client on Linux.

Note

1E Client does not have a license key. Even so, you must adhere to the terms of your license agreement.

2.3.1.1.1 Deployment choices

You must decide how you will configure the 1E Client and deploy to devices.

Note

For more information about configuring 1E Client properties during and after installation, please refer to 1E Client configuration settings and installer properties.

Use your existing software deployment tool to deploy 1E Client, for example, Microsoft System Center Configuration Manager. Some organizations may require the 1E Client to be packaged prior to deployment. The Introducing 1E Client Deployment Assistant is designed to help install Windows versions of 1E Client and other 1E agents using Configuration Manager. It includes template transform files for each combination of client/agent for 32-bit and 64-bit platforms, and automatically creates collections and deployments in Configuration Manager, so that you only need to populate the collections.

Tip

CDA is the recommended method of deploying 1E Client on Windows if your organization uses Configuration Manager. It is a wizard that guides you through common settings for clients and deployments, and provides additional options that the installers do not.

CDA is available as a zip file which you can download from the 1E Support Portal.

You use the CDA wizard to do the following:

- Create a MST transform file for each MSI containing your chosen settings
- Create a text file that contains the command-line for deploying each MSI
- Optionally allow deployment of an MSP patch file for each MSI
- Optionally connect to Microsoft Endpoint Configuration Manager to:
  - Create applications and packages
  - Create deployments and collections for the applications
  - Distribute source files to Distribution Points.

The CDA wizard creates an answer file that records the chosen settings (the wizard uses a template answer file that controls the default settings seen in the wizard).

You can download the latest Accumulated Hotfix MSP for each client, from the 1E Support Portal. The CDA zip that you download may already contain an MSP file for each client. You should remove this if you have alternate methods of deploying patches.

If you are using Configuration Manager, you must run the CDA Wizard on a computer that has the Configuration Manager console installed. Windows ADK (with WinPE add-on) is also required locally if CDA is used to configure a deployment of PXE Everywhere.

Windows installation account

The 1E Client installer installs a service as local system, therefore the installation account for Windows clients must be capable of being elevated in order to run the installer. The simplest way of achieving this is for the account to have full local administrator rights (as a member of the localgroup administrators, either directly or indirectly).

2.3.1.2 Preparation

1E Client installation files are available for download from https://support.1e.com/.

1E Client should be installed on all Windows clients. You must use the correct installer file according to the Windows architecture of the device:

- **1E.Client-x64.msi** is for 64-bit architectures
- **1E.Client-x86.msi** is for 32-bit architectures.

Pending Reboots

Please ensure you allow for a reboot, especially for mission-critical servers. After installing the 1E Client, the computer may request a reboot that appears to be caused by 1E Client, but is actually caused by a pending reboot from a previous software or patch installation. Pending reboots and notifications can occur up to several hours after installation, depending on policies in your organization, such as Computer Restart settings for Configuration Manager clients.

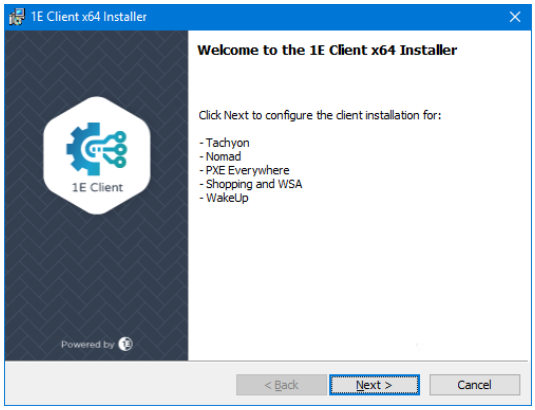
2.3.1.3 Installing the 1E Client interactively

When running the MSI directly or using a command line, please ensure the installation account has the required permissions as described in Installing the 1E Client interactively

The following panels describe each screen of the 1E Client installer.

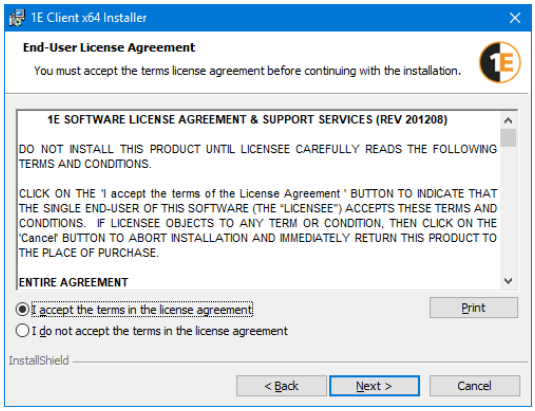
2.3.1.3.1 Welcome

The welcome screen, just click **Next** to continue.



2.3.1.3.2 End-User License Agreement

You must read and then accept this license information by clicking
I accept the terms in the license agreement before you can continue with the installation. Once this is done click **Next**.



2.3.1.3.3 Installation Folder

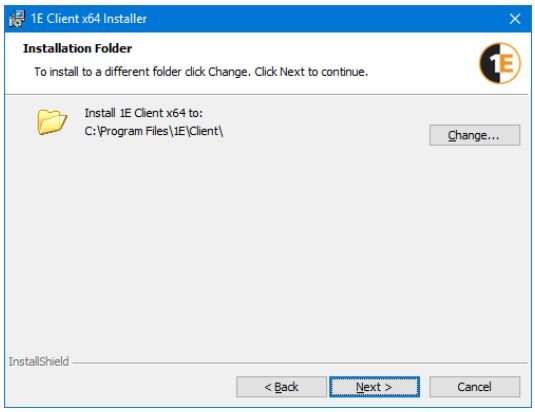
The next screen lets you to choose the folder where the 1E Client will be installed:

By default, this is set to:

`%programfiles%\1E\Client\`

But you can browse to a new folder using the **Change...** button.

Once the desired folder has been set you click the **Next** button to continue to the next screen.



2.3.1.3.4 Tachyon

On this screen you configure how the 1E Client connects with the Tachyon platform. If you are installing the 1E Client only to support Nomad, Shopping or WakeUp and do not have the Tachyon platform installed, uncheck the **Enable Tachyon** checkbox and click **Next**.

Setting	Description
Enable Tachyon	Check this box to enable Tachyon.
Switch	Sets the name and port of the server where the Tachyon Switch is located. The default port is 4000.

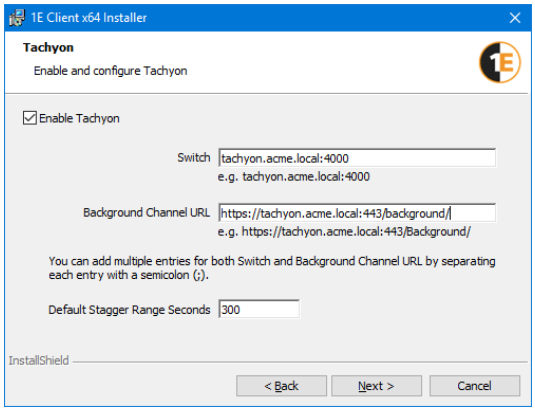
Setting	Description

	If Tachyon and Nomad client features are not required then the connection to Tachyon platform is not required, and both **Switch** and **BackgroundChannelUrl** settings must be set to **none** when doing a non-interactive (silent/quiet) install using installer properties on a command-line or in a MST transform file. When doing an interactive install then you must uncheck the **Enable Tachyon** checkbox.
	
	Client features are not required if the 1E Client is being installed only to support PXE Everwhere, Shopping, or WakeUp. They are only required for Nomad if using Nomad features of the Tachyon platform.
	
	To connect to the Tachyon platform then **Switch** will have one or more entries in the format:
	
	`Switch=<SwitchName>:<SwitchPort>`
	
	<SwitchName> is the DNS Name FQDN for one or more Switches. This is the same as the following except in a custom configuration where the Switch is installed on its own:
	
	• HTTPS Host Header specified on the *Website Configuration* screen of the Tachyon Server installer, which is the HTTPS binding for the Tachyon Web Site
	
	• Same as <BackgroundChannelServer>
	
	• DNS Name specified in the Tachyon Server's Web Certificate.
	
	<SwitchPort> is the Port number, which has default value of 4000. Any other port number is used only in a complex configuration if advised by 1E.
	
	In systems where there are multiple DNS Names, there will be multiple entries using a semi-colon (;) as the delimiter between entries. For example:
	
	`Switch=tachyon.acme.local:4000;tachyon.acme.com:4000`

Background Channel URL	Sets the fully qualified URL that the 1E Client will use to connect to the Tachyon background channel used to transfer large content. If the Tachyon server has been installed to use a

Setting	Description
	custom port for the background channel, the port number must be specified in the URL, for example https://tachyon.acme.local:8443/Background. If Tachyon and Nomad client features are not required then the connection to Tachyon platform is not required, and both **Switch** and **BackgroundChannelUrl** settings must be set to **none** when doing a non-interactive (silent/quiet) install using installer properties on a command-line or in a MST transform file. When doing an interactive install then you must uncheck the **Enable Tachyon** checkbox. Client features are not required if the 1E Client is being installed only to support PXE Everwhere, Shopping, or WakeUp. They are only required for Nomad if using Nomad features of the Tachyon platform. To connect to the platform then **BackgroundChannelUrl** will have one or more entries in the format: `BackgroundChannelUrl=https://<BackgroundChannelServer>:<BackgroundChannelPort>/Background/` **<BackgroundChannelServer>** is the DNS Name FQDN of the server, which is the same as the: • HTTPS Host Header specified on the *Website Configuration* screen of Tachyon Setup, which is the HTTPS binding for the Tachyon website • Same as <SwitchName> • DNS Name specified in the Tachyon Server's Web Certificate. **<BackgroundChannelPort>** is the Port number, which is the same as: • The HTTPS Port specified on the *Website Configuration* screen of Tachyon Setup, which is the HTTPS binding for the Tachyon website • If using the default HTTPS port 443, the port can be omitted from the URL.

Setting	Description
	In systems with multiple server and multiple DNS Names, there will be multiple entries on one line using a semi-colon (;) as the delimiter between entries. For example: `BackgroundChannelUrl=https://tachyon.acme.local:443/Background/;https://tachyon.acme.com:443/Background/`
Default Stagger Range Seconds	Sets the scope for the random delay used by the 1E Client to prevent overburdening the Tachyon Background Channel. Some operations (including HTTPS downloads from the BackgroundChannel) are randomly time-staggered across Tachyon platform clients. This property dictates the upper-limit on the default randomization period in seconds. Range is 0 to 3600. Default is 300. Use **0** to instruct Tachyon platform client not stagger operations by default. **Note** Do not change this value unless advised by 1E. Only use 0 or a low value in systems that support less than 500 clients. **Note** **Note** This setting is not used for HTTPS downloads from the BackgroundChannel if NomadContentDownloadEnabled is **true**, because Nomad does the bandwidth management.



2.3.1.3.5 Nomad

When using Nomad with Configuration Manager you must enable Nomad on Configuration Manager clients and Distribution Points. The 1E Client Nomad module replaces the NomadBranch client from previous versions of Nomad. You can also use the Nomad client with Tachyon to improve the efficiency of content downloads.

Setting	Description
Enable Nomad	Check this box to enable Nomad. Nomad is used to support efficient content download for Configuration Manager and Tachyon. For Tachyon, its Nomad content download feature is enabled by default but only used if Nomad is enabled. **Note** If Nomad is enabled, when the 1E Client starts it will upgrade any previous installation of the NomadBranch client.
Enable 1E Platform features	Check this box to let you configure the Single-Site Download (SSD) options and WakeUp integration.

Options	Enabled
Content Registration only	This configures Nomad to use **Single Site Download** to *provide* content to peers by registering the content it has in its cache in Content Distribution on the Tachyon platform. In the registry SSDEnabled is set to 2 and ContentRegistration is set to 1. This also allows content to be reported in Nomad app dashboards and Device View. Typically, content registration should be enabled, unless there is a specific reason for a computer not to be a master. Content Registration is automatically disabled in WinPE.

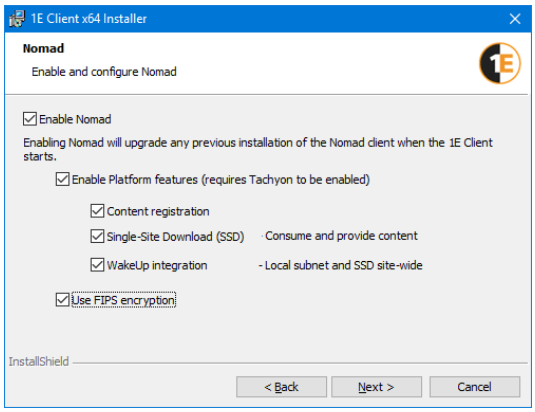
Setting	Description	
	Single-Site Download (SSD) only	This configures Nomad to use **Single Site Download** and *consume* content hat has been registered in Nomad on the Tachyon platform. SSD is used as a fallback if the client is unable to find content on the local subnet. In the registry SSDEnabled is set to 1 and ContentRegistration is set to 1. Nomad queries Nomad on the Tachyon platform asking for peers that have registered content.
	Both enabled	This configures Nomad to use **Single Site Download** so that it can both *consume and provide* content, as well as report in the Nomad app and Device View. In the registry, SSDEnabled is set to 3 and ContentRegistration is set to 1. This is the recommended configuration unless there is a specific reason for a computer not to be a master. Content Registration is automatically disabled in WinPE.
	Neither enabled	The client does not participate in **Single Site Download** activities and does not report content details to Nomad. In the registry, SSDEnabled is set to 0 and ContentRegistration is set to 0. **Enable 1E Platform features** has no effect, and is ignored.

Setting	Description
	If you need to enable reporting but prevent the Nomad client from acting as an SSD provider, then use installer properties or mst transform files to configure MODULE.NOMAD.SSDENABLED and MODULE.NOMAD.CONTENTREGISTRATION. For more information about SSD, please refer to Single Site Download (SSD). **Options** / **Enabled** **WakeUp integration** — If you check **WakeUp integration** but not **Single Site Download (SSD)**, any attempt to wake-up peers with particular content will only be on the local subnet. If **Single Site Download (SSD)** is also checked, Nomad will try to wake peers with particular content in neighboring subnets on the site if peers on the local subnet do not wake. **Note** The Platform settings are only available if you have enabled Tachyon. **Note** These settings do not affect other Platform features such as Pre-caching.
Use FIPS encryption	Checking to **Use FIPS Encryption** configures the Nomad module to use FIPS-encrypted encrypted communications. You must ensure that Nomad is configured with the same **FIPS encryption** setting on all your 1E Client.

Tip

If you are licensed to use Nomad, you should enable it if you have enabled Tachyon, so that Tachyon can take advantage of its content download features that intelligently manage bandwidth and use its peers when downloading content from Tachyon Background Channel and other HTTP/S sources.

You do not require Configuration Manager in order for Tachyon to use Nomad. For more information on this feature, please refer to Downloading client content and Nomad integration.

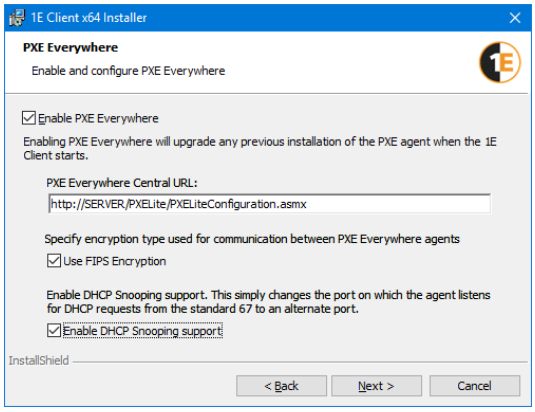


2.3.1.3.6 PXE Everywhere

If you are using PXE Everywhere 4.0, 8.0, 8.1 8.1 or later, you must enable PXE Everywhere. The 1E ClientPXE Everywhere Agent client module of the replaces the PXE Everywhere Agent from previous versions of PXE Everywhere.

Setting	Description
Enable PXE Everywhere	Check this box to enable PXE Everywhere Agent client module. **Note** If enabled, when the 1E Client starts it will attempt to automatically remove any previous installations of PXE Everywhere Agent. Other fields are only enabled if this checkbox is checked.
PXE Everywhere Central URL	URL for the PXE Everywhere Central web service in the format: *http://SERVER/PXELite/PXELiteConfiguration.asmx* where *<SERVER>* is the name of the server (or FQDN) where the PXE Everywhere Central web service is installed. **Note** The http prefix to the URL is case-sensitive and must be entered in all lower case letters. The URL is not verified by the installer, so you will need to ensure that the correct URL is entered.

Setting	Description
Use FIPS Encryption	Checking to **Use FIPS Encryption** configures the PXE Everywhere Agent module to use FIPS encrypted communications. You must ensure that PXE Everywhere is configured with the same **FIPS encryption** setting on all your 1E Client.
Enable DHCP Snooping support	Enable this option if your network uses DHCP Snooping. You will also need to implement one or more PXE Everywhere Responders as described in Design Considerations.



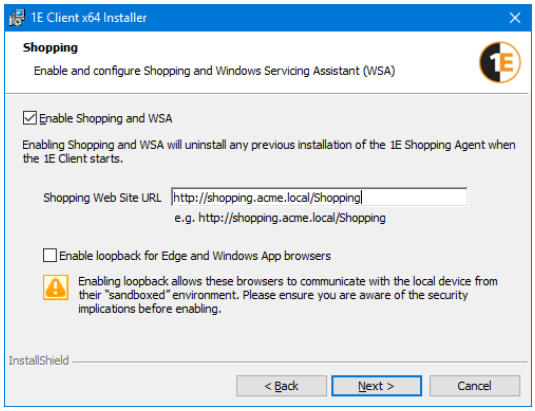
2.3.1.3.7 Shopping

If you are using Shopping 6.0 or later, you must enable Shopping. The 1E Client Shopping module replaces the Shopping Agent from previous versions of Shopping.

Setting	Description
Enable Shopping and WSA	Check this box to enable Shopping Integration and the Windows Servicing Assistant. Shopping must be enabled so that users of a computer can use the 1E Shopping self-service portal, the Windows Servicing Assistant, and the 1E Virtual Assistant. **Note** If enabled, when the 1E Client starts it will attempt to automatically remove any previous installations of the 1E Shopping Agent.

Setting	Description
Shopping Web Site URL	This field is only enabled if the **Enable Shopping and WSA** checkbox is checked. Example: *https://shopping.acme.local/Shopping* This is the URL of the Shopping Central website, comprising: • **scheme** - either http or https • **host header** - DNS Name FQDN - this is the host header configured for the Shopping website, which is normally a DNS Name FQDN • **port number** - you do not have to provide this if using default port 80 or 443 • **path** - this is always /Shopping. The URL is not verified by the installer, so you will need to ensure that the correct URL is entered.
Enable loopback for Edge and Windows App b rowsers	Enable this option if users will connect to the Shopping website using Edge or other Metro-style browsers. When users connect to the Shopping Portal, the website needs to get the latest details about the local computer. Shopping may already have details from the Configuration Manager database, but these need to be confirmed and updated. Browser standards only allow websites to get limited information about the user and computer, therefore the website needs to make loopback calls to the local computer via the Shopping client. The following browsers permit loopback calls by default:

Setting	Description
	• All versions of Chrome • All versions of Firefox • Non-Metro UI based Internet Explorer browsers (including legacy Internet Explorer). If your Shopping users are using **Edge** and **Metro Internet Explorer** browsers, you must enable a **Loopback Exemption** to allow these browsers to make loopback calls. Exemption affects the browser as a whole and is not just restricted to the Shopping website. Before enabling this option, check your corporate security policy and be aware of the implications of allowing access between browsers and the local machine. By enabling loopback, you are only setting the Edge/Metro Internet Explorer browsers to the same level of security as other browsers which allow this setting already. If you are running an unattended install, you can use **MODULE.SHOPPING.LOOPBACKEXEMPTIONENABLED** for all OS but it only works on Windows 8, 8.1, 10 and Windows Server 2012 R2 and later. Shopping client only allows inbound connections to **localhost (127.0.0.1)** which prevents remote access.



2.3.1.3.8 WakeUp

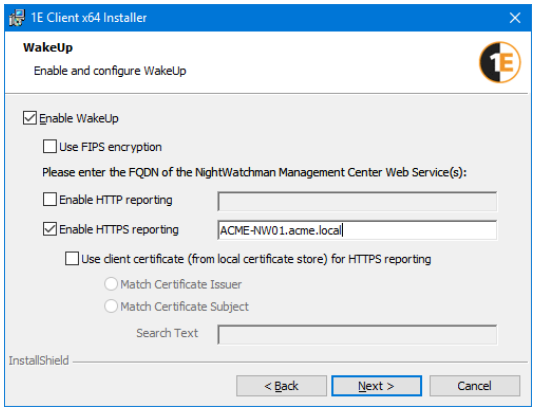
If you are using version 7.2.500 or later of NightWatchman Management Center or WakeUp Server you must install the 1E Client with this option enabled on client devices and on WakeUp server. The 1E Client WakeUp module replaces the WakeUp Agent from previous versions of the 1E Agent.

Setting	Description
Enable WakeUp	Check this box to enable WakeUp integration. WakeUp integration is required to enable 1E WakeUp capabilities on this device. **Note** If WakeUp Integration is enabled, when the 1E Client starts it will attempt to automatically remove any previous installation of the 1E WakeUp Agent. The 1E NightWatchman Agent is not affected.
Use FIPS encryption	Checking **Use FIPS Encryption** configures the WakeUp module to use FIPS encrypted communications. You must ensure that the NightWatchman Management Center, WakeUp Server and 1E NightWatchman Agent

Setting	Description
	components are all set to the same option.
Enable HTTP reporting	Check this box if the NightWatchman Management Center Web Service is configured to use HTTP and you want communications from the WakeUp module to use HTTP. Do not use this option when installing on a WakeUp Server. When checked you must set the DNS Name FQDN for the server hosting the NightWatchman Management Center Web Service in the edit field provided.
Enable HTTPS reporting	Check this box if the NightWatchman Management Center Web Service is configured to use HTTPS and you want communications from the WakeUp module to use HTTPS. Do not use this option when installing on a WakeUp Server. When checked you must set the DNS Name FQDN for the server hosting the NightWatchman Management Center Web Service in the edit field provided.
Use client certificate (from local certificate store) for HTTPS reporting	This checkbox is only enabled when the **Enable HTTPS reporting** checkbox is checked. You will need to check this option if the NightWatchman Management Center Web Service has been configured to request a client certificate.

Setting	Description
	The certificate is retrieved from the local certificate store and is found by providing a certificate issuer or certificate subject search text. The first certificate found that matches the text will be used to authenticate the client with the NightWatchman Management Center Web Service.
Match Certificate Issuer	This option is only enabled when the **Use client certificate for HTTPS reporting** checkbox is checked. When selected this option sets the search in the local certificate store to match against the certificate issuer field of the certificate.
Match Certificate Subject	This option is only enabled when the **Use client certificate for HTTPS reporting** checkbox is checked. When selected this option sets the search in the local certificate store to match against the certificate subject field of the certificate.
Search Text	This option is only enabled when the **Use client certificate for HTTPS reporting** checkbox is checked. When enabled this edit field should be set to the search text used to locate and retrieve the client certificate from the local certificate store. This will be matched against either the certificate issuer or the certificate

Setting	Description
	subject, depending on which option has been selected above.



Note

When installing on client devices, enable HTTP or HTTPS reporting in order for NightWatchman Management Center to track which subnet the client device is on when it powers down. The WakeUp module reports back subnet changes more frequently than the NightWatchman Agent.

WakeUp Server must be installed before installation of the WakeUp client. If WakeUp client is installed first the WakeUp Server installer only provides the WakeUp Administration console installation option.

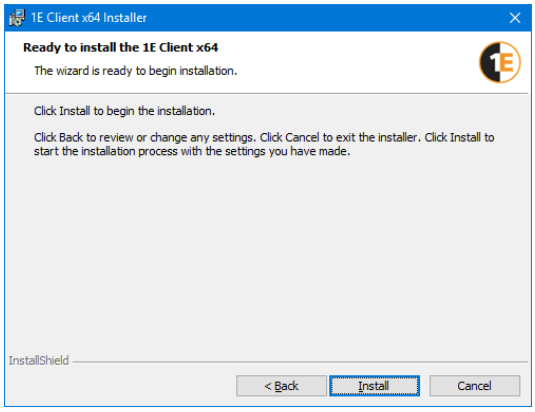
When installing on a WakeUp Server, do **not** enable HTTP or HTTPS reporting, because that prevents the server from appearing as a client in the NightWatchman Management Center Admin Console. This will only disable Agent reporting whilst the WakeUp Server itself should have reporting enabled for reporting statistics.

Warning

Enter the DNS Name FQDN for the server hosting the NightWatchman Management Center Web Service, do not enter the full URL.

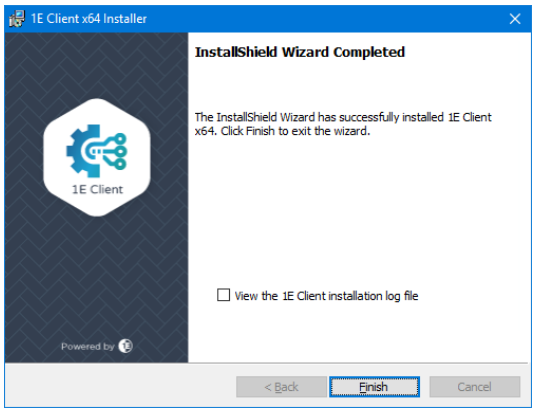
2.3.1.3.9 Ready to Install the 1E Client

Once you have finished entering all the settings, you can begin the installation by clicking on the **Install** button on this screen.



2.3.1.3.10 InstallShield Wizard Completed

After the attempted installation the **InstallShield Wizard Completed** screen will display the results and give you the option to **View the 1E Client installation log file**. To exit the installer click the **Finish** button.



2.3.1.4 Installing the 1E Client by command-line

In most cases the 1E Client will be installed in quiet mode from the command line using a software deployment tool such as Configuration Manager.

Because the expected length of the 1E Client installer command line is likely to exceed the limit imposed by Configuration Manager you will need to use MST transform file(s) for this to work. Please contact your packaging team if you need help creating transform files.

The Introducing 1E Client Deployment Assistant is designed to help install Windows versions of 1E Client and other 1E agents using Configuration Manager. It includes template transform files for each combination of client/agent for 32 and 64-bit platforms, and automatically creates collections and deployments in Configuration Manager so that you only need to populate the collections.

The installer properties listed on this page are for the options visible in the interactive installer above:

- 1E Client - common settings
- Tachyon platform client
- Nomad client

- PXE Everywhere Agent
- Shopping client
- WakeUp client.

Additional installer properties are available for:

- Platform features of the 1E Client
- Content Distribution client settings
- /document/preview/647626#UUID-07a4d117-b2a9-8325-0e8e-1d3649997dc4
- Shopping client settings
- Wakeup client settings.

Some Command-line examples are also provided below.

2.3.1.4.1 1E Client

The following are common settings for the 1E Client.

Installer property	Description
INSTALLDIR	Sets the installation folder. This value is not stored in the 1E Client configuration file. This value is stored as **InstallationDirectory** in the Windows registry under HKLM\SOFTWARE\1E\Client\ and must not be changed. Some client modules that run on Windows store their registry settings under their own keys in HKLM\SOFTWARE\1E. **Note** This installer property is for Windows only.

2.3.1.4.2 Tachyon platform client

When installing the full 1E Client (to be used with the Tachyon platform), the following are typical installer properties to use. Additional installer properties are described on the Platform features of the 1E Client page.

As with other Windows installers, uninstallation will leave behind any files, folders and registry entries that were created after installation.

Installer property	Description

BACKGROUNDCHANNELURL	If Tachyon platform and Nomad client features are not required then the connection to Tachyon Platform is not required, and both **Switch** and **BackgroundChannelUrl** settings must be set to **none** when doing a non-interactive (silent/quiet) install using installer properties on a command-line or in a MST transform file. When doing an interactive install then you must uncheck the **Enable Tachyon** checkbox.
	
	Tachyon client features are not required if the 1E Client is being installed only to support PXE Everwhere, Shopping, or WakeUp. They are only required for Nomad if using Nomad features of the Tachyon platform.
	
	To connect to the Tachyon platform then **BackgroundChannelUrl** will have one or more entries in the format:
	
	`BackgroundChannelUrl=https://<BackgroundChannelServer>:<BackgroundChannelPort>/Background/`
	
	<BackgroundChannelServer> is the DNS Name FQDN of the server, which is the same as:
	
	• the HTTPS Host Header specified on the *Website Configuration* screen of Tachyon Setup, which is the HTTPS binding for the Tachyon website
	
	• the same as <SwitchName>, refer to #UUID24ef0cf654c33163e98e9dc427464c32_id_Deploying1EClientonWindowsSWITCHSWITCH for details
	
	• the DNS Name specified in the Tachyon Server's Web Certificate.
	
	<BackgroundChannelPort> is the Port number, which is the same as:
	
	• the HTTPS Port specified on the *Website Configuration* screen of Tachyon Setup, which is the HTTPS binding for the Tachyon website
	
	• if using the default HTTPS port 443, the port can be omitted from the URL.
	
	In systems with multiple server and multiple DNS Names, there will be multiple entries on one line using a semi-colon (;) as the delimiter between entries. For example:
	
	`BackgroundChannelUrl=https://tachyon.acme.local:443/Background/;https://tachyon.acme.com:443/Background/`

Installer property	Description

SWITCH	If Tachyon and Nomad client features are not required then the connection to Tachyon platform is not required, and both **Switch** and **BackgroundChannelUrl** settings must be set to **none** when doing a non-interactive (silent/quiet) install using installer properties on a command-line or in a MST transform file. When doing an interactive install then you must uncheck the **Enable Tachyon** checkbox.
	
	Tachyon platform client features are not required if the 1E Client is being installed only to support PXE Everwhere, Shopping, or WakeUp. They are only required for Nomad if using Nomad features of the platform.
	
	To connect to the Tachyon platform then **Switch** will have one or more entries in the format:
	
	`Switch=<SwitchName>:<SwitchPort>`
	
	<SwitchName> is the DNS Name FQDN for one or more Switches. This is the same as the following except in a custom configuration where the Switch is installed on its own:
	
	• the HTTPS Host Header specified on the *Website Configuration* screen of the Tachyon Server installer, which is the HTTPS binding for the Tachyon Web Site
	
	• the same as <BackgroundChannelServer>, refer to #UUID24ef0cf654c33163e98e9dc427464c32_id_Deploying1EClientonWindowsBACKGROUNDCHANNELURLBACKGROUNDCHANNELURL for details
	
	• the DNS Name specified in the Tachyon Server's Web Certificate.
	
	<SwitchPort> is the Port number, which has default value of 4000. Any other port number is used only in a complex configuration if advised by 1E.
	
	In systems where there are multiple DNS Names, there will be multiple entries using a semi-colon (;) as the delimiter between entries. For example:
	
	`Switch=tachyon.acme.local:4000;tachyon.acme.com:4000`

DEFAULTSTAGGERRANGESECONDS	Some operations (including HTTPS downloads from the BackgroundChannel) are randomly time-staggered across Tachyon clients. This property dictates the upper limit on the default randomization period in seconds.

Installer property	Description
	Range is 0 to 3600. Default is 300. Use **0** to instruct Tachyon client not stagger operations by default. **Note** Do not change this value unless advised by 1E. Only use 0 or a low value in systems that support less than 500 clients. **Note** **Note** This setting is not used for HTTPS downloads from the BackgroundChannel if NomadContentDownloadEnabled is **true**, because Nomad does the bandwidth management.

Note

The BACKGROUNDCHANNELURL and SWITCH properties are mandatory. If you want to install the 1E Client with the 1E Client modules for Shopping or WakeUp enabled, and the full Tachyon platform infrastructure has not been installed, you should set both of these properties to **none**.

However, note that during an upgrade of **Tachyon Agent**, you must enable the connection to the Tachyon platform, therefore you must define the BACKGROUNDCHANNELURL and SWITCH properties.

Disabling the connection to the Tachyon platform is presently only possible for new installations of the 1E Client. If you wish to disable the connection following an upgrade, you must reconfigure the 1E Client once the upgrade has been completed. For more detail please refer to Reconfiguring 1E Client after installation.

2.3.1.4.3 Nomad client

When installing the 1E Client to support Nomad 7.0 or later, the following installer properties are available. Additional installer properties are described on the Content Distribution client settings page.

As with other Windows installers, uninstallation will leave behind any files, folders and registry entries that were created after installation.

Installer property	Description
MODULE.NOMAD.ENABLED	Nomad is used to support efficient content download for Configuration Manager and Tachyon. For Tachyon, the Nomad content download feature is enabled by default.

Installer property	Description
	Note If Nomad is enabled, when the 1E Client starts it will upgrade any previous installation of the NomadBranch client.
MODULE.NOMAD.PLATFORMURL	This installer property is no longer supported. The Nomad installer determines the location of servers from the platform client. Specifically, it communicates with Response Stack Switches and Background Channel.
MODULE.NOMAD.CONTENTREGISTRATION	Set to 1 to enable the Nomad client to act as a content provider across subnets when using **Single Site Download**.
MODULE.NOMAD.SSDENABLED	Set to 1 to enable **Single-site download**, which requires Tachyon platform with Nomad. If you enable both **Single-Site Download** and **Content Registration** then Nomad will make its own content available to other Nomad peers. If you enable **Single-Site Download** but not **Content Registration** then Nomad will be able to fetch downloads from registered peers on other subnets but will not make its own content available.
MODULE.NOMAD.WAKEUPENABLED	Set to 1 to enable **WakeUp integration**, which requires an ActiveEfficiency Server. If you enable **WakeUp integration** but not **Single Site Download**, any attempt to wake-up peers with particular content will only be on the local subnet. If **Single Site Download** is also checked, Nomad will try to wake peers with particular content in neighboring subnets on the site if peers on the local subnet do not wake.
MODULE.NOMAD.USEFIPS	Set to 1 to configure the Nomad module to use FIPS encrypted communications.

Installer property	Description
	You must ensure that Nomad is configured with the same **FIPS encryption** setting on all your 1E Client.

Note

Previous versions of Nomad required a license key (installer property PIDKEY). 1E Client and the Nomad client module do not require a license key. Even so, you must adhere to the terms of your license agreement.

2.3.1.4.4 PXE Everywhere Agent

When installing the 1E Client to support PXE Everywhere 8.1 or later, the following installer properties are available.

Installer property	Description
MODULE.PXEEVERYWHERE.ENABLED	Set this property to **true** to enable the PXE Everywhere Agent client module. The default value is false. **Note** If enabled, when the 1E Client starts it will attempt to automatically remove any previous installations of PXE Everywhere Agent.
MODULE.PXEEVERYWHERE.CONFIGSERVERURL	URL for the PXE Everywhere Central web service in the format: *http://SERVER/PXELite/PXELiteConfiguration.asmx* where *<SERVER>* is the name of the server (or FQDN) where the PXE Everywhere Central web service is installed. **Note** The http prefix to the URL is case-sensitive and must be entered in all lower case letters. The URL is not verified by the installer, so you will need to ensure that the correct URL is entered.
MODULE.PXEEVERYWHERE.USEFIPS	You must use the same FIPS encryption setting on all PXE Everywhere Agents. Use of FIPS compliant encryption for communications. • 0 – use default encryption

Installer property	Description
	• 1 – use FIPS encryption.
MODULE.PXEEVERYWHERE.DHCPPORT	This installer property is set to 2067 if **Enable DHCP Snooping support** is checked during an interactive installation of the 1E Client installer. This is the UDP port on which the PXE Everywhere Agent will listen for PXE requests. If DHCP Snooping is not being used, then this port must be 67 (default), and you do not need to install Responders. When manually installing the PXE Everywhere Agent, if the DHCP Snooping option is enabled in the installer UI, the default port is changed from 67 (43 hex) to 2067 (813 hex). If the MODULE.PXEEVERYWHERE.DHCPPORT installer property is used to specify a port other than 67, the installer UI assumes the DHCP Snooping option is enabled. If DHCP Snooping is being used, then DhcpPort on Agents must be the same value as AltPxeServerPort on Responders. The default value of AltPxeServerPort is 2067. If a value other than 2067 is specified as a custom port number on Agents, you will also need to manually create the AltPxeServerPort (and AltPxeClientPort) registry values on Responders, refer to #UUIDc24be1a07329bf137cee4da9b75a3a1a_id_PXEEverywhereRespondersettingsAltPxeClientPort.

2.3.1.4.5 Shopping client

When installing the 1E Client to support Shopping v5.5 or later, the following installer properties are available.

Installer property	Description
MODULE.SHOPPING.ENABLED	Shopping must be enabled so that users of a computer can use the 1E Shopping self-service portal, the Windows Servicing Assistant, and the 1E Virtual Assistant. **Note** If enabled, when the 1E Client starts it will attempt to

Installer property	Description
	automatically remove any previous installations of the 1E Shopping Agent.
MODULE.SHOPPING.SHOPPINGCENTRALURL	Example: *https://shopping.acme.local/Shopping* This is the URL of the Shopping Central website, comprising: • **scheme** - either http or https • **host header** - DNS Name FQDN - this is the host header configured for the Shopping website, which is normally a DNS Name FQDN • **port number** - you do not have to provide this if using default port 80 or 443 • **path** - this is always /Shopping.
MODULE.SHOPPING.LOOPBACKEXEMPTIONENABLED	Optional. Default value is **false**. Set this value to **true** if users are likely to use Microsoft Edge or other Metro browsers to access the Shopping website. The Shopping client requests this value from the Shopping Central website (admin console setting: Loopback exemption enabled). If the client fails to connect to the website, it defaults to using this local setting and retries later.

2.3.1.4.6 WakeUp client

When installing the 1E Client to support the WakeUp component of NightWatchman Enterprise v7.3 or later, the following are typical installer properties to use. Additional installer properties are described on the /document/preview/647736#UUID-b588cdab-ae07-3331-ceb1-c8c6ed63aa1e page.

Installer property	Description
MODULE.WAKEUP.ENABLED	Set this property to **true** to enable the WakeUp client module. The default value is **false**. Enabling this will also cause any installation of the 1E Agent's WakeUp component to be uninstalled the first time the 1E Client is started, leaving the NightWatchman component if that was installed. **Note** When **true** then you must also specify either the name of the NightWatchman Management Center reporting server, or that reporting is turned off. For details of these and all other installer properties please refer to /document/preview/647736#UUID-b588cdab-ae07-3331-ceb1-c8c6ed63aa1e.
MODULE.WAKEUP.USEFIPS	Set to **1** to force the WakeUp agent to use a FIPS-compliant algorithm for: • WakeUp Reporting to the **NightWatchman Management Center Web Service** by setting **UseFipsComplianceEncryption** registry value to 1. • Communication between WakeUp Agents and WakeUp Servers. It will override the MODULE.WAKEUP.ENCRYPTIONLEVEL installer property and set the **EncryptionLevel** registry value to 3. If enabled, then all components in the NightWatchman and WakeUp system must have FIPS enabled. EncryptionLevel and FIPS settings used by WakeUp do not affect other 1E Client communications.
MODULE.WAKEUP.REPORTING	Enables WakeUp reporting. Sets whether the Agent sends reporting messages to the **NightWatchman Management Center Web Service**. May be set to one of the following values: • **ON** – reporting is enabled and messages are forwarded to the NightWatchman server. It is mandatory to specify one of the following:

Installer property	Description
	MODULE.WAKEUP.REPORTINGSERVER or MODULE.WAKEUP.SECUREREPORTINGSERVER • **OFF** – no information is reported to the server. **Tip** When installing the 1E Client on a WakeUp Server, set **MODULE.WAKEUP.REPORTING=OFF** so that the server does not appear as a client in the NightWatchman Management Center Admin Console. This will only disable Agent reporting whilst the WakeUp Server will have reporting enabled for reporting statistics.
MODULE.WAKEUP.REPORTINGSERVER	Set this parameter to the FQDN (recommended) or NetBIOS name of the server hosting the NightWatchman Management Center Web Service. **Warning** Mandatory when WakeUp reporting is enabled (default) and using **HTTP** for communications. **Tip** If **HTTP** is not using standard port 80 then specify the port number as part of the server name: MODULE.WAKEUP.REPORTINGSERVER="ACMESERVER.ACME.COM:8080"
MODULE.WAKEUP.SECUREREPORTINGSERVER	Set this parameter to the FQDN (*required*) or NetBIOS name of the server where the NightWatchman Management Center Web Service component secure site has been installed. **Warning** Mandatory when WakeUp reporting is enabled (default) and using **HTTPS** for communications. **Tip** If **HTTPS** is not using standard port 443 then specify the port number as part of the server name: MODULE.WAKEUP.SECUREREPORTINGSERVER="ACMESERVER.ACME.COM:7433"

Installer property	Description
MODULE.WAKEUP.CERTISSUER	Specify the text used to search for a client certificate in the client certificate store. Either MODULE.WAKEUP.CERTISSUER or MODULE.WAKEUP.CERTSUBJECT is mandatory when all the following are true: • **HTTPS** communications is being used • MODULE.WAKEUP.SECUREREPORTINGSERVER is configured • SSL Settings for the **NightWatchman Management Center Web Service** is configured to require a client certificate. If this property is used, it will use the first certificate it finds where the specified text matches the certificate's Issuer CN.
MODULE.WAKEUP.CERTSUBJECT	Specify the text used to search for a client certificate in the client certificate store. Either MODULE.WAKEUP.CERTISSUER or MODULE.WAKEUP.CERTSUBJECT is mandatory when all the following are true: • **HTTPS** communications is being used • MODULE.WAKEUP.SECUREREPORTINGSERVER is configured • SSL Settings for the **NightWatchman Management Center Web Service** is configured to require a client certificate. If this property is used, it will use the first certificate it finds where the specified text matches the certificate's Subject CN.

2.3.1.4.7 Command-line examples

When installing 1E Client, you should include **/l*vx** for verbose logging to a log file. The following examples also use **/qn** for a non-interactive (silent/quiet) installation.

2.3.1.4.7.1 Example command-line using a MST transform file

```
msiexec /i 1E.Client-x64.msi TRANSFORMS="1EClient.mst" /qn /l*vx C:\Windows\temp\1EClient-install.log
```

An MST typically only works with a specific version of an MSI, therefore you should test before using an old MST file. An MST may work with both 32 and 64-bit versions of an MSI, provided the MST does not contain any transforms that are platform-specific. Please contact your packaging team if you need help creating transform files.

The Introducing 1E Client Deployment Assistant is designed to help install Windows versions of 1E Client and other 1E agents using Configuration Manager. It includes template transform files for each combination of client/agent for 32 and 64-bit platforms and automatically creates collections and deployments in Configuration Manager so that you only need to populate the collections.

2.3.1.4.7.2 Example which enables only Tachyon client

Example Windows 1E Client installer command-line with only the 1E Client features enabled, other client modules are not enabled. Tachyon uses HTTPS only.

```
msiexec /i 1E.Client-x64.msi SWITCH="tachyon.acme.local:4000" BACKGROUNDCHANNELURL="https://tachyon.acme.local:443/Background/" /qn /l*vx C:\Windows\temp\1EClient-install.log
```

2.3.1.4.7.3 Example which enables only Nomad client

Example Windows 1E Client installer command-line with only **Nomad** module enabled, which also requires Tachyon client features to be enabled. Tachyon uses HTTPS only.

```
msiexec /i 1E.Client-x64.msi SWITCH="tachyon.acme.local:4000" BACKGROUNDCHANNELURL="https://tachyon.acme.local:443/Background/" MODULE.NOMAD.ENABLED=true MODULE.NOMAD.CONTENTREGISTRATION=1 MODULE.NOMAD.SSDENABLED=1 /qn /l*vx C:\Windows\temp\1EClient-install.log
```

2.3.1.4.7.4 Example which enables only PXE Everywhere Agent

Example Windows 1E Client installer command-line with only **PXE Everywhere Agent** client module enabled, and Tachyon features disabled (by setting SWITCH and BACKGROUNDCHANNELURL to none). PXE Everywhere uses only HTTP.

```
msiexec /i 1E.Client-x64.msi SWITCH=none BACKGROUNDCHANNELURL=none MODULE.PXEEVERYWHERE.ENABLED=true MODULE.PXEEVERYWHERE.CONFIGSERVERURL="http://pxecentral.acme.local/PXELite/PXELiteConfiguration.asmx" /qn /l*vx C:\Windows\temp\1EClient-install.log
```

2.3.1.4.7.5 Example which enables only Shopping client

Example Windows 1E Client installer command-line with only **Shopping client** module enabled, and Tachyon features disabled (by setting SWITCH and BACKGROUNDCHANNELURL to none). Ensure you use HTTP or HTTPS as appropriate.

```
msiexec /i 1E.Client-x64.msi SWITCH=none BACKGROUNDCHANNELURL=none MODULE.SHOPPING.ENABLED=true MODULE.SHOPPING.SHOPPINGCENTRALURL="https://appstore.acme.loca
```

```
l/shopping" MODULE.SHOPPING.LOOPBACKEXEMPTIONENABLED=true /qn /l*vx C:\Windows\
temp\1EClient-install.log
```

2.3.1.4.7.6 Example which enables only WakeUp client

Example Windows 1E Client installer command-line with only **WakeUp client** module enabled, and Tachyon features disabled (by setting SWITCH and BACKGROUNDCHANNELURL to none).

```
msiexec /i 1E.Client-x64.msi SWITCH=none BACKGROUNDCHANNELURL=none MODULE.WAKEU
P.ENABLED=true MODULE.WAKEUP.REPORTINGSERVER="nwmserver.acme.local" /qn /l*vx C
:\Windows\temp\1EClient-install.log
```

2.3.1.5 Sysprep and OS images

The following steps are required if the 1E Client will be included in an OS image.

1. Stop the 1E Client service.
2. Stop the NomadBranch service (if Nomad is enabled).
3. Delete the logs folder and its contents. Default is **%ALLUSERSPROFILE%\1E\Client**
4. Delete the registry key and its contents **HKLM\SOFTWARE\1E\Client**
5. Delete the registry key and its contents **HKLM\SOFTWARE\1E\Common**
6. Other registry keys for clients may exist. Please refer to their product documentation for details of sysprepping them.
   - HKLM\SOFTWARE\1E\NightWatchman
   - HKLM\SOFTWARE\1E\NomadBranch
   - HKLM\SOFTWARE\1E\PXEEverywhere
   - HKLM\SOFTWARE\1E\WakeUpAgt
   - HKLM\SOFTWARE\1E\WSA

You can disable the services during image preparation and re-enable it as an OS Deployment step. The folder and registry keys will be automatically re-created when the services are restarted after the OS is deployed.

> **Note**
>
> By default, the OS resolves %ALLUSERSPROFILE% to **C:\ProgramData**

If you have 1E WakeUp client module enabled, or 1E NightWatchman Agent installed, then please refer to Installing the 1E NightWatchman Agent for Windows: The 1E NightWatchman Agent, Sysprep and diskimaging.

2.3.1.6 Uninstalling 1E Client

2.3.1.6.1 Manual uninstallation

1E Client can be uninstalled manually by using Windows Apps and Features (appwiz.cpl). A reboot is not normally required.

2.3.1.6.2 Disabling a feature or client module

Please refer to Reconfiguring 1E Client for examples of how to use the **-reconfigure** command-line to reconfigure the 1E Client.

2.3.1.6.3 Uninstallation using the Windows Installer

1E Client can be uninstalled automatically by using a Windows Installer command line, where the {product code} is dependent on the version of the 1E Client. The example below also includes switches that prevent prompting and restart and creates a log file.

```
msiexec /x {BF6F5FA9-64C8-4B72-A6B6-14A582BF96B8} /qn /norestart /l*vx C:\Windo
ws\temp\1EClient-uninstall.log
```

2.3.1.6.4 Tidy up after uninstallation

After the uninstallation of 1E Client, the following is left behind. As with other Windows installers, uninstallation will leave behind any files, folders, and registry entries that were created after installation.

Location	Artifacts	Recommendation
Installation folder	None.	
Logs folder	Log files remain. Please refer to Log files for log file locations of 1E Client and its client modules.	The log files can be deleted or renamed. If not deleted, then a new installation that uses the same logs folder will continue to use the old log file.
Client\Persist folder remains.	Leave this folder which contains status information about current instructions. The Persist folder should be deleted only if you do not intend re-installing the 1E Client with Tachyon enabled, or when preparing OS images, refer to Sysprep and OS images for details.	

Location	Artifacts	Recommendation
Tachyon client registry	HKLM\SOFTWARE\1E\Client\Persist	This registry exists if the Tachyon platform client feature of the 1E Client is enabled. It is used to keep a record of hash values for its persistent storage files, which includes status information about current instructions. This registry key should be deleted only if you do not intend re-installing the 1E Client with Tachyon enabled, or when preparing OS images, refer to Sysprep and OS images for details.
Nomad Cache	%ALLUSERSPROFILE%\1E\NomadBranch	The folder should be deleted only if you do not intend re-installing the 1E Client with Nomad enabled. Downloaded content is retained so that if the Nomad client is re-enabled it will be scanned and re-registered, to make it available for peer sharing with other Nomad clients.

Note

HKLM\SOFTWARE\1E\Common and HKLM\SOFTWARE\1E\NightWatchman are used by the 1E NightWatchman Agent, previously part of the 1E Agent.

2.3.2 Deploying 1E Client on macOS

Guidance for deploying 1E Client onto **macOS** devices, including installation and uninstallation. Only the Tachyon features of 1E Client are available on macOS.

2.3.2.1 Requirements

- Please review Planning for 1E Client pages. After installation, please review the Verifying page.
- For details of supported OS platforms, please refer to Common client requirements page.
- Guidance provided below is for installation on macOS.

Note

1E Client does not have a license key. Even so, you must adhere to the terms of your license agreement.

2.3.2.1.1 Deployment choices

You must decide how you will configure the 1E Client and deploy to devices. Deploying the 1E Client is normally achieved using your existing software deployment tool.

Note

For more information about configuring the 1E Client properties during and after installation, please refer to 1E Client configuration settings and installer properties.

2.3.2.1.2 Non-Windows installation account

To install the 1E Client on a non-Windows client the installation account must have privileges to run the **sudo** command.

2.3.2.1.3 Certificate files

Each Tachyon client device requires a **.pfx** certificate file. Please refer to Client certificates for steps to create and use the **.pfx** file.

The 1E Client for macOS needs to have the storage of the client authentication certificate and the public certificates for the chain of trust for the Tachyon Switch.

If you have configured Tachyon Server to require client certificates then each device requires a certificate with the following properties, so the client can be authenticated by the Tachyon Switch.

1. Issued by a trusted Certificate Authority (CA)
   - The certificate for the Root CA in the Certification Path must exist in the Trusted Root CA store of the client
   - If the issuing CA is not the Root CA then the certificate for the issuing CA and any intermediate CA in the Certification Path must exist in the Intermediate CA store of the client
   - If either of these CA certificates is different from those used by the Tachyon Web Server, they will need to be exported and imported on the Tachyon Web Server
   - Most organizations have automated distribution of these CA certificates to clients and servers, using Group Policy for example.
2. Has at least the following Enhanced Key Usage:
   - Client Authentication.

3. Has at least the following Key Usage:
    - Digital Signature
    - Key encipherment.
4. Has a private key:
    - For workgroup and non-Windows devices, the **private key must be exportable**
5. Revocation information is included:
    - References at least one CRL Distribution point that uses HTTP
6. Has a Subject Name of type Common Name (**CN=<computername>**) or Subject Alternative Name (**DNS Name=<computername>**) where <computername> depends on the type of device:
    - On domain-joined Windows PCs this must be the **computername FQDN** of the computer, for example, **W701.ACME.LOCAL**
    - On workgroup Windows PCs and non-Windows devices, this must be the computername of the computer - as returned by the **hostname** command, for example on Windows PC this could be **W701**, and on a Mac this could be **MAC01.local**.

Note

Tachyon clients and Switches use OpenSSL and its validation process to verify certificates.

2.3.2.2 Client certificates

The 1E Client for macOS needs to have the client authentication certificate and the public certificates for the chain of trust for the Tachyon Switch in the System key chain.

First, you need to issue a certificate and create the **.pfx** file.

2.3.2.2.1 Key Store method

The client certificate, and Certificate Authority (CA) certificate(s) for the Switch certificate, are stored within the **macOS Key Store**.

2.3.2.2.1.1 Obtain and import Certificate Authority (CA) certificates

You can skip this step if the Certificate Authority (CA) certificates used by the client and the Switch are the same, and are included in the client certificate.

If the client certificate does not contain the CA certificates for itself, *or* the CA certificates used by the Switch, then the individual CA certificates will need to be obtained and imported into the macOS Key Store as follows:

1. Obtain Certificate Authority (CA) certificates as individual **.cer** files.
    a. They must be exported individually because when presented with a bundle of certificates the Keychain Access UI only imports the last one it encounters.

b. Use Microsoft's Manage Computer Certificates (MMC) to export as a **.cer** file using base-64 encoded X.509 format.

2. Copy the certificate .cer file(s) onto the macOS device.

3. Open Finder and double-click on each .cer file in turn to import each certificate into the macOS Keychain store. Or use File→Import Items... directly from Keychain Access.

4. Open Keychain Access; the certificates should appear under the system keychain.

5. If required, move (by dragging) each newly imported certificate to the System keychain, to ensure that it is trusted by all users and local system processes including the 1E Client which will run on this macOS machine.

6. Starting with the root CA certificate, if it is shown as not trusted, double-click to open. At the top left, above the Details section, expand the Trust section and ensure that When using this certificate Always Trust is selected and save the changes.

If you experience problems importing certificates using the Keychain Access app, for example if it reports error -25294 and *CSSM_CODE_MEMORY_ERROR*, an alternative way of importing public certificates and trusting them is to use the security command line tool. For example:

```
sudo security add-trusted-cert -d -r trustRoot -k /Library/Keychains/System.keychain <certificate.cer>
```

2.3.2.2.1.2 Create a client certificate for each macOS device

Each macOS device requires its own client certificate. Below is a guide for using a Microsoft Certificate Authority (CA) to issue a client certificate, then exporting it ready for installation on the device.

First, create a new Certificate template on your Certificate Authority by making a duplicate of either the Computer or Workstation template and configuring it with at least the following properties:

- General - use a suitable name such as **Tachyon Devices** and validity period.
- Request Handling - Allow private keys to be exported.
- Subject Name - Allow information to be supplied in the certificate request, rather than being built from Active Directory information.
- Extensions - Application Policies should contain only Client Authentication.
- Security - ensure relevant users and computers will be able to request certificates.

Please refer to Client Certificates for more information on client certificate requirements.

Once the new template is created on the Certificate Authority (CA), issue it.

Using the issued template, request a certificate for a target device, and export it in .pfx form and remember the password. The certificate and associated private key should be exported, together with all extended properties, except *include all certificates in the certification path if possible and Enable certificate privacy*.

Warning

The Subject Name of the certificate must be the host name of the mac device. You will supply this value during enrollment. To find the host name of the mac open Finder and click the Apple icon in the upper left. Select System Preferences - Sharing - Screen Sharing. Below the computer name field you will see "Computers on your local network can access your computer at:" this value will be your host name. It must be typed exactly as displayed in the certificate request (case-sensitive and including any special characters).

2.3.2.2.1.3 Install a client certificate on each macOS device

To install a client certificate on each macOS device follow the instructions below.

1. Copy the client certificate onto the macOS device.
2. Open Keychain Access and from its File menu select **Import Items,** then navigate to the certificate. Double-click it and enter its password when prompted, then the client certificate and its associated private key should appear under the login keychain. Alternatively, double-click on the **.pfx** file in the Finder.
3. Copy the client certificate and its associated private key separately under the System keychain.
4. Allow access to the private key for the 1E Client by following these instructions:
5. Open the Keychain Access app, either by pressing command-space and searching for keychain or from the Finder app, top left select Go > Utilities and double click to invoke the Keychain Access app.
6. Locate the private key of the Tachyon Agent within the System keychain.
7. The private key will appear under its associated public certificate.
8. Ensure the private key is present in the System keychain.
9. Double-click the private key and select the Access Control tab.
10. Ensure **Confirm before allowing access** is selected and then add the Tachyon Agent binary to the **Always allow access by these applications**; adding the 1E Client by its path name, which is typically /Library/Application Support/1E/Client/1E.Client

Warning

The Keychain Access app cannot be guaranteed to always refresh its view following, for example, an update of access control permission. However, after exiting the app, killing the process */Applications/Utilities/Keychain Access.app/Contents/MacOS/Keychain Access* and then restarting the app, will ensure the Keychain Access view will correctly display the contents of the Key Store.

An alternative approach to using the Keychain Access app is to import the **.pfx** file using the command-line security command:

```
sudo security import <download location>/<macOSpfx>.pfx -k /Library/Keychains/System.keychain -t agg -f pkcs12 -P <password> -T '/Library/Application Support/1E/Client/1E.Client'
```

This command imports a client certificate and the associated private key (termed **an identity** on macOS) from a **.pfx** file to a <keychain> as an aggregated type in PKCS #12 format using the specified password and giving access to the 1E Client.

> **Warning**
>
> When upgrading the 1E Client, by default the new version will not automatically be granted access to the private key in the Key Store. You can either repeat the import process during upgrade, or avoid the overhead by using the command-line security command with the import -A flag instead of -T . Please note that Apple do not recommend this approach as it is considered less secure. For more information on the security command please refer to the macOS page: https://ss64.com/osx/security-export.html.

If you do not grant correct access to the client certificate's private key, and the 1E Client debug logging is configured the log will show that it cannot obtain the client certificate's private key because the user name or passphrase entered is not correct.

2.3.2.3 Preparation

1E Client installation files are available for download from https://support.1e.com/.

Installation source files for non-Windows are available in a zip file called **1EClient-Non-Windows.v8.1.x.x.zip**

Within the zip, **1E Client for macOS** is provided as an Apple Disk Image file, such as **1e.client-macOS_v8.1.x.x.dmg**.

> **Warning**
>
> 1E Client for macOS is written for Intel and supported on Apple devices using Intel processors. It is also supported on Apple devices using the M1 chip, provided you have installed Rosetta 2, which is included with Big Sur. 1E Client is a daemon (not an app), therefore, during installation or running it will not prompt for Rosetta 2, which does not get installed on-demand.
>
> You only need to install Rosetta 2 once, using one of the following commands, but repeating the command will safely reinstall it. The second version of the command requires root permission. Attempting to install on an Intel device will issue a harmless "unrecognized option" usage message.

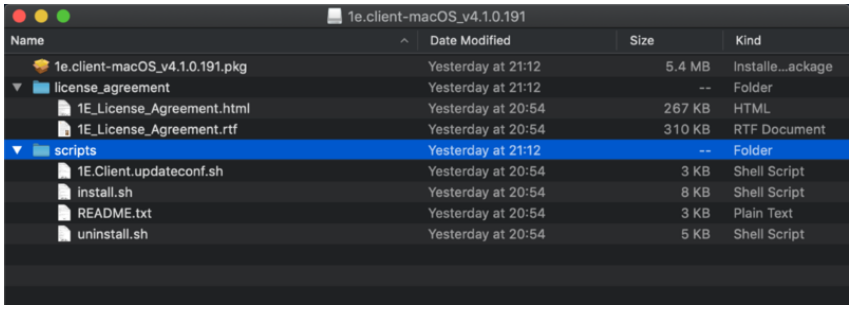
```
/usr/sbin/softwareupdate --install-rosetta
/usr/sbin/softwareupdate --install-rosetta --agree-to-license
```

Once the **dmg** file is copied to macOS, double-click on the **dmg** file to automount it under **/Volumes** and display it in a Finder window, as shown.

If you wish, you can script this using all or parts of the following example:

```
mkdir ~/Downloads/1e.client
cd ~/Downloads/1e.client
wget https://<<serverURL>>/1e.client-macOS_v8.1.x.x.dmg
hdiutil attach 1e.client-macOS_v8.1.x.x.dmg
```

The last line of the output of the **hdutil** command will show the location of the mount point, which is likely to be **/Volumes/image.1e.client-macOS_v8.1.x.x**



2.3.2.4 Installation

To install the macOS 1E Client perform **only one** of the following three options:

1. Use the **install.sh** script provided under the scripts directory, to install and configure the client, as shown in the pictures:
   - Copy the script to a separate directory together with the package you wish to use for installation or upgrade.
   - Invoke **install.sh** script to install, configure and start the 1E Client, giving the Switch host and port as the first parameter and the Background Channel URL as the second:

     ```
     sudo ./install.sh tachyon.acme.local:4000 https://tachyon.acme.local/Background
     ```

     Note

     This method will start the client, but connection to the Tachyon Switch will fail unless the client has the necessary certificates, as described in Client certificates below.
2. Install the package file from a command window to install using defaults. The **-target** is the volume mount point, not the path in the file system at which it will be installed.

   ```
   sudo installer -pkg /path/to/pkg/1e.client-macOS_v8.0.x.x.pkg -target /
   ```
3. Double-click on the package (.pkg) file within the Finder window to install using defaults.

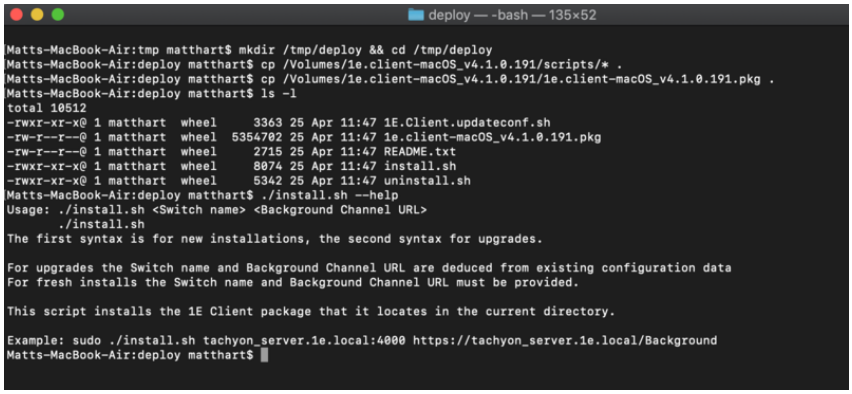
Note

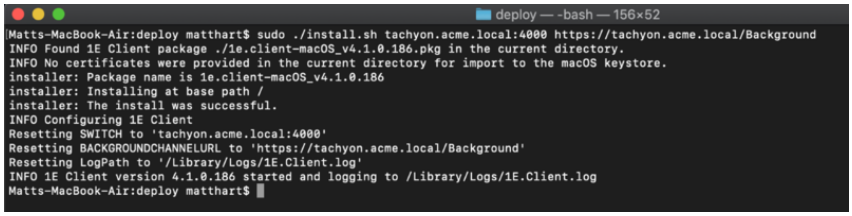
For options 2 and 3, you will need to reconfigure the 1E Client either using the **1E.Client.updateconf.sh** script or by editing the **/etc/1E/Client/1E.Client.conf** file, as described in Reconfiguration.

You will also need to provide the necessary client certificates, as described in Client certificates, and then start the client.

After installation, you can unmount the **dmg** using the following command:

```
hdiutil eject /Volumes/image.1e.client-macOS_v8.0.x.x
```





2.3.2.5 Reconfiguration

You will need to use the **1E.Client.updateconf.sh** script if you want to reconfigure the client, or you installed 1E Client using the previous installation options.

The **pkg** installation package for macOS includes a bash script called **1E.Client.updateconf.sh**. The configuration properties for the Switch and Background Channel are mandatory, therefore assuming they are on the same Tachyon Server which has a DNS Name FQDN **tachyon.acme.local** then the post-installation command line would be similar to the following but all on one command line. The second Switch and Background Channel can be removed if a DMZ server is not used. Single quotes avoid escape characters and are necessary to allow the use of the **;** character.

```
sudo sh '/Library/Application Support/1E/Client/1E.Client.updateconf.sh'
'/Library/Application Support/1E/Client/1E.Client.conf'
SWITCH='tachyon.acme.local:4000;tachyon.acme.com:4000'
BACKGROUNDCHANNELURL='https://tachyon.acme.local:443/Background/;https://tachyo
n.acme.com:443/Background/'
```

Please refer to 1E Client configuration settings and installer properties for a list of other configuration properties that can be appended to the above command-line.

2.3.2.6 Starting the 1E Client

To load and start the 1E Client use the command:

```
sudo launchctl load -w /Library/LaunchDaemons/com.1e.pkg.1E.Client.plist
```

> **Note**
>
> The client starts automatically if the switch and background URL are passed in the installation command as parameters as well as after client upgrade.

If it is necessary to stop the 1E Client use the command:

```
sudo launchctl unload /Library/LaunchDaemons/com.1e.pkg.1E.Client.plist
```

If the 1E Client should fail to start correctly please check:

- **sudo launchctl list | grep -i 1e** - to confirm the service is actually running. It should appear as **com.1e.pkg.1E.Client**
- **/Library/Logs/1E.Client.Daemon.log** - shows any service start errors
- **tail -f /Library/Logs/1E.Client.log** - shows the current operation of the 1E Client.
- If necessary raise the **/Library/Application Support/1E/Client/1E.Client.conf** to **LoggingLevel=debug** using a suitable text editor such as vi and then restart the 1E Client.

2.3.2.7 Uninstallation

To uninstall the 1E Client from a macOS device invoke the *uninstall.sh* script from within a sudo bash script. *uninstall.sh* is available within the scripts directory of the Apple Disk Image (dmg) file of the macOS 1E Client.

Alternatively, enter the following commands inside a sudo bash shell:

```
bash$ cd /Library
bash$ pkgutil --only-files --files com.1e.pkg.1E.Client | tr '\n' '\0' | xargs
-n 1 -0 rm
bash$ pkgutil --forget com.1e.pkg.1E.Client
```

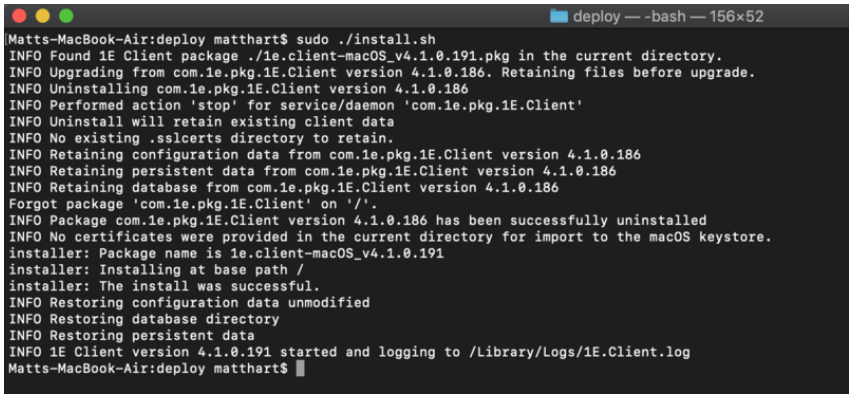
2.3.2.8 Upgrading

The **install.sh** script can be used for upgrading as well as installing. The bash script will deduce parameters from the existing configuration so no parameters are necessary, as shown in the picture.

If the installation of the macOS 1E Client is performed by double clicking on the latest .pkg file, then the new 1E Client will install successfully, but the contents of 1E.Client.conf will be reset to their default settings. To ensure that existing 1E.Client.conf settings are preserved across a 1E Client upgrade, please use the install.sh script.

When upgrading the 1E Client, by default the new version will not automatically be granted access to the private key in the Key Store. You can either repeat the import process during the upgrade or avoid the overhead by using the command-line security command with the import -A flag instead of -T . Please note that Apple does not recommend this approach as it is considered less secure. For more information on the security command please refer to the macOS page: https://ss64.com/osx/security-export.html.

If you do not grant correct access to the client certificate's private key, and the 1E Client debug logging is configured the log will show that it cannot obtain the client certificate's private key because the user name or passphrase entered is not correct.



2.3.3 Deploying 1E Client on Linux

Guidance for deploying 1E Client onto **Red Hat Enterprise Linux** devices, including installation and uninstallation. Only the platform features of 1E Client are available on Linux and other non-Windows OS.

2.3.3.1 Requirements

Please review Planning for 1E Client pages. After installation, please review the Verifying page.

For details of supported OS platforms, please refer to Common client requirements page.

Guidance provided below is for installation on Red Hat Enterprise.

> **Note**
>
> 1E Client does not have a license key. Even so, you must adhere to the terms of your license agreement.

2.3.3.1.1 Deployment choices

You must decide how you will configure the 1E Client and deploy to devices. Deploying the 1E Client is normally achieved using your existing software deployment tool.

> **Note**
>
> For more information about configuring the 1E Client properties during and after installation, please refer to 1E Client configuration settings and installer properties.

2.3.3.1.2 Non-Windows installation account

To install the 1E Client on a non-Windows client the installation account must have privileges to run the **sudo** command.

2.3.3.1.3 Certificate files

Each platform client device requires a **.pfx** certificate file. Please refer to Deploying 1E Client on macOS, for steps to create and use the **.pfx** file. For Linux devices, the client does not use proprietary certificate stores. Instead, the client requires the certificate exists as a .PFX file in the client installation folder structure.

If you have configured Tachyon Server to require client certificates (Client certificates) then each device requires a certificate with the following properties, so the client can be authenticated by the Tachyon Switch:

1. Issued by a trusted Certificate Authority (CA):
   - The certificate for the Root CA in the Certification Path must exist in the Trusted Root CA store of the client.
   - If the issuing CA is not the Root CA then the certificate for the issuing CA and any intermediate CA in the Certification Path must exist in the Intermediate CA store of the client.
   - If either of these CA certificates is different from those used by the Tachyon Web Server, they will need to be exported and imported on the Tachyon Web Server.
   - Most organizations have automated distribution of these CA certificates to clients and servers, using Group Policy for example.
2. Has at least the following Enhanced Key Usage
   - Client Authentication.
3. Has at least the following Key Usage
   - Digital Signature
   - Key encipherment.
4. Has a private key
   - For workgroup and non-Windows devices, the **private key must be exportable**
5. Revocation information is included.
   - References at least one CRL Distribution point that uses HTTP.
6. Has a Subject Name of type Common Name (**CN=<computername>**) or Subject Alternative Name (**DNS Name=<computername>**) where <computername> depends on the type of device:
   - On domain-joined Windows PCs this must be the **computername FQDN** of the computer, for example **W701.ACME.LOCAL**
   - On workgroup Windows PCs and non-Windows devices, this must be the computername of the computer - as returned by the **hostname** command, for example on Windows PC this could be **W701**, and on a Mac this could be **MAC01.local**

Note

Tachyon clients and Switches use OpenSSL and its validation process to verify certificates.

2.3.3.2 Preparation

1E Client installation files are available for download from https://support.1e.com/.

Installation source files for non-Windows are available in a zip file called **1EClient-Non-Windows.v8.1.x.x.zip**

2.3.3.3 Installation

The basic command to install an RPM package is **rpm -i <package_file>**. Although RPM, by design, does not support configuration during installation (with the Linux recommended approach to configure after installation) - the 1E Client does in fact support configuration through the use of environment variables. These can be easily set in a bash command line by one or more space-separated name=value pairs preceding the install command. So, if the RPM package file name is **1e.client-RHEL_8.3_x64_v8.0.4.261.rpm** and the Tachyon Server (assuming that the switch and the background channel are both installed on the Tachyon Server) has the DNS Name FQDN tachyon.acme.local then the command to run would be:

```
sudo SWITCH=tachyon.acme.local:4000 BACKGROUNDCHANNELURL=https://tachyon.acme.local:443/Background/ rpm -i 1e.client-RHEL_8.3_x64_v8.0.4.261.rpm
```

Please refer to 1E Client configuration settings and installer properties for a list of other configuration properties that can be configured in the same way.

> **Note**
>
> The correct case for each property must be used when entering the Linux installer command.

> **Note**
>
> When the package starts to install you may notice that the **ldconfig** command generates a warning saying that a
> **.py file is not an ELF file - it has the wrong magic bytes at the start**.
>
> This is because **ldconfig** assumes all files in **/usr/lib** are ELF files, and that file is a python file.
>
> You can safely ignore this warning.

After the package is installed the application configuration files will be installed to the following directory:

```
/etc/1E/Client
```

After running the Linux RPM package the client is installed and started as a daemon (service).

The client certificate **Tachyon.pfx** and a **cacert.pem** file are required in the hidden directory: */etc/1E/Client/.sslcerts*

If **Tachyon.pfx** contains the same certificate trust chain as the Tachyon Switch, then **cacert.pem** is optional. This is because the client will have already cached the public certificates when it parses **Tachyon.pfx** and **cacert.pem** will be duplicating the public certificate information. If **Tachyon.pfx** is using a different certificate trust chain from the Tachyon Switch, then **cacert.pem** is always required.

2.3.3.4 Reconfiguration

Please refer to 1E Client command-line parameters if you would like to see details of other CLI commands.

Note

This method is suitable for 1E Clientreconfiguring all settings on non-Windows devices because only platform client features are available and all settings are stored in the 1E Client configuration file.

Example:

```
/usr/sbin/1E.Client -reconfigure Switch=ACME-DMZ01.ACME.LOCAL:4000 BackgroundCh
annelUrl=https://ACME-DMZ01.ACME.LOCAL:443/Background/ -restart
```

2.3.3.5 Client certificates

Each client device requires its own certificate, which must be created as a **.pfx** file.

2.3.3.5.1 Using OpenSSL to create the .pfx file

Each non-Windows device requires its own certificate. Below is a guide for using a Microsoft CA to issue a certificate (which is the same for Windows computers), then exporting it and using OpenSSL to prepare it before installing it on a non-Windows device.

First, you will need to have created a new Certificate template on your Certificate Authority by making a duplicate of either the Computer or Workstation template and configuring it with at least the following properties:

- **General** - use a suitable name such as **Tachyon Devices** and validity period
- **Request Handling** - Allow private keys to be exported
- **Subject Name** - Allow information to be supplied in the certificate request, rather than being built from Active Directory information
- **Extensions** - Application Policies should contain only Client Authentication
- **Security** - ensure relevant users and computers will be able to request certificates.

Once the new template is created on the CA, issue it.

Using the issued template, request a certificate for a target device, and export it in **.pfx** form and remember the password.

The target device requires a copy of the basic **cacert.pem** and the **.pfx** file with its password removed. You can do this using the following steps. Use the relevant OpenSSL version for the OS. OpenSSL is normally available by default on Linux and Mac devices. If you want to follow these steps on Windows, you will need to download the open-source version appropriate to your OS.

1. First, extract the certificate:

   ```
   openssl pkcs12 -clcerts -nokeys -in <YourPKCSFile>.pfx -out certificate.c
   rt
   ```

2. Second, the CA key:

   ```
   openssl pkcs12 -cacerts -nokeys -in <YourPKCSFile>.pfx -out ca-cert.ca
   ```

3. Now, the private key:

   ```
   openssl pkcs12 -nocerts -in <YourPKCSFile>.pfx -out private.key -passout
   pass:TemporaryPassword
   ```

4. Remove the passphrase:

   ```
   openssl rsa -in private.key -out new.key -passin pass:TemporaryPassword
   ```

5. Put things together for the new PKCS-File (on Windows, **type** can be used instead of **cat**):

   ```
   cat new.key > PEM.pem
   cat certificate.crt >> PEM.pem
   cat ca-cert.ca >> PEM.pem
   ```

6. And create the new **.pfx** file, when prompted for a password ensure that you enter an empty password (that is press enter when prompted for the password and confirmation without entering any text):

   ```
   openssl pkcs12 -export -nodes -CAfile ca-cert.ca -in PEM.pem -out Tachyon
   .pfx
   ```

Now you have a new PKCS12 key file without a passphrase on the private key part. This **Tachyon.pfx** file and the **cacert.pem** file, must be placed in one of the following locations - depending on the OS. These are hidden folders.

2.3.3.5.2 Storing the .pfx on the client

The client certificate file (**Tachyon.pfx**), and Certificate Authority (CA) certificate(s) for the Switch certificate (**cacert.pem** file) are stored in the hidden directory:

/etc/1E/Client/.sslcerts

If the client certificate:

- (**Tachyon.pfx**) uses the same certificate trust chain as the Tachyon Switch, then **cacert.pem** is optional. This is because the client will have already cached the public certificates when it parses **Tachyon.pfx**.
- (**Tachyon.pfx**) uses a different certificate trust chain from the Tachyon Switch, then **cacert.pem** is always required.

2.3.3.6 Uninstallation

The following command-line can be used to uninstall the 1E Client on Linux:

```
sudo rpm -e 1e.client
```

Uninstallation will leave behind files, folders and registry entries that were created after installation:

Location	Artifacts	Recommendation
Installation folder	None.	
Logs folder	Log files remain.	The log files can be deleted or renamed. If not deleted, then a new installation that uses the same logs folder will continue to use the old log file.
Client\Persist folder remains.	You should keep the **Persist** folder, which contains status information about current instructions, only if you intend to re-install the 1E Client.	

2.3.4 Deploying 1E Client on Solaris

Note

1E Client is no longer available for Solaris, but 1E may reintroduce it, if there is sufficient demand.

2.3.5 Reconfiguring 1E Client

The 1E Client will be installed with the configuration required at the time. After the initial installation, it may be necessary to reconfigure the 1E Client. For example, you may want to enable a module that was not enabled when the client was first installed. This page provides guidance on changing the configuration of the 1E Client after the initial installation and configuration.

1E Client installers include a **template configuration file** that contains the more important settings with default values that match hard-coded default values. The configuration file is updated during installation and named **1E.Client.conf** in the installation folder along with the 1E Client executable.

After installation, configuration file settings can be managed using 1E Client reconfiguration, Explorer configuration instructions, Guaranteed State policies, Configuration Manager baselines or other means. Registry settings can also be managed by Windows Group Policy.

This page describes how to use Configuration Manager Configuration Baselines to reconfigure the 1E Client, which applies only to Windows devices. For non-Windows devices please see Reconfiguring on non-Windows devices.

Please refer to 1E Client configuration settings and installer properties for a summary, and links to further pages with more details.

2.3.5.1 Understanding how 1E Client settings are managed

You can enable or disable 1E Client features using the **1E.Client.exe -reconfigure** command line interface described in Example command-lines for reconfiguring the 1E Client below. Once enabled, additional configuration is likely to be required.

- All 1E Client and Shopping/WSA configuration settings can be modified using the **1E.Client.exe -reconfigure** command line interface.
- All Nomad and most of WakeUp configuration settings are managed in the registry, so must be addressed in addition to enabling the module using the **1E.Client.exe -reconfigure** command.

The table below summarizes which settings can be modified after installation using **1E.Client.exe -reconfigure** and which require modification in the registry. If you are using Configuration Manager, registry settings are best managed using Configuration Baselines.

Client / module	Set with 1E.Client.exe -reconfigure	Set in registry
1E Client	All Platform features of the 1E Client	None
Shopping/WSA	All Shopping client settings	None
WakeUp	Module.WakeUp.Enabled Module.WakeUp.ManageFirewallRules	All other /document/preview/647736#UUID-b588cdab-ae07-3331-ceb1-c8c6ed63aa1e
Nomad	Module.Nomad.Enabled	All other Content Distribution client settings
PXE Everywhere	Module.PXEEverywhere.Enabled	All other PXE Everywhere Agent settings

Installer Properties and registry values

Installer properties allow configuration of the 1E Client during installation. While there is generally a one-to-one mapping of Installer property to registry value, the Installer properties are all prefixed with MODULE.<PRODUCT> whereas registry values are not. Aside from the prefix in Installer property names, in some cases the registry value name is different from the installer property name. When configuring the Nomad and WakeUp client module registry settings, be careful to refer to the registry value names in the above settings links rather than the Installer property names.

2.3.5.2 Using Configuration Manager to enable and reconfigure the 1E Client after installation

The 1E Client can be configured after installation using a Configuration Manager Configuration Baseline. The following template Configuration Items have been prepared and are available to be downloaded and imported into Configuration Manager.

You can download the set of template Configuration Items available here **1EClientCIs.zip** and unzip to a working directory accessible from a CM console.

Note

The current version of 1EClientCIs.zip does not support changes to PXE Everywhere.

CI Name	Description
Enable and Configure Shopping module in 1E Client	PowerShell script CI that detects if Shopping module is enabled. If not, the remediation script will enable and configure the Shopping module using the **1E.Client.exe -reconfigure** command and restart the 1E Client for the settings to take effect. The following settings are applied by the script. • Module.Shopping.Enabled=true • Module.Shopping.ShoppingCentralUrl=https://<<FQDN>>/shopping • Module.Shopping.LoopbackExemptionEnabled=True You will need to modify the remediation script as described in the process below this table with the FQDN of your Shopping host (typically a DNS alias for the Shopping website host header). You may also want to disable the Loopback Exemption (set it to false).
Configure Tachyon client in 1E Client	PowerShell script CI that detects if the Switch and Background Channel have been defined. If not, the remediation script will configure these settings using the **1E.Client .exe -reconfigure** command and restart the 1E Client for the settings to take effect. The following settings are applied by the script. • Switch=<SERVERFQDN>:4000 • BackgroundChannelUrl=https://<SERVERFQDN>:443/Background/ You will need to modify the remediation script as described in the process below this table with the FQDN of your Tachyon host (typically a DNS alias for Tachyon server). Note that the Tachyon client cannot actually be enabled or disabled. It is an intrinsic part of the 1E Client and is always enabled. If you are not using the Tachyon platform, you install 1E Client with the SWITCH and BACKGROUNDCHANNELURL properties set to NONE.

CI Name	Description
Enable Nomad module in 1E Client	PowerShell script CI that detects if the Nomad module is enabled. If not, the remediation script will enable the Nomad module using the **1E.Client.exe -reconfigure** command and restart the 1E Client for the settings to take effect. There are no settings in this remediation script that need to be modified for Content Distribution.
Enable WakeUp module in 1E Client	PowerShell script CI that detects if WakeUp module is enabled. If not, the remediation script will enable the WakeUp module using the **1E.Client.exe -reconfigure** command and restart the 1E Client for the settings to take effect. There are no settings in this remediation script that need to be modified for WakeUp
Nomad Registry Settings	Registry Value CI that includes commonly configurable Nomad registry settings with their default values. You will need to modify these if your Nomad design requires any non-default configuration settings. **Tip** The zip does not contain all registry settings for Nomad. You can create your own Configuration Item for the Nomad module using Nomad Baseline Wizard.
WakeUp 7.3 Registry Settings	Registry Value CI that includes all commonly configurable WakeUp 7.3 registry settings with their default values. You will need to modify these at a minimum to define the SerivceURL (the URL of the AFWebService) and any non-default WakeUp configuration settings required by your design.

To configure the 1E Client after installation:

1. Import template Configuration Items
    a. Download the set of template Configuration Items available here **1EClientCIs.zip** and unzip to a working directory accessible from a CM console
    b. Start the CM console and open the **Assets and Compliance** workspace
    c. Expand the **Compliance Settings** folder, right-click **Configuration Items** and select **Import Configuration Data** to start the **Import Configuration Data Wizard**
    d. From the **Import Configuration Data Wizard Select Files** page, click **Add...** and browse to the files extracted from 1EClientCIs.zip. You can select to import all files, or select only those relevant to the modules you want to enable and configure right now, using the above table for reference. Click **Open** to import the selected files
    e. As the Configuration Items have not been signed you will be prompted to confirm that you want to import them - click **Yes** to import each file, then click **Next**

f. On the **Summary** page click **Next** to import the Configuration Items

g. On the **Confirmation** page click **Close**.

Supported Platforms

After importing the Configuration Items, double-click each in turn to view the CI properties and review the Supported Platforms tab to ensure all Operating Systems you currently manage are selected. For example, if you are managing Windows Server 2019 with CM CB 1902 or later, you will need to select Windows Server 2019.

2. If you want to configure **Tachyon**

   a. Double-click the **Configure Tachyon client in 1E Client** Configuration Item to edit its properties

   b. Click on the **Settings** tab, then double-click the **Configure Tachyon client in 1E Client** setting

   c. From the **General** tab of the **Configure Tachyon client in 1E Client Properties** dialog box, select the **Edit Script** button under **Remediation Script (optional)**

   d. In the script editor, replace <SERVERFQDN> with the FQDN of your Tachyon server for both the Switch and BackgroundChannelUrl. If you are using custom ports, then modify these accordingly too, then click **OK** to save and close the script editor.

   e. Click **OK** on the remaining dialog boxes to save the updated CI and return to Configuration Items in the CM console.

3. If you want to configure **Shopping**

   a. Double-click the **Enable and Configure Shopping module in 1E Client** configuration Item to edit its properties

   b. Click on the **Settings** tab, then double-click the **Enable and Configure Shopping module in 1E Client** setting

   c. From the **General** tab of the **Enable and Configure Shopping module in 1E Client Properties** dialog box, select the **Edit Script** button under **Remediation Script (optional)**

   d. In the script editor, replace <<FQDN>> with the FQDN of your Shopping web server (typically this is a DNS alias for the Shopping website host header), then click **OK** to save and close the script editor

   e. Click **OK** on the remaining dialog boxes to save the updated CI and return to Configuration Items in the CM console.

4. If you want to configure **WakeUp**, there are no changes required to the Enable WakeUp module in 1E Client CI, but you will need to modify the WakeUp 7.3 Registry Settings CI as follows:

   a. Double-click the **WakeUp 7.3 Registry Settings** configuration Item to edit its properties

   b. Click on the **Compliance Rules** tab and review the values defined for each of the registry values. To modify any of these, double-click the item and in the **Edit Rule** dialog box, define the value that should be used:

- If the AFWebService website is using HTTP, replace the <SERVERFQDN> in the **ServiceUrl (HTTP)** setting with the FQDN of the web server and ensure the **ServiceUrl (HTTPS)** value is blank
- If the AFWebService website is using HTTPS, blank the **ServiceUrl (HTTP)** value and replace the <SERVERFQDN> in the **ServiceUrl (HTTPS)** setting
- When using HTTPS you must also define either **CertIssuer** or **CertSubject** setting.

c. Click **OK** to save the properties and return to Configuration Items in the CM console.

5. If you want to configure **Nomad**, there are no changes required to the Enable Nomad module in 1E Client CI, but you will need to modify the Nomad 7.0 Registry Settings CI as follows:

   a. Double-click the **Nomad 7.1 Registry Settings** configuration Item to edit its properties

   b. Click on the **Compliance Rule**s tab and review the values defined for each of the registry values. To modify any of these, double-click the item and in the **Edit Rule** dialog box, define the value that should be used. If you are using ActiveEfficiency you will need to replace the <<AEServerFQDN>> in the **PlatformUrl** setting with the FQDN of the ActiveEfficiency web server

   c. Click **OK** to save the properties and return to Configuration Items in the CM console.

6. Create a baseline to configure the 1E Client to include the required Configuration Items as follows:

   a. Right-click **Configuration Baselines** and select **Create Configuration Baseline**. Enter a suitable name and description.

   b. Click the **Add** button and select Configuration Items from the drop-down list. Select the Configuration Items as follows:

      - To configure **Tachyon** with this baseline, select the **Configure Tachyon Client in 1E Client** CI and click **Add**
      - To configure **Shopping**, select the **Enable and Configure Shopping module in 1E Client** CI and click **Add**
      - To configure **WakeUp**, select the **Enable WakeUp module in 1E Client** and **WakeUp 7.3 Registry Settings** CIs and click **Add**
      - To configure **Nomad**, select the **Enable Nomad module in 1E Client** and **Nomad 7.0 Registry Settings** CIs and click **Add**

   c. When you have added all the CIs you want to include, click **OK** to save and close the **Add Configuration Items** dialog box, then click **OK** to close the Create Configuration Baseline dialog box.

7. Deploy the Configuration Baseline to systems with the 1E Client installed

   a. Right-click the Configuration Baseline created in the previous step and select **Deploy**

   b. In the **Deploy Configuration Baselines** dialog box check the option **Remediate noncompliant rules when supported**

c. Click the **Browse...** button and select a Collection to deploy the baseline to (typically you would use the same Collection that was targeted with the initial 1E Client installation deployment)

d. Modify the scheduling according to your preferences and click **OK**.

Clients in the targeted Collection will start to apply the Configuration Baseline after the next machine policy refresh. You can check the compliance status periodically Configuration Baselines view in the console.

2.3.5.3 Example command-lines for reconfiguring the 1E Client

After installing the 1E Client, it may be necessary to enable additional modules, disable modules, or change configuration settings. For example, the 1E Client may have been initially installed just for the Shopping or WakeUp modules and you now want to use the full 1E Client with the Tachyon Platform, or conversely you may have deployed the 1E Client without the Shopping module enabled and subsequently implemented Shopping and therefore need to enable the Shopping module. These scenarios can be managed using the **1E.Client.exe -reconfigure** command-line interface, so it is easy to implement using software distribution tools such as Configuration Manager.

Please refer to 1E Client command-line parameters if you would like to see details of other CLI commands.

Warning

You can change only configuration file settings using this method, you must use other methods to change registry settings. For further guidance, please refer to Reconfiguring 1E Client.

Note

Any name=value pair can be added to the configuration file, no validation is done. If a key with the name does not already exist in the configuration file, it will be added to the file and a warning output (in case the name has been misspelled).

2.3.5.3.1 Reconfiguring on Windows devices

The **-reconfigure** command-line option changes the settings in the **1E.Client.conf** configuration file. These changes are only available from Tachyon instructions when the 1E Client service is running. Use the **-restart** option on the command line to restart the service after the configuration changes have been made. Note that the restart will be delayed by a random duration (based on the Tachyon client reconnection interval) to disperse the load as clients connect to Tachyon, NightWatchman or Shopping servers on startup.

Tachyon client - to configure Tachyon feature settings if the 1E Client was initially installed with only the Shopping, WakeUp or Nomad client modules enabled, execute the following command line:

```
"%ProgramFiles%\1E\Client\1E.Client.exe" -reconfigure Switch=tachyon.acme.local
:4000 BackgroundChannelUrl=https://tachyon.acme.local/Background -restart
```

The above command can be extended to reconfigure any Tachyon settings because they are all stored in the 1E Client configuration file.

Nomad client - to enable the Nomad client module on a deployed 1E Client, execute the following command line:

```
"%ProgramFiles%\1E\Client\1E.Client.exe" -reconfigure Module.Nomad.Enabled=true
```

The above command only enables the Nomad client module, which is the only Nomad setting in the 1E Client configuration file. The command does not configure registry settings necessary for using ActiveEfficiency. You can update the registry using commands such as:

```
REG ADD HKLM\Software\1E\NomadBranch\ActiveEfficiency /v PlatformUrl /t REG_SZ
/d https://aeserver.acme.local/ActiveEfficiency
```

PXE Everywhere client - to enable the PXE Everywhere client module on a deployed 1E Client, execute the following command line:

```
"%ProgramFiles%\1E\Client\1E.Client.exe" -reconfigure Module.PXEEverywhere.Enab
led=true
```

The above command only enables the PXE Everywhere client module, which is the only PXE Everywhere setting in the 1E Client configuration file. The command does not configure registry settings necessary for connecting to the PXE Everywhere Central server. You can update the registry using commands such as:

```
REG ADD HKLM\Software\1E\PXEEverywhere /v ConfigServerAddress /t REG_SZ /d http
://SERVER.acme.local/PXELite/PXELiteConfiguration.asmx
```

Shopping client - to enable the Shopping client module on a deployed 1E Client, execute the following command line:

```
"%ProgramFiles%\1E\Client\1E.Client.exe" -reconfigure Module.Shopping.Enabled=t
rue Module.Shopping.ShoppingCentralUrl=http://appstore.acme.local/shopping -res
tart
```

The -reconfigure method can be used for all Shopping client settings because they are all stored in the 1E Client configuration file. If required, add Shopping client settings=true.

WakeUp client - to enable the WakeUp client module on a deployed 1E Client, execute the following command line:

```
"%ProgramFiles%\1E\Client\1E.Client.exe" -reconfigure Module.WakeUp.Enabled=tru
e Module.WakeUp.ManageFirewallRules=true
```

The above command only enables the WakeUp client module and enables Windows firewall rules. These are the only WakeUp settings in the configuration file. The command does not configure registry settings necessary for reporting to the NightWatchman Management Center server. You can update the registry using commands such as:

```
REG ADD HKLM\Software\1E\WakeUpAgt\Reporting\HTTP /v ServiceUrl /t REG_SZ /d ht
tp://nwmmc.acme.local/AFWebService/PostMessage.aspx
```

2.3.5.3.2 Reconfiguring on non-Windows devices

Please refer to 1E Client command-line parameters if you would like to see details of other CLI commands.

> **Note**
>
> This method is suitable for 1E Clientreconfiguring all settings on non-Windows devices because only platform client features are available and all settings are stored in the 1E Client configuration file.

On Linux and Solaris:

```
/usr/sbin/1E.Client -reconfigure Switch=ACME-DMZ01.ACME.LOCAL:4000 BackgroundCh
annelUrl=https://ACME-DMZ01.ACME.LOCAL:443/Background/ -restart
```

On macOS:

```
cd /Library/Application Support/1E/Client # Do not prefix cd with sudo
./1E.Client -reconfigure Switch=ACME-DMZ01.ACME.LOCAL:4000 BackgroundChannelUrl
=https://ACME-DMZ01.ACME.LOCAL:443/Background/ -restart
```

2.3.5.3.3 Starting and Stopping the 1E Client from the command line

On Windows devices, you can start, stop and restart the 1E Client from the command-line, as an alternative to using the Windows Services console UI. Please refer to 1E Client command-line parameters for more details.

On Linux, Solaris and macOS devices, you can start, stop and restart the 1E Client from the command-line.

2.3.6 Verifying

Links to other 1E product documentation to verify or troubleshoot their features that are dependent on the 1E Client.

- Tachyon platform: Verifying.
- Nomad: /document/preview/675710#UUID-ed88d585-22d1-0311-3246-8f71845db40c.
- PXE Everywhere: Verifying.
- Shopping: /document/preview/723100#UUID-b7e84337-1c0b-c10e-1146-03d4a06bc15e.
- NightWatchman Enterprise: /document/preview/712264#UUID-0e963042-5df7-7f6d-737e-0e98ab02ed2e.

2.3.6.1 General verification of the 1E Client

1. Confirm the 1E Client service is running.
2. Ensure you know which client features are enabled - review the **<INSTALLDIR>\1E\Client\1E.Client.conf** file.
3. Review the log files for errors.

1E Client logs on Windows

%ALLUSERSPROFILE%\1E\Client\1E.Client.log (used by 1E Client and Tachyon features, and Shopping client)

%ALLUSERSPROFILE%\1E\Client\NomadBranchUninstall-YYYY_MM_HHTMM_HH_SS_000Z.log

1E Client logs on macOS

/Library/Logs/1E.Client.Daemon.log (shows any service start errors)

/Library/Logs/1E.Client.log (shows the current operation of the 1E Client)

1E Client logs on other non-Windows platforms

/var/log/1E/Client/1E.Client.log

Nomad client log

%ALLUSERSPROFILE%\1E\NomadBranch\LogFiles\NomadBranch.log

PXE Everywhere Agent log

%ALLUSERSPROFILE%\1E\PXEEverywhere\PXEEverywhere.log

Shopping WSA client log

%ALLUSERSPROFILE%\1E\Client\WSA.log

WakeUp client log

%ALLUSERSPROFILE%\1E\Agent\WakeUpAgt.log

> **Note**
>
> By default, Windows resolves %ALLUSERSPROFILE% as C:\ProgramData\

2.4 Upgrading 1E Client

Guidance for upgrading Tachyon and other legacy 1E agents to 1E Client. This page contains detailed steps for upgrading Tachyon Agent and a summary of considerations for upgrading other legacy agents. The 1E Client contains clients for 1E products and solutions, and their upgrade documentation should be consulted before upgrading their clients and agents.

When upgrading a 1E product or solution, you should upgrade its server infrastructure first. For more information, please refer to the following:

- Upgrading Nomad - from 7.1 onwards you will be replacing ActiveEfficiency Server with Tachyon Platform, which includes Content Distribution

- Upgrading PXE Everywhere
- NightWatchman Enterprise - Upgrading NightWatchman Enterprise
- Shopping - Upgrading to Shopping
- Upgrading Tachyon Platform.

Note

Upgrading from earlier versions of 1E Client to 8.1 simply requires deploying the new version, using the same or different configuration settings.

Please refer to:

- Deploying 1E Client on Windows
- Deploying 1E Client on macOS
- Deploying 1E Client on Linux
- Deploying 1E Client on Solaris

If you are upgrading any legacy 1E agents then please read sections below.

Please refer to Reconfiguring 1E Client for how to reconfigure the 1E Client after it has been deployed.

2.4.1 1E Client versions

2.4.2 Upgrading legacy 1E agents to 1E Client 8.1

Before deploying the 1E Client you need to decide which:

- Client modules to enable.
- Client modules are new and what their settings should be.
- Legacy agents will be upgraded and replaced.
- Legacy agents will remain.

1E Client contains the following client modules which are only supported on Windows OS:

- **Nomad client** module - replaces Nomad Branch client.
- **PXE Everywhere Agent** module - replaces PXE Everywhere Agent (also known as PXELite and PXE Everywhere Local).

- **WakeUp client** module - replaces the WakeUp Agent component of 1E Agent, but does not affect 1E NightWatchman Agent.
- **Shopping client** module - replaces the Shopping Agent and also includes a feature called Windows Servicing Assistant (WSA).

Note

Non-Windows platforms support **Tachyon** features only.

Note

If a client module is enabled, it replaces the legacy version if present. Existing settings are retained unless individual setting are set during deployment.

The client upgrade process is the same as the interactive and command-line installation processes described in Deploying 1E Client on Windows.

When 1E Client is installed with one or more client modules enabled then if the older version of the legacy client is already installed then it is replaced with the current configuration settings retained unless overridden by new settings. The replacement process is not strictly an MSI upgrade because the 1E Client actually uninstalls the old product or component when the 1E Client service starts, not during installation of the 1E Client, and will only do this if the corresponding client module is enabled. First the 1E Client service copies registry values and re-instates them after uninstallation so they can be used by the client module.

Note

If legacy Agents have been deployed as Applications in Configuration Manager, you should define supersedence on each Application that installs the new version so that it supersedes the previous versions. This is *very important* as it prevents attempts at downgrading Tachyon, Nomad, WakeUp or Shopping clients through **Application Deployment Enforcement** if there are still active deployments for the previous versions.

Supersedence is the recommended way of preventing downgrades because other methods are not guaranteed, such as disabling old deployments (may be temporarily re-enabled), or using Exclude Collections (collection memberships can change).

1E NightWatchman Agent is unaffected by 1E Client, but is included in Introducing 1E Client Deployment Assistant) with the 1E Client, which also includes the WakeUp client, as described below.

The 1E Client Deployment Assistant is designed to help install Windows versions of 1E Client and other 1E agents using Configuration Manager. It includes template transform files for each combination of client/agent for 32 and 64-bit platforms, and automatically creates collections and deployments in Configuration Manager, so that you only need to populate the collections.

2.4.2.1 Nomad client

1E Client includes the Nomad client which is a replacement for the legacy Branch client that is installed on client computers, and on Distribution Points if Configuration Manager is used. Both new and legacy versions of the Nomad client are also known as the Nomad Branch client.

The client upgrade process is the same as the interactive and command-line installation processes described in Deploying 1E Client on Windows.

Please refer to Upgrading Nomad for more detail about upgrading the Nomad infrastructure. From Nomad 7.1 onwards you will be replacing ActiveEfficiency Server with Tachyon platform.

Upgrading Nomad may also require updates to existing Task Sequences. Existing Nomad Task Sequence steps will continue to work after the upgrade, but it may be necessary to remove and replace them after the upgrade to implement any fixes or improvements included in the new version.

2.4.2.2 PXE Everywhere Agent

1E Client includes the PXE Everywhere Agent which is a replacement for the legacy PXE Everywhere Agent (also known as PXELite and PXELocal) that is installed on client computers, and on Distribution Points if Configuration Manager is used.

The client upgrade process is the same as the interactive and command-line installation processes described in Deploying 1E Client on Windows.

Please refer to Upgrading to PXE Everywhere 8.1 for more detail about upgrading the PXE Everywhere infrastructure.

Upgrading PXE Everywhere will also require updates to existing Task Sequences to use updated boot images.

2.4.2.3 1E Agent, NightWatchman and WakeUp Agents

When upgrading 1E Agent that has both WakeUp and NightWatchman enabled and you require continuity of WakeUp features, then first deploy the **1E Client** with WakeUp client module enabled, and then deploy the **1E NightWatchman Agent**.

The legacy 1E Agent installer is replaced by two new installers:

- WakeUp Agent component of legacy 1E Agent is replaced by **1E Client** (with its WakeUp client module enabled)
- NightWatchman Agent component of the legacy 1E Agent is replaced by **1E NightWatchman Agent**.

The following occurs when upgrading a computer that has a legacy version of 1E Agent installed (with NightWatchman and/or WakeUp Agent enabled):

New client	What happens to the existing client when upgraded
1E NightWatchman Agent	Deploying **1E NightWatchman Agent** upgrades the legacy NightWatchman Agent component of 1E Agent and uninstalls the legacy WakeUp Agent component if installed. This process maintains the WakeUp registry, to be used by the WakeUp client module of the 1E Client if installed later. The **1E NightWatchman Agent** can only be installed on Windows workstation OS and *not* on server OS.

New client	What happens to the existing client when upgraded
1E Client	Deploying **1E Client** (with its WakeUp client module enabled) causes the legacy 1E Agent WakeUp component to be uninstalled the first time the 1E Client is started, leaving intact the NightWatchman Agent component if that was installed. The **1E Client** (with WakeUp client module enabled) can be installed on Windows workstation OS *and* on server OS. It *must* also be installed on **WakeUp Server** servers, which must be upgraded to WakeUp Server 7.3 or later.

Please refer to the following for more detailed steps for upgrading from **1E Agent**:

- Deploying 1E Client on Windows
- NightWatchman Enterprise 7.3 - Upgrading to 1E NightWatchman Agent 7.3.

You can use the Introducing 1E Client Deployment Assistant to assist with the deployment of **1E Client** and **1E NightWatchman Agent** using Configuration Manager.

Please refer to NightWatchman Enterprise 7.3 - Upgrading NightWatchman Enterprise for more details about upgrading the server infrastructure for **NightWatchman Enterprise** and **WakeUp Server**.

2.4.2.4 Shopping Agent

1E Client includes the Shopping client which is a replacement for the legacy Shopping Agent that is installed on client computers.

The client upgrade process is the same as the interactive and command-line installation processes described in Deploying 1E Client on Windows.

Please refer to Shopping 6.1 - Upgrading to Shopping for more detail about upgrading the Shopping infrastructure.

2.5 Troubleshooting

A general methodology for investigating issues with the 1E Client, as well as identifying key issues and their resolutions.

For known issues relating to specific components, please refer to the respective troubleshooting pages:

Clients

- 1E Client
- 1E Client Deployment Assistant

Platform

- 1E

Applications

- Endpoint Automation
- Experience Analytics
- Endpoint Troubleshooting

Integration

- 1E Core for ServiceNow
- 1E ITSM Connect for ServiceNow

- PXE Everywhere
- Writing 1E Instructions (1E SDK)
- 1E Service Catalog Connect for ServiceNow
- 1E Virtual Assistant

2.5.1 1E Support contact details

2.5.1.1 Support Web portal

Maintenance support customers can log onto the 1E Support Web Portal at https://support.1e.com/ using the login details provided with their maintenance contract. This provides issue tracking, product hotfixes, and knowledge base articles related to each product.

2.5.1.2 Telephone support

Maintenance support customers can contact the technical support department at 1E through the following support numbers. Just phone the relevant number for your area, so your call can be routed quickly and efficiently to the correct support group:

- US/Canada: 1-866-349-4032 (Toll-Free)
  1-917-339-2360 (Standard)
- UK/Europe: +44 (0)208 326 3499
- India: +91 120 402 4002
- Australia: +61 739 111 118

2.5.1.3 Email support

Maintenance customers can use the following email for additional support. Evaluation customers can also use this email with the temporary access code that is provided through customercare@1e.com as part of their evaluation.

support@1e.com

2.5.2 The technical support process

1. Read through the Troubleshooting pages to see if there are known issues, or quick resolutions to any problems you may have encountered.

2. Maintenance support customers can use the 1E Support Web Portal to review knowledge base articles and download hotfixes.

3. If still encountering problems, create a technical report (log files and details) and then contact the 1E technical support team.

2.5.2.1 Creating a technical report

If possible, please obtain the following details and log files before contacting 1E, to include in your technical report.

2.5.2.1.1 Version details

- The OS, version number, and patch level for:
  - Tachyon Servers
  - 1E Client
  - Configuration Manager - if used
  - Other 1E Server software, for example, Shopping, Nightwatchman, and WakeUp.
- For Nomad and Shopping, please provide OS, version number, and patch level for:
  - Configuration Manager DPs
  - Nomad extensions used on Configuration Manager Consoles
  - ActiveEfficiency Server.

2.5.2.1.2 Environmental details

- If there were any recent changes made to your configuration
- The name of the machines, Configuration Manager Application and/or Package IDs for when the issue occurred

2.5.2.1.3 Problem details

- When did the issue occur, ensure log files cover this period
- The scope of the issue – did it affect a particular geographical location, group of users, or client machines
- Details of any self-help troubleshooting steps you carried out
- In the event of a service crash or if you are experiencing high CPU or memory usage, provide us with the dump file, event viewer logs, and traces. We will provide you with FTP details to upload these files.

2.5.2.2 1E Client log files

1E Client logs on Windows

1E Client logs on macOS

1E Client logs on other non-Windows platforms

Nomad client log

PXE Everywhere Agent log

Shopping WSA client log

WakeUp client log

> **Note**
>
> By default, Windows resolves %ALLUSERSPROFILE% as C:\ProgramData\

2.5.3 Client issues

Troubleshooting common issues that you may be having with the installation and configuration of the Nomad.

If for any reason you are unable to install it, then please review the Planning for 1E Client.

When installing interactively, please confirm you are logged on using an account that has local Administrator rights.

You can troubleshoot installation issues by reviewing the installation log file. On Windows, start an Administrative command prompt and use a msiexec command line including a log file as described in Installing the 1E Client by command-line.

If your problem is not identified on this page, then please review the relevant client section on the Known issues page.

Please ensure you have run through the verification steps on the relevant pages:

- Tachyon Verifying
- Nomad /document/preview/675710#UUID-ed88d585-22d1-0311-3246-8f71845db40c
- PXE EveryWhere Verifying
- Shopping - Troubleshooting
- NightWatchman Enterprise - Troubleshooting.

2.5.3.1 Client certificate issues

If the Tachyon Server has been configured to require client certificates, clients must be running on devices where a valid device certificate has been applied. If this is not the case, the following symptoms will appear:

- The device where the client is running will not be able to connect to the Tachyon Server

- A warning similar to the following will appear in the **Tachyon.Switch.Host.log** file (the default location for all the Tachyon Server logs is **%AllUsersProfile%\1E\Tachyon** folder on the server where Tachyon Server is installed):

  ```
  WARN  - Error receiving data from [tachyon.test.local]:4000 : An establis
  hed connection was aborted by the software in your host machine
  ```

- On the Tachyon client device, you will see an error similar to the following in the **1E.Client.log** file (the default location for the 1E Client log is **%AllUsersProfile%\1E\Client** folder on the device where the client is installed):

  ```
  Received WS message: SwitInfo{"SwitchId":1,"SwitchName":"","WorkerNum":0,
  "SlotNum":3,"DisconnReason":"No Certificate"}
  ```

If you find log entries similar to these appearing in the log files, you can check that Tachyon is working correctly for the device by manually requesting a device certificate. If the device can then connect to the Tachyon Server, you should contact your network PKI administrator.

Note

Each client/agent in 1E Client uses certificates independently of each other.

Platform clients search for a client certificate so they can be authenticated by Tachyon servers.

Nomad clients search for a suitable client certificate so they can be authenticated by CM Distribution Points, and for use with Peer to Peer sharing. They can optionally use Nomad CertIssuer/CertSubject configuration settings to help find suitable certificates.

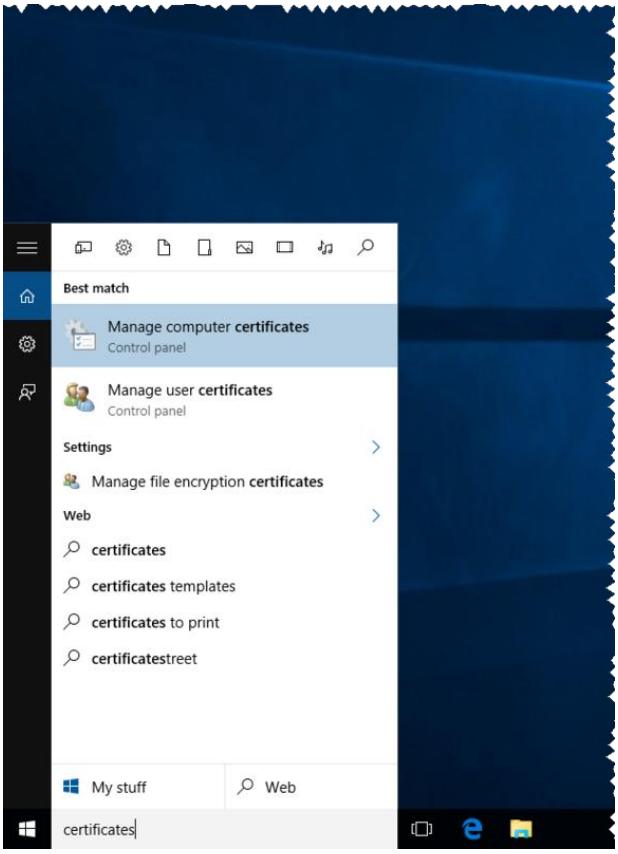
Shopping and WakeUp clients each have their own CertIssuer/CertSubject configuration settings that determine which client authentication certificate they each use. These are only needed if their websites have an HTTPS binding that is configured to require certificates.

PXE Everywhere Agent does not use client authentication certificates.

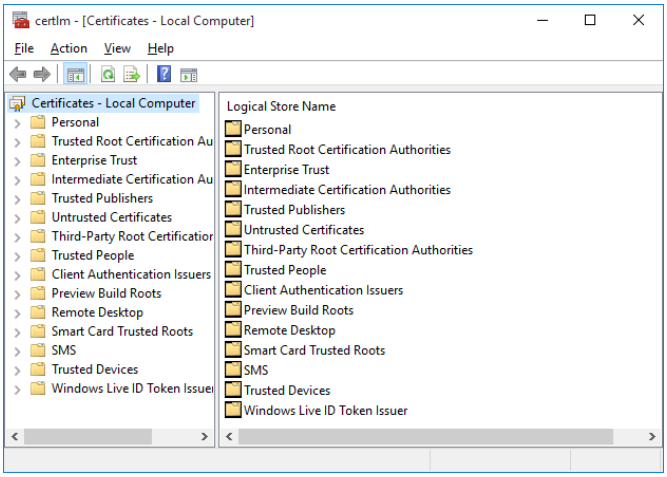
2.5.3.1.1 Manually requesting a device certificate on Windows 10

The following steps show the manual process of requesting a certificate (enrolling) for the computer on which the platform client is installed. Although these instructions cover Windows 10 the general approach of using the Certificates MMC snap-in can be extrapolated to cover most Windows Operating Systems.

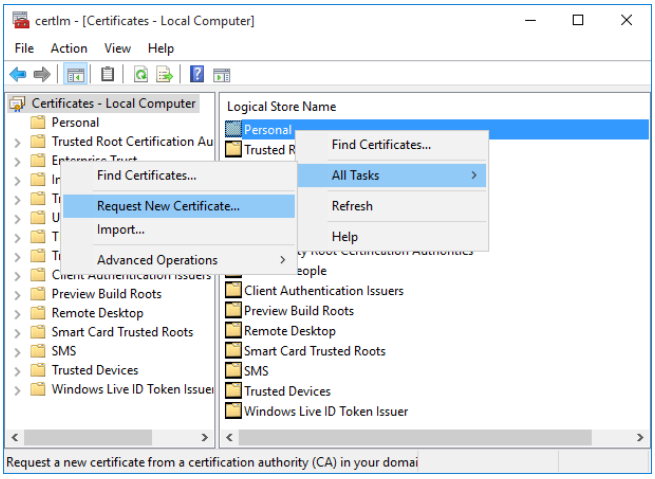
1. Run the certificate mmc snap-in. For example, by finding the **Manage computer certificates** application, as shown in the following picture.



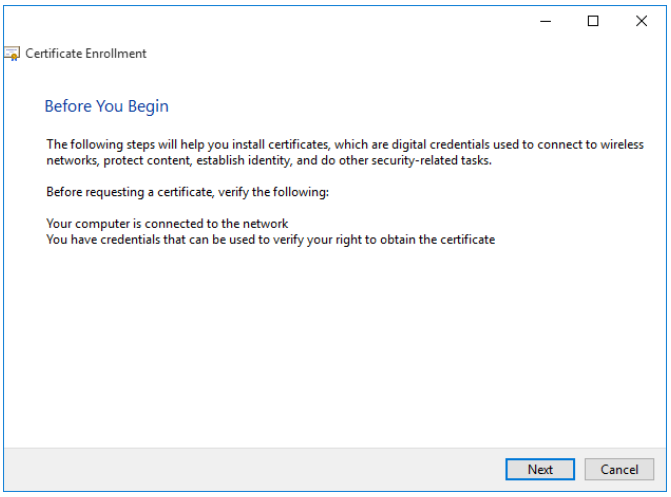
2. Doing this displays the certlm MMC snap-in, as shown in the following picture.



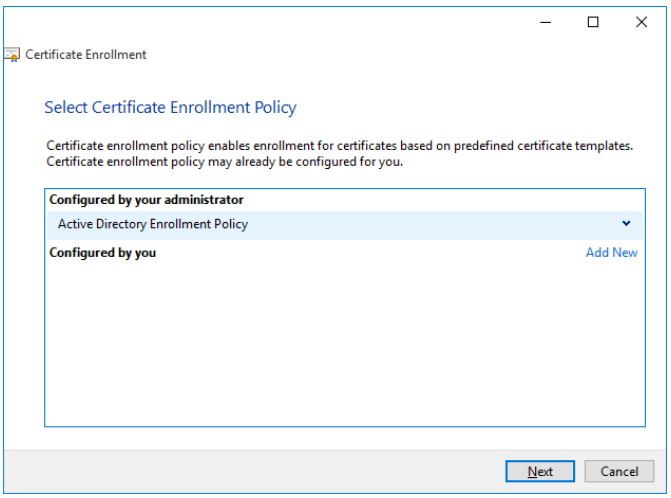
3. Right-click on the Personal folder and select the **All Tasks**->**Request New Certificate...** menu option from the right-click menu, as shown in the following picture.



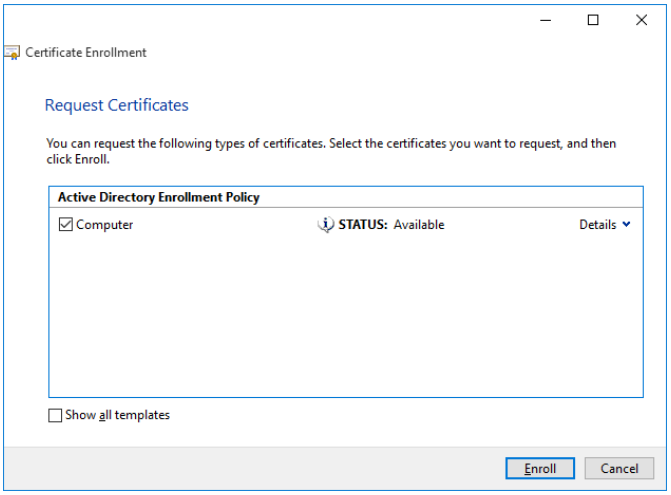
4. Doing this displays the Certificate Enrollment wizard. On the **Before You Begin** screen click **Next** to continue.



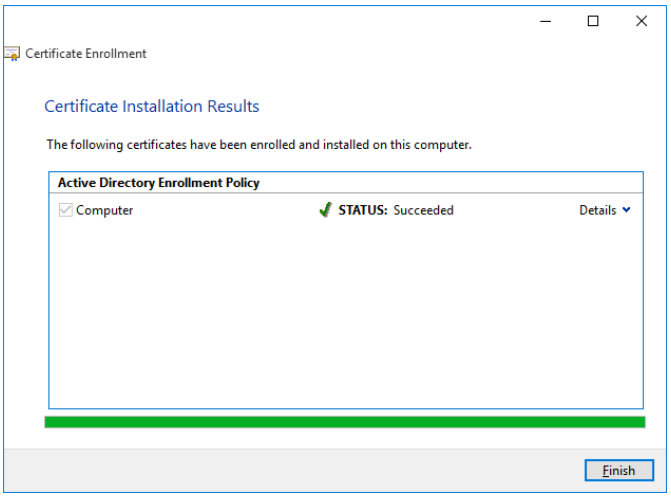
5. On the **Select Certificate Enrollment Policy** screen select the **Active Directory Enrollment Policy** option, as shown in the following picture.



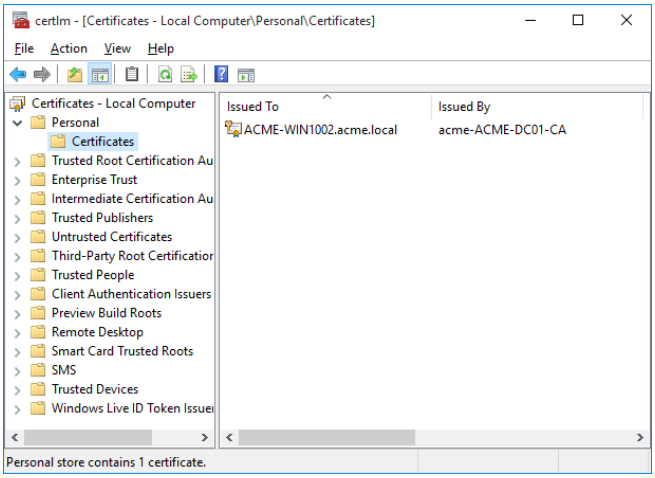
6. On the **Request Certificates** screen select the **Computer** certificate checkbox, as shown in the following picture, then click the **Enroll** button.



7. The **Certificate Installation Results** screen shows whether the certificate has been installed correctly. When it has, as shown in the following picture, click **Finish** to exit the wizard.



8. Once the wizard has completed you should see the new certificate under the **Personal->Certificates** folder, as shown in the following example.



2.5.3.2 Enabling SHA-512 to work with TLSv1.2

Tachyon uses TLSv1.2. On new installations of some Windows OS, SHA-512 is disabled when using TLSv1.2, as described in KB2973337. This means Windows cannot use TLSv1.2 with certificates that have a SHA-512 signature hash algorithm, including those in the certification path (trust chain).

One method of seeing whether your installation is affected, is when Chrome browser refuses to connect to a website, but Internet Explorer allows the connection. Unlike Chrome, if Internet Explorer cannot use TLS 1.2 it will downgrade to TLS 1.0 or 1.1 if enabled in the Advanced tab of Internet Options. If you disable these check-boxes then Internet Explorer will refuse to connect. This issue occurs only when one or more certificates in the trust chain is using SHA-512 as a signature hash algorithm.

To resolve this, you must install relevant updates on each OS as described in the KB, which may already be installed by Windows Updates. However, you may not have updated a new installation, for example in a lab. The table below is a guide only, and you should read KB2973337 first and apply prerequisite updates. A restart is required after each update.

OS	Update	Prerequisites
Windows 10 and later OS	Not applicable	
Windows 8.1 and Server 2012 R2	KB2975719	KB2919442 then KB2919355
Windows 8 and Server 2012	KB2975331	KB2993651
Windows 7 and Server 2008 R2	KB2973337	
Windows XP and Server 2003	KB968730	

2.5.3.3 1E Digital Signing Certificates

As described in Digital signing certificates, the root signing certificate is **DigiCert High Assurance EV Root CA** and the root timestamping certificate is

DigiCert Assured ID Root CA. These must exist in the **Trusted Root Certification Authorities** store, which contains a replica of the **Third-Party Root Certification Authorities** store.

Issue

If the relevant certificates are not available on a Windows computer, then the 1E Client will stop shortly after starting up, and the **1E.Client.log** file will show an error similar to the following.

```
INFO  - Loading providers...
ERROR - Unable to verify signature for 'C:\Program Files\1E\Client\Extensibilit
y\1E.Client.Provider.Cli.dll'
ERROR - Unable to verify signature for 'C:\Program Files\1E\Client\Extensibilit
y\1E.Client.Provider.Http.dll'
ERROR - Unable to verify signature for 'C:\Program Files\1E\Client\Extensibilit
y\1E.Client.Provider.Json.dll'
ERROR - Unable to verify signature for 'C:\Program Files\1E\Client\Extensibilit
y\1E.Client.Provider.Nomad.dll'
ERROR - Unable to verify signature for 'C:\Program Files\1E\Client\Extensibilit
y\1E.Client.Provider.PowerShell.dll'
ERROR - Unable to verify signature for 'C:\Program Files\1E\Client\Extensibilit
y\1E.Client.Provider.Registry.dll'
ERROR - Unable to verify signature for 'C:\Program Files\1E\Client\Extensibilit
y\1E.Client.Provider.TcpIp.dll'
ERROR - Unable to verify signature for 'C:\Program Files\1E\Client\Extensibilit
y\1E.Client.Provider.Wmi.dll'
```

Cause

This occurs when 1E Client is unable to validate the code signing signature of the executables or libraries. This can happen if one or more of the following is true:

- the trusted root certificate of the countersignature is missing from the Windows **Trusted Root Certification Authorities** certificate store - this may be because **Automatic Root Certificates Update** is disabled
- other certificates in the trust path are missing, and Windows is unable to connect to the Internet and dynamically download them during validation.

In either case, the failure to download trusted certificates may be due to the computer being disconnected from the Internet, for example in a lab.

The issue can also affect installation and patching because MSI and MSP files are also countersigned, but that depends on your organizations security policies for software installation.

The issue may not be apparent until after installation, when restarting and not able to connect to the Internet, for example if the computer has been moved into lab.

The root CA certificates are normally automatically provided by Microsoft's Update Root Certificates feature, however this may not be present for legacy OS. You can tell if the root CA certificate is present as follows:

- view the properties of the **1E.Client.exe** file
- select the **Digital Signatures** tab

- select the sha1 signature and click Details (this may take some time to respond while Windows is trying to check the certificate revocation)
- click **View Certificate**
- select the **Certification Path**
- if you do not see **Digicert** at the top of the certification path, then you do not have the root CA certificate

In a lab environment that is not connected to the Internet, the computer may not be able to automatically obtain intermediate CA certificates.

Resolution

Ensure that your Root Certificates are up-to-date. The Update Root Certificates feature is enabled by default but its configuration may have been changed or restricted by Group Policy. You may see *DisableRootAutoUpdate = 1 (dword)* in *HKLM\Software\Policies\Microsoft\SystemCertificates\AuthRoot.*

If disconnected from the Internet, then manually import the certificates for:

- Root CA into the **Third-Party Root Certification Authorities** store or **Trusted Root Certification Authorities** store.
- Issuing CA into the **Intermediate Certification Authorities** certificate store.

You can distribute certificates to client computers by using Group Policy, as described in https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/deployment/distribute-certificates-to-client-computers-by-using-group-policy.

The table below applies to software and hotfixes released in 2020.

2020	Signing certificate	Timestamping certificates
Certificate	1E Limited	TIMESTAMP-SHA256-2019-10-15 ***and*** DigiCert Timestamp Responder
Issuing CA	**DigiCert EV Code Signing CA (SHA2)** Thumbprint: 60ee3fc53d4bdfd1697ae5beae1cab1c0f3ad4e3	**DigiCert SHA2 Assured ID Timestamping CA** Thumbprint: 3ba63a6e4841355772debef9cdcf4d5af353a297 ***and*** **DigiCert Assured ID CA-1** Thumbprint: 19a09b5a36f4dd99727df783c17a51231a56c117

2020	Signing certificate	Timestamping certificates
Root CA	**DigiCert High Assurance EV Root CA** Thumbprint: 5fb7ee0633e259dbad0c4c9ae6d38f1a61c7dc25	**DigiCert Assured ID Root CA** Thumbprint: 0563b8630d62d75abbc8ab1e4bdfb5a899b24d43

2.5.4 Known issues

Lists of the current known issues with implementing, configuring, using and extending Tachyon.

If you need further help, please refer to the Troubleshooting page for how to contact 1E Support and the technical support process.

2.5.4.1 Tachyon

Please refer to Troubleshooting for issues with other components of Tachyon.

2.5.4.1.1 Client installation issues on Windows

Issue	Description	Workaround
1E Client installed on Windows 11 device reports Operating System value as "Windows 10 21H2"	1E Client installed on Windows 11 device reports Operating System value as "Windows 10 21H2".	None
1E Client UI runs even when the Tachyon module is not enabled (e.g. Nomad only install)	Installing the 1E Client without enabling the Tachyon Module (only Nomad or Shopping module is enabled) enables and displays the survey notifications in 1E Client notification icon.	In order to suppress this, the Module.Interaction.Enabled=false can be set in the config file on the 1E Client or use the corresponding MSI property (i.e. MODULE.INTERACTION.ENABLED=false).
TemporaryDirectory config does not work properly with non-ASCII in the path and the	The error is seen if the TEMPORARYDIRECTORY MSI property for the 1E Client contains a non-ASCII value such as "c:\tâ,¬mp\acme€" and the directory exists.	Please provide a path that only uses ASCII values.

Issue	Description	Workaround
following is seen in 1E.Client.logs: `ERROR - Temporary directory: Cannot create file in overriding path 'c:\tâ,¬mp\acme€'; using default location`	The same applies if this is added directly to 1E.Client.conf.	
Manually uninstall of 1E Client using Programs and Features displays dialog "The setup must update files or services that cannot be updated while the system is running. If you choose to continue, a reboot will be required to complete the setup."	Running the 1E Client MSI manually with the Remove option displays the following: "The setup was unable to automatically close all requested applications. Please ensure that the applications holding the files in use are closed before continuing with the installation." These messages appear as the services that are about to be removed are running, but the 1E Client handles the shutdown so this message can be ignored. Silent uninstall does not present this issue.	None
1E Client installer adds the Nomad registry settings even when the Nomad module is NOT enabled during installation. If someone deletes	1E Client installer creates the majority of the Nomad registry values because the service does not create them all and Nomad does not tolerate the absence of all the settings that the service does not create. If these settings are deleted and the Nomad module is enabled later, then Nomad is unable to function correctly.	In such a scenario, 1E Client will need to be reinstalled with a new set of properties / transform that enables the Nomad module with the appropriate configuration.

Issue	Description	Workaround
those registry settings and enables the Nomad module later, Nomad will not function correctly.		
When upgrading an existing 1E Client, none of the manually added configuration file properties in the *.conf file have been retained.	1E Client does not retain any configuration file property values that have been added as the upgrade process currently only checks the default values that exist in the old Tachyon.Agent.conf or new 1E.Client.conf. This includes the Module.Inventory.ProcessUsage.Enabled=false values that was included in Tachyon Agent v4.0. After an upgrade this configuration file property will no longer appear and 1E Client uses the default (true).	The additional configuration file property values need to be added to the 1E.Client.conf file if they are required. Please refer to Tachyon client settings for list of the available configuration options.
When upgrading an existing 1E Client that has been installed to a non-default installation directory, installation folder reverts to the default path.	If the previous Tachyon Agent was installed anywhere other than the default location "%ProgramFiles%\1E\Tachyon\Agent", then the Installation folder in the wizard will revert to the new default path "%ProgramFiles%\1E\Client". The same applies to silent upgrades where the Tachyon Agent was installed to another path, the installation folder will revert to the default unless the required directory is specified using INSTALLDIR.	Please upgrade by specifying the required Installation folder in the wizard or using the installer property: INSTALLDIR
Repair installation of the 1E Client	A repair of the 1E Client will retain the existing configuration file and any non-default settings. However, if the	To rectify this, either run an instruction to configure a relevant

Issue	Description	Workaround
does not keep previous configuration changes and some Nomad registry settings will have BLANK values.	configuration file had been deleted, then a repair will not be able to apply previous settings and will use default settings. Also a repair will set any properties passed in the command line, but will leave some Nomad properties like KnownMobileDevices and LocalCachePath as blank.	setting, or re-install the 1E Client using desired settings. Use a 1E Client configuration instruction in Explorer for centralized post-installation configuration. Please contact 1E if you require the Product Pack that has this instruction.
Potential blue screen of death (BSOD) with Windows 7 SP1 and Tachyon inventory capture.	If Tachyon inventory is enabled on Windows 7 SP1 (without updates) there is the potential for BSOD issues on systems using out of date Windows drivers. Microsoft investigated the issue and confirmed the **usbccgp.sys** driver has a potential issue where it can fail to complete a power IRP in a timely manner.	Microsoft recommends the following fix: 1. Update the **usbccgp.sys** driver as follows: • – Update the **usbccgp.sys** driver by installing update KB3125574. Prerequisites: To apply this update, you must first install: • – Service Pack 1 for Windows 7 or Windows Server 2008 R2: KB976932 – April 2015 servicing stack update for Windows 7 and Windows Server 2008 R2: KB3020369 2. Update **tdx.sys** to 6.1.7600.21050 to address TDI driver response issues as per: KB2028827

Issue	Description	Workaround
Tachyon features of the 1E Client cannot read private key for a Trusted Platform Module (TPM) protected certificate.	The client uses the Windows certificate store but is currently unable to access the private key of a client certificate that is protected using the Windows Trusted Platform Module (TPM). This issue was seen when a customer used Microsoft Intune for client certificate deployment and the Simple Certificate Enrollment Protocol (SCEP) certificate profile included 'Enroll to Trusted Platform Module (TPM) KSP'. The 1E Client was unable to extract a handle to the private key in the Windows Certificate Store; 'NCryptExportKey failed with 0x8009000a' (NTE_BAD_TYPE) was reported as an error in the 1E Client log.	Use a client certificate that is not protected using Windows Trusted Platform Module (TPM). Examples of Microsoft cryptography providers that do not use TPM are: • Microsoft Enhanced (RSA and) AES Cryptographic Provider • Microsoft RSA/SChannel Cryptographic Provider • Microsoft Enhanced Cryptographic Provider • Microsoft Software Key Storage Provider (CNG). Also, Microsoft Software Key Storage Provider is the only CNG provider supported by this version of the client.

2.5.4.1.2 Client connection issues

Issue	Description	Workaround
1E Client fails to connect to the Switch with following error: ERROR - Failed to connect to tachyon.acme.local: invalid padding (138)	During the establishment of an https connection between the client and the Switch, the client receives and verifies the Switch certificate. This is received from the Switch as an X.509 certificate chain, from which the 1E Client will extract the Switch's public key and verify the certificate chain. On a successful SSL handshake where the CRL is checked, it will report both the serial number of each certificate as it walks the chain and the Authority Key Id (AKID) of the CA that issued that certificate. This is stored in the 1E Client	Delete the cached certificate entries in the 1E Client persistent storage (default location is C:\ProgramData\1E\Client\Persist) and restart the 1E Client.

Issue	Description	Workaround
	persistent storage and re-used until it has expired. If the 1E Client connects to another Switch where the certificate chain is different (e.g. CA certs have been re-issued), the 1E Client may log the following warning since there is a mismatch of the Authority Key Id (AKID) saved in the persistent storage from previous CA: WARN - X509: error:04067072:rsa routines:rsa_ossl_public_decrypt:padding check failed WARN - X509: error:0D0C5006:asn1 encoding routines:ASN1_item_verify:EVP lib WARN - X509: error:1416F086:SSL routines:tls_process_server_certificate: certificate verify failed	
Non-Windows clients may disconnect due to the keep-alive period being too high.	Clients on Non-Windows may disconnect if the keep-alive period is too high. Non-Windows clients need to have a maximum keep-alive time of 4 minutes (240s).	The keep-alive time needs to be updated in the 1E.Client.conf file: *ConnectionKeepaliveTimeInSecondsMin* should be set to 120 (default) and *ConnectionKeepaliveTimeInSecondsMax* should be set to 240 (default is 600). These settings can be set during installation or changed post-install.
A client does not start and the 1E Client log shows: ERROR - Certificate Verification failed : CRL path validation error.	The client will not connect if it is unable to create a trust chain, despite having the correct root CA certificates. This is due to the local computer certificate store containing "CrossCA" certificates.	Please ensure the client certificate store does not contain any "CrossCA" certificates in the local Trusted Root or Intermediate CA stores.

Issue	Description	Workaround
This occurs even when CRLChecks=soft.		
The client is unable to start on the Root CA.	A client attempting to run on a Root CA server will log the following error: WinTrustVerify returns 0x800b010a (CERT_E_CHAINING) “A certificate chain could not be built to a trusted root authority” A Root CA sits at the top of the public key infrastructure (PKI), there are no higher authorities, and so it effectively self-signs its certificates, which Tachyon is specifically prevented from using.	It is not good security practice to have a Root CA online therefore do not install the Tachyon client. You could configure your system to not use client certificates.
Resetting Hyper-V Agents can cause the Switch to become unresponsive and log erroneously.	Powering off or resetting a guest Hyper-V virtual machine without shutting it down, can cause the Switch to refuse connections from the client when it restarts, and the Switch starts spurious logging.	To rectify this issue restart both the Switch and the 1E Client service.
The client fails to start and the 1E Client log shows errors relating to Certificate Revocation List (CRL).	See Tachyon client settings. An error is logged if CRLChecks=hard and the client is unable to locate a valid HTTP-based CRL Distribution Point for a certificate. An error is logged if CRLChecks=soft and the client is able to get a CRL from the CRL DP, but the CRL indicates revocation of the device certificate or a certificate in its trust path. The client requires a valid SSL certificate presented by each server it connects to.	If the machine is not be able to contact a HTTP-based CRL Distribution Point, please ensure *CRLChecks=soft within* the *1E.Client.conf* file. This will prevent the client from failing in the event of being unable to locate a CRL Distribution Point

Issue	Description	Workaround
	This includes any Switch, Background Channel or other HTTPS server from which the client downloads content. The client does not connect to a server if it knows a certificate is invalid. CRLs are obtained by contacting the CRL Distribution Point(s) whose URL is embedded within the certificates. At present, the client supports only HTTP-based CRL Distribution Points. It ignores any non-HTTP CRL DPs that may be included in a certificates, such as file or LDAP, and does not support OCSP.	
Enabling, disabling, adding or removing network adapters on the 1E Client Server computer will cause issues with Switches issuing instructions or unable to use features like "Export All Results".	The 1E Client Server Core web applications have access restricted by the IIS feature **IP Address and Domain Restrictions**. All connections are denied, except for local connections. Changing adapter configuration after installation can cause the entries in the IIS feature to become incorrect and cause issues with 1E Client Server. If for example the IPv6 address assigned is different from the one which was installed by 1E Client, then Tachyon.Workflow.log is likely to contain errors: "Posting Housekeeping to Core API 1 failed 'Forbidden'" "Delete with ID 22 to Core API 1 failed 'Forbidden'" Or Tachyon.ConsumerAPI.log may have "Data export fail" errors when attempting to "Export All Results".	Please update entries in the **IP Address and Domain Restriction** feature of the CoreInternal and the Core website to include all local IP v6 and v6 addresses. Please refer to IP Address and Domain Restrictions.

2.5.4.1.3 Client issues specific to non-Windows

Issue	Description	Workaround
Microsoft InTune cannot be used to deploy the 1E Client package for macOS.	By design, Microsoft InTune can only be used to deploy macOS packages to the /Applications folder. However, the 1E Client must be installed to /Library/Application Support since that is a secure location, writable only by root. Also the associated launch property list file must be installed under /Library/LaunchDaemons.	Use an alternative deployment method for the 1E Client macOS package.
The 1E Client on macOS may not be able to validate the switch certificate if there is a cacert.pem in the .sslcerts folder that does not contain the relevant list of CA public keys. The following is logged: ERROR - Either the Switch certificate or the client certificate is not trusted, use the 1E Client debug log setting to obtain	If the 1E Client for macOS finds a valid cacert.pem in the hidden directory: */Library/Application Support/1E/Client/.sslcerts*, then the Keychain Access is not checked. This cacert.pem is then used to validate the trust chains for the client certificate the client will submit and also the Switch certificate received. The client will be unable to connect to the Switch if it does not contain the relevant list of CA public keys to do the validation.	Ensure the cacert.pem contains all the public keys for all the intermediate CAs, up to and including the Root CA required. Alternatively, remove the cacert.pem if the 1E Client for macOS is to use the certificates from the Keychain Access.

Issue	Description	Workaround
certificate details.		

2.5.4.2 Nomad

Please refer to /document/preview/675710#UUID-ed88d585-22d1-0311-3246-8f71845db40c for issues with other components of Nomad.

2.5.4.2.1 Client installation issues

Issues	Description	Workaround
1E Client installer adds Nomad registry settings even when Nomad module is NOT enabled while installation. If someone deletes those registry settings and enables the module later, Nomad won't function correctly.	The installer is currently creating the majority of Nomad registry values because the service doesn't create them all and Nomad doesn't tolerate the absence of all the settings that the service doesn't create. If someone deletes those settings and enables the Nomad module later, Nomad won't function correctly.	In such a scenario, we recommend reinstalling the 1E Client with a new set of properties / transform that enables the Nomad module. This will be fixed in a future release of 1E Client.
On Windows XP, 1E.Client.log displays a warning "Unsupported OS version. Will not install Nomad." however the very next log lists that "Module 'Nomad' has been installed".	Nomad is not supported on Windows XP therefore when 1E Client is installed with the Nomad module, the module is not enabled, and the Nomad Branch service is not installed.	None.
Nomad may be downgraded by active Application deployments in CM, which may cause	If there is an active Application deployment in CM of an earlier version of Nomad, clients that have been upgraded with	To avoid this situation, always define Application Supersedence on the 1E Client Application such that it supersedes any Applications that install previous versions

Issues	Description	Workaround
issues with behaviour of the 1E Client Nomad module.	the 1E Client with the Nomad module enabled may be downgraded when the Application Enforcement cycle runs. In this scenario, if the Nomad module is subsequently disabled in the 1E Client, the Nomad service will be removed. This is because once the Nomad module has been enabled, it is not aware nor does it check for older versions. If the Nomad module is subsequently disabled, the service is removed as the Nomad module believes it is not longer required.	of Nomad (and the 1E Client when introducing new versions of the 1E Client). To resolve this issue should it occur, first address the Application Supersedence to prevent it from recurring. Then run the following command from the 1E Client installation directory on the affected devices. *1E.Client.exe -reconfigure MODULE.NOMAD.ENABLED=false -restart & 1E.Client.exe -reconfigure MODULE.NOMAD.ENABLED=true -restart* This will disable the Nomad module and remove the Nomad service, then re-enable the Nomad module, which will, in turn, uninstall the earlier version of Nomad and install the Nomad module. The settings defined by the earlier Nomad install will be migrated - these may differ from the settings with which the Nomad module was initially configured.
1E Nomad Branch and 1E Client Health services may be stopped if upgrading to Nomad 8.0 if previous version of Nomad installer is no longer in source folder or the Windows Installer cache.	The 1E Client installer stops the 1E Nomad Branch and 1E Client Health services if the Nomad module is enabled. The 1E Client installation completes successfully, after which the Nomad module attempts to uninstall the older version of Nomad. The uninstallation fails as Windows Installer cannot find the original source installer. The Nomad module is not enabled and the Nomad and Client	In this scenario, to immediately restore Nomad functionality simply start the services. To fix it completely you will need to remediate the installer source for the old version of Nomad on the affected client, then run the following command from the 1E Client installation directory to restart the 1E Client service. *1E.Client.exe -restart*

Issues	Description	Workaround
	Health services remain stopped.	
Uninstalling 1E Client doesn't delete Nomad's P2P server certificate.	When P2PEnabled value was set to 79 then NomadBranch server certificate does not get deleted after uninstallation.	
NomadBranch - 1E Client - Creation of Nomad COM object failed with 0x80070424	Install the latest build with Nomad. Creation of Nomad COM object failed with 0x80070424-	Disable the Nomad module and restart the 1E Client service. Enable Nomad again and restart the 1E Client service. Nomad should install successfully.
Nomad users see the 1E Client UI in the device system tray even when the Tachyon module is not enabled.	The 1E Client UI runs despite only the Nomad or Shopping modules being installed, without the Tachyon feature enabled.	None.

2.5.4.3 PXE Everywhere

Please refer to Troubleshooting for issues with other components of PXE Everywhere.

2.5.4.3.1 Client installation issues

Issue	Description	Workaround

PXE Everywhere is not responding as expected. Log file shows messages similar to:
 	
`Error: failure to bind to 192.168.18228:69.`
`The specified address is already in use`
`TFTP: retry in 1000ms`
`Error: failure to bind to 192.168.18228:40`
	PXE Everywhere Agent and PXE Everywhere Responder cannot co-exist on the same computer and are not supported together. Whilst it is possible to install them together, they will not work and will have issues such as failure to bind to ports.	Either uninstall PXE Everywhere Responder, or disable PXE Everywhere module in 1E Client. Then restart the computer, or restart the relevant service (PXE Everywhere or 1E Client).

Issue	Description	Workaround
11. The specified address is already in use DHCP: retry in 1000ms		
PXE Everywhere Agent fails to connect to PXE Everywhere Central.	An incorrect URL has been specified during installation of PXE Everywhere Agent. The installer wizard does not validate the PXE Lite Central URL is provided during the PXE Lite Local GUI installation.	Ensure you specify the correct URL when installing PXE Everywhere Agent.
PXE Everywhere does not support RISC based architecture.	PXE Everywhere does not support RISC based architecture and therefore not able to PXE boot clients using RISC. For instance, architecture being used by Microsoft Surface Pro 10 LTE Models is ARM 64-BIT UEFI (11) which is a RISC architecture and *not* recognized by PXE Everywhere.	None.
PXE Everywhere Agent installation fails when an unprivileged user installs it after providing administrator credentials (UAC prompted) for installation.	PXE Everywhere Agent installation fails with error when an unprivileged user initiates PXE Everywhere Agent installation even after validating credentials after UAC prompt.	When installing the agent interactively, run the installer from a command prompt with elevated permissions.

2.5.4.4 WakeUp

2.5.4.4.1 Client installation issues

Issue	Description	Workaround
No issues known.		

2.5.4.5 Shopping and WSA

Please refer to Shopping 6.1 - Troubleshooting for issues with other components of Shopping, and WSS 4.1 - Troubleshooting.

2.5.4.5.1 Client installation issues

Issue	Description	Workaround
Shopping module does not send machine details on a TLS enabled Windows 7 environment	The Shopping module in the Tachyon 3.2 Agent fails to send machine details on a TLS enabled Windows 7 (32 and 64 bit) environment.	
Firefox prompts you to restart the browser when connecting to the Shopping website. After restarting you are no longer prompted.	Firefox must be restarted to allow changes made by Shopping client to take effect. The Shopping Console has a setting for WSA**Firefox support enabled**. The Shopping client module reads this setting from Shopping Web and if enabled (default is true) then it does the following: • Creates a certificate chain of a CA certificate and a leaf certificate signed by the CA certificate • Configures Firefox to import certificates from the standard Windows certificate store (by default Firefox uses its own certificate store). This Console setting for WSA is only required if using Firefox and HTTPS because Firefox is stricter in which certificates it accepted on an HTTPS connection and by default uses its own certificate store. The WSA setting can be disabled in the Shopping Console if only using other browsers, or not using HTTPS. 1E Client log shows entries: *INFO - Added '1E Ltd CA Certificate' certificate to ROOT certificate store* *INFO - Added '1E Ltd localhost Certificate' certificate to MY certificate store*	If you are using Shopping HTTPS then use Internet Explorer or Chrome browsers to login to Shopping. If you are using Firefox browsers with a Shopping HTTTPS website then you will need this. If you are using Shopping HTTP website then you can disable the Shopping Console setting for WSA **Firefox support enabled**.

2.6 Reference

All the list type information, such as installer properties, in alphabetical lists etc.

2.6.1 1E Client configuration settings and installer properties

Settings are available in the 1E Client configuration file, with details of which settings are mandatory or optional during installation, and which settings can be re-configured post-installation.

1E Client installers include a **template configuration file** that contains the more important settings with default values that match hard-coded default values. The configuration file is updated during installation and named **1E.Client.conf** in the installation folder along with the 1E Client executable.

After installation, configuration file settings can be managed using 1E Client command-line parameters, Explorer configuration instructions, Guaranteed State policies, Configuration Manager baselines, or other means. Registry settings can also be managed by Windows Group Policy.

2.6.1.1 1E Client installer zips

Zip files for **1E Client** installers can be downloaded from the https://support.1e.com/. The following installer zips are available and contain the following files, where **8.0.x.xxx** is a specific build:

1EClient.v8.0.x.xxx.zip	1EClient_Non-Windows.v8.x.x.xxx.zip
• Release Information.html • **1EClient-x64.msi** • **1EClient-x86.msi** • Licenses.txt	• Release information.html • **1e.client-CentOS_8_x64_v8.x.x.xxx.rpm** • **1e.client-Debian_10.4_x64_v8.x.x.xxx.deb** • **1e.client-Fedora_34_x64_v8.x.x.xxx.rpm** • **1e.client-macOS_v8.x.x.xxx.dmg** • **1e.client-macOS_v8.x.x.xxx.pkg** • **1e.client- openSUSE_Leap_15.2_x64_v8.x.x.xxx.rpm** • **1e.client-RHEL_7.9_x64_v8.x.x.xxx.rpm** • **1e.client-RHEL_8.5_x64_v8.x.x.xxx.rpm** • **1e.client-SLES_15.2_x64_v8.x.x.xxx.rpm** • **1e.client-Ubuntu_18.04_x64_v8.x.x.xxx.deb** • Licenses.txt

Please refer to Supported Platforms for details of supported OS versions and their prerequisites.

2.6.1.2 Deploying the 1E Client

2.6.1.2.1 Windows computers

When deploying 1E Client to Windows devices you can install using the MSI interactively but this only allows you to specify some configuration settings. You can configure these and some other settings using installer properties on the command line or in one or more MST transform files.

The Introducing 1E Client Deployment Assistant is designed to help install Windows versions of 1E Client and other 1E agents using Configuration Manager. It includes template transform files for each combination of client/agent for 32 and 64-bit platforms, and automatically creates collections and deployments in Configuration Manager so that you only need to populate the collections.

Please refer to:

- Installing the 1E Client interactively
- Installing the 1E Client by command-line.

2.6.1.2.2 Non-Windows devices

Please refer to:

- Deploying 1E Client on macOS
- Deploying 1E Client on Linux
- Deploying 1E Client on Solaris.

2.6.1.2.3 1E Client settings

Configuration settings can be set during or after installation, depending on the platform, as described in the table below. Installer command-lines are described in Deploying 1E Client on Windows.

Platform	Notes
Windows	• Some settings may be set during installation and others can only be set in the configuration file • Setting names is not case sensitive • You must use UPPERCASE when specifying the *name* of any installer property in a **mst** transform file, and preferably when including them in a msiexec command-line. • Nomad, PXE Everywhere, and WakeUp client modules have settings that are stored in the registry instead of the configuration file.
Linux	• Settings may be set during installation or modified in the configuration file • Setting names is not case-sensitive.

Platform	Notes
Mac and Solaris	• Settings must be set after installation using the supplied bash script • Setting names is not case-sensitive.

The following applies to all configuration settings that are stored in the 1E Client configuration file:

- They can be reconfigured after installation either manually or as described in 1E Client command-line parameters
- Property names and values are not case-sensitive, but the convention is to store them in mixed-case
- If you omit a mandatory property or its value, the 1E Client will not start
- If you omit an optional property or its value, the 1E Client will use the default value instead.

2.6.1.3 1E Client configuration file location and name

The 1E Client is controlled via the 1E Client configuration file **1E.Client.conf** which resides in the installation folder along with the 1E Client executable.

The default installation location used for the different OS supported by the 1E Client are given in the following table:

OS	Default install location
Windows	**%ProgramFiles%\1E\Client**
Linux and Solaris	**/etc/1E/Client**
Mac	**'/Library/Application Support/1E/Client'**

Note

The configuration file uses ASCII encoding.

A comment line starts with the # symbol.

2.6.1.4 Installer properties and configuration settings

The following are alphabetical lists of all **installer properties** and **configuration settings** for 1E Client modules and features.

Those **installer properties** listed in mixed case are stored in the 1E Client configuration file, and those listed in UPPERCASE are stored in the registry. Where relevant, the locations of Windows registry settings are provided.

Note

You must use UPPERCASE when specifying the *name* of any installer property in a **mst** transform file, and preferably when including them in a msiexec command-line.

Note

Names of settings stored in the configuration file are not case-sensitive. Setting names stored in the registry may be case-sensitive and should be specified as shown.

2.6.1.5 1E Client settings

Installer and configuration settings for 1E Client which affect all client features and modules.

Note

Installer properties:

DataRoot | INSTALLDIR | LogPath | TemporaryDirectory

Note

Configuration file settings:

DataRoot | LogPath | TemporaryDirectory

Please refer to the following pages when deploying 1E Client.

- Deploying 1E Client on Windows
- Deploying 1E Client on macOS
- Deploying 1E Client on Linux
- Deploying 1E Client on Solaris
- Reconfiguring 1E Client
- Verifying

1E Client installers include a **template configuration file** that contains the more important settings with default values that match hard-coded default values. The configuration file is updated during installation and named **1E.Client.conf** in the installation folder along with the 1E Client executable.

After installation, configuration file settings can be managed using 1E Client command-line parameters, Explorer configuration instructions, Guaranteed State policies, Configuration Manager baselines or other means. Registry settings can also be managed by Windows Group Policy.

2.6.1.5.1 1E Client settings

Note

You must use UPPERCASE when specifying the *name* of any installer property in a **mst** transform file, and preferably when including them in a msiexec command-line.

Names of settings stored in the configuration file are not case-sensitive. Setting names stored in the registry may be case-sensitive and should be specified as shown.

Settings that have numeric values must be set using decimal integers, unless otherwise specified.

Setting	Default	Description
DataRoot	%ALLUSERSPROFILE%\1E\Client	Sets the root directory under which the Client will create the **DBs** and **Persist** subfolders and hence the locations of the databases and persistent storage within the local file system. If the specified directory doesn't exist it will be created. Local System (SYSTEM) requires at least modify rights on the directory. If the specified directory is invalid, or cannot be used, the 1E Client will log an error and refuse to start. For example if the directory name is a file, non-existent volume, or SYSTEMdoes not have permission. If not specified, the default is the **%ALLUSERSPROFILE%\1E\Client** directory. This is also the default location of client log files, which are not affected by this setting. The location and name of the 1E Client log file is determined by the LogPath setting. Please refer to Log files for details of other client log files. **Note** By default, Windows resolves %ALLUSERSPROFILE% as C:\ProgramData\ **Note** This setting is for Windows only. It is ignored on non-Windows platforms, without warnings or errors logged. Do not use this setting unless required, for example if security software unavoidably conflicts with 1E Client.

Setting	Default	Description
INSTALLDIR	%ProgramFiles%\1E\Client	Sets the installation folder. This value is not stored in the 1E Client configuration file. This value is stored as **InstallationDirectory** in the Windows registry under HKLM\SOFTWARE\1E\Client\ and must not be changed. Some client modules that run on Windows store their registry settings under their own keys in HKLM\SOFTWARE\1E. **Note** This installer property is for Windows only.
LogPath	**1E Client logs on Windows** %ALLUSERSPROFILE%\1E\Client\1E.Client.log **1E Client logs on macOS** /Library/Logs/1E.Client.Daemon.log (shows any service start errors) /Library/Logs/1E.Client.log (shows the current operation of the 1E Client) **1E Client logs on other non-Windows platforms** /var/log/1E/Client/1E.Client.log	The **LogPath** setting is stored in the **1E.Client.Conf** file and determines the full path and filename of the 1E Client log file. The 1E Client log is shared by: • 1E Client • Tachyon client features • Shopping client module (only available on Windows OS) To change the logging level, please refer to LoggingLevel in the 1E.Client.CONF file. The following are not configurable in this version: • Maximum size of 5MB • 5 rollover files numbered 1 (newest) to 5 (oldest) with the

Setting	Default	Description
		rollover number included as n.log **Note** By default, Windows resolves %ALLUSERSPROFILE% as C:\ProgramData\ The LogPath setting is not used by Nomad, PXE Everywhere, and WakeUp client modules. For a fresh install they use their defaults, and for upgrades they re-use what is in their registry. In each case these can be over-ridden by installer properties described in Content Distribution client settings, PXE Everywhere Agent settings, and /document/preview/647736#UUID-b588cdab-ae07-3331-ceb1-c8c6ed63aa1e. Shopping WSA also has its own configuration file. Please refer to Log files for more details.
TemporaryDirectory	*(none)*	The **TemporaryDirectory** setting is stored in the **1E.Client.Conf** file specifying the directory path below which the 1E Client and its subprocesses will create temporary files and subdirectories. The following table shows the OS-specific defaults used if the setting is omitted, blank, or invalid. The default is recommended. Platform: Windows; Environment Variable(s): TMP; Default: *%windir%\Temp* which is the

Setting	Default	Description		
			TEMP	default *%TEMP%* location for SYSTEM.
		Linux	TMPDIR	/tmp

Tip

Using this setting to specify a non-default value is only necessary if the OS default location is not suitable. For example, some security software forbids scripts being run from certain locations. Or you want to simplify configuration of Windows anti-virus and malware software to the same location as 1E logfiles.

The specified directory:

- Must be an absolute path appropriate for the OS
- Must already exist - it will not be created
- Must be writable by the 1E Client (SYSTEM on Windows, root on Linux)

If any of these criteria is not satisfied then the 1E Client and subprocess falls back to using the default temporary directory.

If the value is validated successfully then environment variables are set so that subprocesses inherit the same temporary directory.

Warning

Setting	Default	Description
		The path can only contain ASCII characters but that is not validated. Unicode characters are not supported. **Note** The 1E Client itself creates a subdirectory under the specified path called ***1e.client*** which it uses for its own temporary files and directories. Subprocesses invoked by the 1E Client, such as commands, PowerShell scripts, etc. create their temporary files directly under the specified path. **Note** This setting was introduced in a v5.0 hotfix.

2.6.1.6 Platform features of the 1E Client

Configuration file settings, and their installer properties, for the platform features of the 1E Client.

Note

Configuration file settings and installer properties:

Note

Some configuration file settings do not have equivalent installer properties. These are indicated in the tables below.

Note

- Core settings common to Windows and non-Windows platforms:
  - AuthenticationPolicy | BackgroundChannelUrl | ConnectionKeepaliveTimeInSecondsMin | ConnectionKeepaliveTimeInSecondsMax | ConnectionRetryTimeInSecondsMin | ConnectionRetryTimeInSecondsMax | ConnectionTimeout | CRLChecks | DefaultStaggerRangeSeconds | EnablePayloadCompression | LoggingLevel | LogPath | PolicyEnabled | SSL | Switch | WorkerThreads

- Core settings for Windows only:
  - NomadContentDownloadEnabled | NomadContentDownloadTimeoutSecs
- Interaction module settings (only supported on Windows):
  - Module.Interaction.Enabled | Module.Interaction.ActiveSessionThresholdSeconds | Module.Interaction.CompanyName | Module.Interaction.DoNotDisturb | Module.Interaction.IdleSessionThresholdMinutes | Module.Interaction.ITSM.ServiceNow.CreateIncidents | Module.Interaction.ITSM.ServiceNow.Enabled | Module.Interaction.ITSM.ServiceNow.GoBackDays | Module.Interaction.ITSM.ServiceNow.Url | Module.Interaction.LogSessionNotificationReadiness | Module.Interaction.MinimumMinutesAfterLogonBeforePrompt | Module.Interaction.MinimumMinutesAfterSessionActivationBeforePrompt | Module.Interaction.MinimumMinutesBetweenPrompts | Module.Interaction.NotificationIcon | Module.Interaction.PeriodsBeforeUiLaunch | Module.Interaction.PeriodsBeforeUiLaunchTimeout | Module.Interaction.Port | Module.Interaction.ResponseAuditsBeforeTidy | Module.Interaction.ResponseRetentionRows | Module.Interaction.SampleExclusionList | Module.Interaction.SampleUserInteraction | Module.Interaction.SnoozeTimeMinutes | Module.Interaction.Theme
- Inventory module settings:
  - Module.Inventory.Enabled | Module.Inventory.NoEventTracing | Module.Inventory.AggregationIntervalSeconds | Module.Inventory.<source>.Enabled | Module.Inventory.<source>.BufferSize | Module.Inventory.<source>.PollIntervalSeconds | Module.Inventory.<source>.AggregationsBeforeGroom | Module.Inventory.<source>.LiveRetention | Module.Inventory.<source>.HourlyRetention | Module.Inventory.<source>.DailyRetention | Module.Inventory.<source>.MonthlyRetention | Module.Inventory.ProcessStabilization.Fuzziness | Module.Inventory.ProcessStabilization.MonitoredProcesses | Module.Inventory.ProcessUsage.VerboseLogging | Module.Inventory.UserUsage.VerboseLogging
  - Where <source> is:
    - ARP | BootPerformance | DeviceInteraction | DevicePerformance | DeviceResourceDemand | DNS | OperatingSystemPerformance | PerformanceEvent | Process | ProcessStabilization | ProcessUsage | SensitiveProcess | Software | SoftwareInteraction | SoftwarePerformance | TCP | UserUsage
  - Additional settings common to Windows and non-Windows platforms that are only available in the Configuration file, not as installer properties:

- CRLTimeoutInSeconds | FastReconnectTimeInSeconds | SelectRowsLimit

Additional Windows installer properties that are not available in the Configuration file: TAGS

1E Client installers include a template configuration file that contains the more important settings with default values that match hard-coded default values. The configuration file is updated during installation and named **1E.Client.conf** in the installation folder along with the 1E Client executable.

After installation, configuration file settings can be managed using 1E Client command-line parameters, Tachyon Explorer configuration instructions, Guaranteed State policies, Configuration Manager baselines or other means. Registry settings can also be managed by Windows Group Policy.

2.6.1.6.1 Windows installer properties

Note

You must use UPPERCASE when specifying the *name* of any installer property in a **mst** transform file, and preferably when including them in a msiexec command-line.

Names of settings stored in the configuration file are not case-sensitive. Setting names stored in the registry may be case-sensitive and should be specified as shown.

Settings that have numeric values must be set using decimal integers, unless otherwise specified.

The following table shows Windows installer properties for the Tachyon client, that are not available in the client configuration file. They can be set only during installation, by specifying on the command line or in a **mst** transform file.

Installer property	Default	Description
TAGS	*(empty)*	Configures one or more device and freeform tags, either on the msiexec command-line in or in a **mst** transform file. For more information about transform files please refer to Advanced configuration. The format of the installer property is: [*]<Tag1>=<Value1>|[*]<Tag2>=<Value2>|…|[*]<Tagn>=<Valuen> Where: • **<Tag>** is the name of a tag. The name must be prefixed with an asterisk ***** if it is a device tag • **<Value>** is the value for that tag. Use the pipe | delimiter when specifying more than one tag. For example, the following would be added to the command-line to set a device tag **Department=Finance** and a freeform tag **Persona=Clerk**

Installer property	Default	Description

- TAGS="*Department=Finance|Persona=Clerk"

Double-quotes - these are recommended when using a command line, as shown in the above example, and required if any tag values have spaces. Double quotes are not required in a **mst** transform.

This optional installer property is only available *during* installation or upgrade of 1E Client on Windows OS. It is not available in the client configuration file. To configure device and freeform tags *after* installation, you must use Tachyon instructions, as described in Tagging client devices.

Note

You can only use the device tags in the coverage feature of Explorer, if you have also added the tag in the Device Tags page in Tachyon Platform Settings.

2.6.1.6.2 Settings for platform features of the 1E Client

The following table shows 1E Client settings for Tachyon platform features; all are included in the template configuration file except where indicated.

Note

Tachyon client must be enabled to use platform or Content Distribution features of the Tachyon Platform.

If neither Tachyon platform or Content Distribution client features are not required then the connection to Tachyon Platform is not required, and both **Switch** and **BackgroundChannelUrl** settings must be set to **none** when doing a non-interactive (silent/quiet) install using installer properties on a command-line or in a **mst** transform file.

When doing an interactive install then you must uncheck the **Enable Tachyon** checkbox. Platform features are not required if the 1E Client is being installed only to support basic Content Distribution, PXE Everywhere, Shopping, or WakeUp.

Core setting	Installation default	Description
AuthenticationPolicy	Required	Determines whether the Tachyon client presents a certificate when authenticating with a Switch. A Switch will reject a connection if configured to **require certificates from clien**

Core setting	Installation default	Description
		ts and a client does not present a valid certificate. The value must be set to one of the following. The default value is set to **Required**. **Note** The default applies to new installations of the 1E Client. Upgrades from a previous version always retain the existing setting as defined in 1E.Client.conf. **Value** — **Description** none — Do not present a certificate. This option is not visible when installing the 1E Client interactively, but can be configured using a command-line installer property. optional — Present a certificate if a suitable one exists. If none exists continue with the connection anyway. This is the default value.

Core setting	Installation default	Description	
			This option is useful if you are deploying the 1E Client before you have deployed certificates. Switches can be configured so they do not require client certificates, but if you did not select that option during installation then you can change the server setting.
		required	Present a certificate if a suitable one exists, otherwise fail the connection.
BackgroundChannelUrl	*(none)*		If Tachyon and Content Distribution client features are not required then the connection to Tachyon Platform is not required, and both **Switch** and **BackgroundChannelUrl** settings must be set to **none** when doing a non-interactive (silent/quiet) install using installer properties on a command-line or in a MST transform file. When doing an interactive install then you

Core setting	Installation default	Description
		must uncheck the **Enable Tachyon** checkbox. Tachyon client features are not required if the 1E Client is being installed only to support PXE Everwhere, Shopping, or WakeUp. They are only required for Content Distribution if using Content Distribution features of the Tachyon Platform. To connect to the Tachyon platform then **BackgroundChannelUrl** will have one or more entries in the format: `BackgroundChannelUrl=https://<BackgroundChannelServer>:<BackgroundChannelPort>/Background/` **<BackgroundChannelServer>** is the DNS Name FQDN of the server, which is the same as: • the HTTPS Host Header specified on the *Website Configuration* screen of Tachyon Setup, which is the HTTPS binding for the Tachyon website • the same as <SwitchName> • the DNS Name specified in the Tachyon Server's Web Certificate

Core setting	Installation default	Description
		<BackgroundChannelPort> is the Port number, which is the same as: • the HTTPS Port specified on the *Website Configuration* screen of Tachyon Setup, which is the HTTPS binding for the Tachyon website • if using the default HTTPS port 443, the port can be omitted from the URL In systems with multiple server and multiple DNS Names, there will be multiple entries on one line using a semi-colon (;) as the delimiter between entries. For example: `BackgroundChannelUrl=https://tachyon.acme.local:443/Background/;https://tachyon.acme.com:443/Background/` Multiple DNS Names may exist in complex systems where there are multiple servers, Switches, and devices on different networks, such as the Internet as well as the corporate network. Each time Tachyon needs to download content, it will try each entry in turn, starting at the first, until it is able to download or stops trying and reports an error.

Core setting	Installation default	Description
ConnectionKeepaliveTimeInSecondsMin	600 (10 minutes)	Determines the time in seconds for the Tachyon client to wait between sending a keep-alive messages to the Switch. Tachyon client will wait a random amount of time between the two values set as minimum and maximum. Range is 0 to 900 seconds (No keepalive to 15 minutes).
ConnectionKeepaliveTimeInSecondsMax	840 (14 minutes)	
ConnectionRetryTimeInSecondsMin	30 (seconds)	Determines the time in seconds the Tachyon client waits before trying to reconnect to a Switch after a connection failure. The Tachyon client tries once for each Switch in the list of Switches, and if it fails to connect then it waits before trying again. The wait is a random amount of time between the two values set as minimum and maximum. Range is 5 to 86400 (5 seconds to 24 hours). See also FastReconnectTimeInSeconds.
ConnectionRetryTimeInSecondsMax	900 (15 minutes)	
ConnectionTimeout	30 (seconds)	The maximum time in seconds that can elapse between the Tachyon client initialising the

Core setting	Installation default	Description
		connection with a Switch and having a fully established websocket. Range is 1 to 60.
CRLChecks	soft	Determines whether Tachyon client does Certificate Revocation List (CRL) checking for: • the certificate it presents to the Switch when requesting a connection (see also AuthenticationPolicy, which determines whether Tachyon clients present a certificate or not) • the certificate received from the Switch when requesting a connection • the certificate received from the Background Channel server before attempting to download content • the certificate received from any other HTTPS-based endpoint from which Tachyon client downloads content • the certificates used for digital signing of 1E Client executables (typically the certificate is found in

Core setting	Installation default	Description
		the Trusted Publishers Store) The value must be set to one of the following. The default value is set to **soft**. Value — Description off — No CRL checking is performed by the 1E Client. soft — This is the default. Full CRL checking is performed by the 1E Client for each certificate in the list above. However if a CRL Distribution Point (CDP) is unreachable then only a warning will be reported. A certificate error occurs if a CDP is available and the CRL cannot be retrieved or refreshed, or the certificate is revoked. hard — Full CRL checking is performed by the 1E Client for each certificate in the list above. If a certificate error occurs then Tachyon client stops

Core setting	Installation default	Description
		processing the request. A certificate error occurs if a CDP is not available, or the CRL cannot be retrieved or refreshed, or the certificate is revoked. If a certificate error occurs then Tachyon client will not proceed, or will not start in the case of a digital signing certificate error. **Note** By default, the Switch will reject the connection if it cannot check a certificate presented by Tachyon client. Please contact your 1E Account Team if you need help with configuring Switches if you are unable to use CRL checking.
CRLTimeoutInSeconds **Note** This setting does not have an equivalent Windows Installer property and is not in the template	3 (seconds)	The maximum time in seconds that is allowed to elapse whilst the Tachyon client attempts to download a Certificate Revocation List (CRL) from a CRL Distribution Point. The range is 1 to 10 seconds.

Core setting	Installation default	Description
configuration file.		
DefaultStaggerRangeSeconds	300 (5 minutes)	Some operations (including HTTPS downloads from the BackgroundChannel) are randomly time-staggered across clients. This property dictates the upper-limit on the default randomization period in seconds. Range is 0 to 3600. Default is 300. Use **0** to instruct Tachyon client not stagger operations by default. **Note** Do not change this value unless advised by 1E. Only use 0 or a low value in systems that support less than 500 clients. **Note** This setting is not used for HTTPS downloads from the BackgroundChannel if NomadContentDownloadEnabled is **true**, because Nomad does the bandwidth management.
EnablePayloadCompression	true	Determines whether the client should attempt to compress payloads when responding to instructions, if it looks like

Core setting	Installation default	Description
		compression would be beneficial. Must be set to **true** or **false**.
FastReconnectTimeInSeconds **Note** This setting does not have an equivalent Windows Installer property and is not in the template configuration file.	15 (seconds)	During machine wakeup, following a machine sleep or hibernation, the first reconnect attempt to the Switch will occur in <FastReconnectTimeInSeconds> seconds. This value is configurable between 5 and 60 seconds. For the majority of Windows devices the default value of 15 seconds is more than adequate for the Windows network stack to stabilise on wakeup. On non-Windows platforms this property is currently ignored. See also ConnectionRetryTimeInSecondsMin/Max.
LoggingLevel	Info	Determines how much logging information is generated. This may be set to one of the following values. The default value is **info**. Value — Description **Error** — Only outputs errors. An error is a serious problem, typically requiring

Core setting	Installation default	Description
		operator intervention of some sort to restore full functionality. **Warn** Outputs errors and warnings. A warning indicates a potential problem, where the system can nonetheless function without intervention. **Info** Outputs general information in addition to the errors and warnings. This is the default. **Debug** Outputs debugging information in addition to all the previous levels. **Trace** Outputs the maximum information available. Used only in exceptional circumstances as it will generate huge amounts of logging output. **Warning** Logging levels should only be changed from **info**

Core setting	Installation default	Description
		only if requested by 1E Support and reset to **info** after investigation is complete.
LogPath **Note** This setting is shared with the 1E Client.	**1E Client logs on Windows** %ALLUSERSPROFILE%\1E\Client\1E.Client.log (used by 1E Client and Tachyon features, and Shopping client) %ALLUSERSPROFILE%\1E\Client\NomadBranchUninstall-YYYY_MM_HHTMM_HH_SS_000Z.log **1E Client logs on macOS** /Library/Logs/1E.Client.Daemon.log (shows any service start errors) /Library/Logs/1E.Client.log (shows the current operation of the 1E Client) **1E Client logs on other non-Windows platforms** /var/log/1E/Client/1E.Client.log	The **LogPath** setting is stored in the **1E.Client.Conf** file and determines the full path and filename of the 1E Client log file. The 1E Client log is shared by: • 1E Client • Tachyon client features • Shopping client module (only available on Windows OS) To change the logging level, please refer to LoggingLevel in the 1E.Client.CONF file. The following are not configurable in this version: • Maximum size of 5MB • 5 rollover files numbered 1 (newest) to 5 (oldest) with the rollover number included as n.log **Note** By default, Windows resolves %ALLUSERS PROFILE% as C:\ProgramData\ See Log files for more details about 1E Client logs.

<table>
<tr><th>Core setting</th><th>Installation default</th><th>Description</th></tr>
<tr><td>NomadContentDownloadEnabled</td><td>true</td><td>The Content Distribution integration feature is for Windows clients only. The feature is enabled if this value is set to true and Content Distribution is running on the device. There is no dependency on Configuration Manager which Content Distribution also integrates with.

<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td>false</td><td>• Tachyon client waits a randomized stagger period defined by its DefaultStaggerRangeSeconds setting, and then downloads content from the specified Background Channel.
• Tachyon client retains modules and extensibles that it has downloaded, but does not retain instruction scripts after they have been run. Any</td></tr>
</table>
</td></tr>
</table>

Core setting	Installation default	Description
		instruction that requires a script or other file will download the latest version each time the instruction is run.
	tru e	• Tachyon client immediately requests Content Distribution to download content from the specified HTTP source, such as the **Background Channel**. Content Distribution behaves in the same way as it does with Configuration Manager by ensuring the latest version of content is obtained and electing a master to perform the actual download. • Content Distribution maintains its own cache of downloaded

Core setting	Installation default	Description
		content which avoids the need for repeat downloads over the WAN, and provides content to peers that require the same resources which avoids peer devices having to download over the WAN.
NomadContentDownloadTimeoutSecs	600 (10 minutes)	The Content Distribution integration feature is only for Windows computers. If this feature is enabled, and requested content is not provided within the timeout period, The Tachyon client will fall back to downloading directly from the Background Channel The most likely reason for a timeout is if Content Distribution is busy downloading other content. The range is 10 to 3600 (1 hour). **Note** On all non-Windows platforms this property defaults to 0 and is ignored.

Core setting	Installation default	Description
PolicyEnabled	true	Determines if the Policy feature of the Tachyon client is enabled (**true**) or not (**false**). The Policy feature is responsible for downloading, evaluating and reporting on policy rules defined in the Guaranteed State application on the Tachyon platform. If set to **true** then you must also configure settings for Switch and Background Channel. Must be set to **true** or **false**.
SelectRowsLimit **Note** This setting does not have an equivalent Windows Installer property, but *is* in the template configuration file.	100000 (10^5)	Limits the number of rows returned by a SELECT expression. The principle is that if there is more than this number of rows then something has gone wrong. This limit prevents an unexpectedly excessive amount of both data and CPU usage. The range is 1 to 1000000000 (10^9). The default value is 100000 (10^5). **Note** It is *not* considered an execution error if the limit is reached, although a warning will be written to the 1E Client log.
SSL	TLSv1.2	Determines which security protocol the Tachyon client uses when connecting to

<table>
<tr><th>Core setting</th><th>Installation default</th><th>Description</th></tr>
<tr><td></td><td></td><td>Switches and Background Channel.

SSL must be set to one of the following values:

<table><tr><th>Value</th><th>Description</th></tr><tr><td>TLSv1.2</td><td>TLS version 1.2 is a cryptographic protocol aimed at securing the network transport layer, and has recently been adopted by all the major browsers. It is considered to be more secure than SSLv3. This is the default.

Warning
Always use the default TLSv1.2 unless advised by 1E.</td></tr></table></td></tr>
<tr><td>Switch</td><td>(none)</td><td>If Tachyon and Content Distribution client features are not required then the connection to Tachyon Platform is not required, and both Switch and BackgroundChannelUrl settings must be set to none when doing a non-interactive (silent/quiet) install using installer properties on a</td></tr>
</table>

Core setting	Installation default	Description
		command-line or in a MST transform file. When doing an interactive install then you must uncheck the **Enable Tachyon** checkbox. Tachyon client features are not required if the 1E Client is being installed only to support PXE Everwhere, Shopping, or WakeUp. They are only required for Content Distribution if using Content Distribution features of the Tachyon Platform. To connect to the Tachyon platform then **Switch** will have one or more entries in the format: `Switch=<SwitchName>:<SwitchPort>` **<SwitchName>** is the DNS Name FQDN for one or more Switches. This is the same as the following except in a custom configuration where the Switch is installed on its own: • the HTTPS Host Header specified on the *Website Configuration* screen of the Tachyon Server installer, which is the HTTPS binding for the Tachyon Web Site • the same as <BackgroundChannelServer>

Core setting	Installation default	Description
		• the DNS Name specified in the Tachyon Server's Web Certificate. **<SwitchPort>** is the Port number, which has default value of 4000. Any other port number is used only in a complex configuration if advised by 1E. In systems where there are multiple DNS Names, there will be multiple entries using a semi-colon (;) as the delimiter between entries. For example: `Switch=tachyon.acme.local:4000;tachyon.acme.com:4000` Multiple DNS Names may exist in complex systems where there are multiple servers, Switches, and devices on different networks, such as the Internet as well as the corporate network. When the Tachyon client attempts to find a Switch, it will try each entry in turn, starting at the first. If all attempts fail Tachyon restarts the connection process after a period determined by ConnectionRetryTimeInSecondsMin/Max.
WorkerThreads	2	Determines the number of threads that will execute instructions concurrently. This property enables instructions

Core setting	Installation default	Description
		to be run simultaneously and prevents long running instructions from blocking others. Range is 1 to 8. 1 means all instructions are run sequentially on the same thread.

2.6.1.6.3 Interaction module settings

This section describes configuration settings for the **Real-Time Control Center** and **1E Client UI** (User Interaction) features provided by the Interaction module.

1E Client, while running, continuously captures details of certain user activity, such as which window is in the foreground on the user's desktop, and when the user is interacting (keyboard and mouse activity) with that window. Data is regularly written into a local, compressed and encrypted **persistent storage tables**, that are accessible using Interaction methods. The whole process is designed to minimize impact on device performance, storage and security.

The Interaction module is supported only on Windows OS (not Windows XP, Vista or other legacy OS). The 1E Client UI, which is launched by the Interaction module, requires Microsoft .NET Framework.

Configuration setting	Installation default	Description
Module.Interaction.Enabled **Note** This interaction setting is in the template configuration file.	true	Set this setting to **true** to enable the Interaction module. Default value is **true**. Must be set to **true** or **false**.
Module.Interaction.ActiveSessionThresholdSeconds	2	This setting is used to ensure that if the user is currently busy interacting, then focus will not be stolen from the user to display a notification. Notification display will only be considered if the user stopped interaction at least Active

Configuration setting	Installation default	Description
		Session Threshold Seconds before. Active Session Threshold Seconds is configurable between 0 and 30.
Module.Interaction.CompanyName	1E Ltd.	The organization name that is displayed in the header of the **Real-Time Control Center** and other **1E Client UI** dialogs. Can be set by the installer.
Module.Interaction.DoNotDisturb **Note** This interaction setting is in the template configuration file.	false	Set **true** to enable **Do not disturb**, and stop notifications after startup. Surveys sent to this device will respond as Timed out. Set **false** to disable **Do not disturb**, and show notifications after startup. In each case, if the **Module.Interaction.NotificationIcon** setting is true, the user can still use the notification area icon to enable or disable notifications. However, each time the user signs in, the **Do not disturb** mode will be reset.
Module.Interaction.IdleSessionThresholdMinutes	30	To ensure that notifications only appear when the user is present, this threshold specifies that notifications should not be displayed if more than the configured number of idle minutes has elapsed.

Configuration setting	Installation default	Description
		Idle Session Threshold Minutes is configurable between 1 and 1440.
Module.Interaction.ITSM.ServiceNow.CreateIncidents	false	If set to **true**, and ServiceNow integration is enabled, then users can create new incident tickets. (New in 8.0)
Module.Interaction.ITSM.ServiceNow.Enabled	false	Enable ServiceNow integration. This feature shows ServiceNow ticket information in the **Real-Time Control Center**. This feature also requires the following: • Module.Interaction.Enabled to be set to true • Module.Interaction.ITSM.ServiceNow.Url to be configured with the URL of the ServiceNow instance.
Module.Interaction.ITSM.ServiceNow.GoBackDays	30	Sets how far back to look for tickets that changed state to inactive (closed, resolved or cancelled). By default, the **Real-Time Control Center** shows all active tickets for the user. The user can also choose to view inactive tickets that have changed state during this period. The range is 1 to 365.

Configuration setting	Installation default	Description
		Only used if Module.Interaction.ITSM.ServiceNow.Enabled is **true**. Can be set by the installer. (New in 8.0)
Module.Interaction.ITSM.ServiceNow.Url	*(none)*	The URL to a ServiceNow instance, for example https://acme12345.service-now.com. Only used, and required, if Module.Interaction.ITSM.ServiceNow.Enabled is **true**. Can be set by the installer. (New in 8.0)
Module.Interaction.LogSessionNotificationReadiness	false	If set to **true**, the 1E Client will log an INFO message to indicate that a given user session is ready for notifications. If set to **false**, this information will be logged only at TRACE level. Intended for troubleshooting purposes only.
Module.Interaction.MinimumMinutesAfterLogonBeforePrompt	60	To ensure that notifications don't appear too soon after logon, this setting specifies the minimum time in minutes that must elapse after the user has been logged onto a session before notifications can appear. Minimum Minutes After Logon Before Prompt is configurable between 1 and 1440.

Configuration setting	Installation default	Description
Module.Interaction.MinimumMinutesAfterSessionActivationBeforePrompt	15	To ensure that notifications don't appear immediately after session unlock or reconnect, this setting specifies the minimum time in minutes that must elapse since the user session has been reactivated before notifications can appear. Minimum Minutes after Session Activation Before Prompt is configurable between 1 and 1440.
Module.Interaction.MinimumMinutesBetweenPrompts	60	To ensure that notifications don't appear too frequently, this setting specifies the minimum time in minutes since a notification was displayed before another notification will appear. Minimum Minutes Between Prompts is configurable between 1 and 1440.
Module.Interaction.NotificationIcon **Note** This interaction setting is in the template configuration file.	true	If set to **true**, a notification area icon will appear when the Client UI is running. If set to **false**, the icon will not be visible. Users may see notification popups, but will not be able to: • select User Sentiment surveys from the menu

Configuration setting	Installation default	Description
		• use the **Do not disturb** option
Module.Interaction.PeriodsBeforeUiLaunch	2	Specifies how many time periods to wait before launching the 1E Client UI, typically a launch time period is 5 seconds. Periods Before UI Launch is configurable between 1 and 120.
Module.Interaction.PeriodsBeforeUiLaunchTimeout	12	Specifies how many time periods may elapse before it is considered that the 1E Client UI has failed to launch, typically a launch time period is 5 seconds. Periods Before UI Launch Timeout is configurable between 1 and 24.
Module.Interaction.Port **Note** This interaction setting is in the template configuration file.	7766	The port number used for communication between the 1E Client service and 1E Client UI. Port is configurable between 100 and 65535.
Module.Interaction.ResponseAuditsBeforeTidy	100	This setting defines how frequently responses should be pruned to retain only the most recent responses. A response audit typically occurs each time a user responds to a notification, where a response includes

Configuration setting	Installation default	Description
		dismissing or snoozing a notification. Response Audits Before Tidy is configurable between 10 and 1000.
Module.Interaction.ResponseRetentionRows	5000	This setting ensures that the 1E Client only retains the most recent responses, with this value indicating how many responses should be retained. Response Retention rows is configurable between 100 and 50000.
Module.Interaction.SampleExclusionList	*(none)*	A comma-separated list of process names that are excluded from User Interaction sampling. Case is not significant. Only used if Module.Interaction.SampleUserInteraction is **true**. When User Interaction sampling is enabled, the Interaction module uses regular sampling to determine the responsiveness of application windows on the user's desktop. If the foreground window's process name has any of these values as a substring then it is excluded from the interactivity test.
Module.Interaction.SampleUserInteraction **Note**	true	Set to **true**, to enable User Interaction sampling.

Configuration setting	Installation default	Description
This interaction setting is in the template configuration file.		The Interaction module uses regular sampling to determine the responsiveness of application windows on the user's desktop, and will also track user keyboard and mouse input to determine the level of activity.
Module.Interaction.SnoozeTimeMinutes	15	This setting specifies the time in minutes that must elapse before a notification can be considered for re-display, after the user clicked on the **Later** button, or it had timed out. Snooze Time Minutes is configurable between 1 and 1440.
Module.Interaction.Theme	*(none)*	Specifies a theme that should be applied to the notifications. Can be one of: **Light**, **Dark** or **HighContrast**. If a value is not provided, the 1E Client UI will automatically determine the most appropriate theme based on the user's Windows desktop settings.

2.6.1.6.4 Inventory module settings

This section describes configuration settings for the Tachyon Activity Record feature provided by the Inventory module.

The Tachyon client, while running, continuously captures details of certain activities and events as they happen, similar to Windows Task Manager or Perfmon. During startup, the Tachyon client is able to detect some events that occurred when it was not running. Data is regularly written into a local, compressed and encrypted **persistent storage tables**, that are accessible to SCALE as SQL tables. The Tachyon client periodically

aggregates data in order to minimize the amount of storage required, so that each capture source has a live, hourly, daily and monthly table. The whole process is designed to minimize impact on device performance, storage and security. Please refer to /document/preview/737017#UUID-41152f15-7fd9-e142-94e1-9f86562abb75 for details of what data is captured and how to query these tables.

Other than **Module.Inventory.Enabled**, these Inventory module settings are not included in the template configuration file, and therefore use default values. To set any other value for these the setting must be added to the configuration file.

There are no SCALE methods available in the inventory module for creating instructions.

2.6.1.6.4.1 Capture sources

The table below lists the capture sources supported by the **Tachyon Activity Record** feature (also known as the Inventory module) and on which OS they are supported. The source name is used in each of the Capture source settings.

Source Name	Description	Windows	macOS	Linux	Solaris
ARP	ARP cache entries - the Inventory module captures the results of cached IP address to physical address resolutions	3.2	n/a	n/a	n/a
BootPerformance	Windows boot performance metrics.	8.0	n/a	n/a	n/a
DeviceInteraction	User session input metrics (keyboard and mouse activity).	5.1	n/a	n/a	n/a
DevicePerformance	Device performance metrics for device performance by interrogating Windows Performance Counters. These metrics cover disk, memory, network and processor performance. This capture source is required by the **Experience** application.	5.0	n/a	n/a	n/a
DeviceResourceDemand	Disk, network, memory, and processor performance metrics.	5.1	n/a	n/a	n/a
DNS	DNS resolution queries - the Inventory module captures whenever a DNS address is resolved	2.1	2.1	n/a	n/a

Source Name	Description	Windows	macOS	Linux	Solaris
OperatingSystemPerformance	Performance metrics for OS - the metrics executable runs every 4 hours by default This capture source is required by the **Experience** application.	5.0	n/a	n/a	n/a
PerformanceEvent	Distinct events which may be of relevance when diagnosing performance or end-user experience issues.	5.0	n/a	n/a	n/a
Process	Process execution - the Inventory module captures whenever a process starts on the device	2.1	2.1	2.1	2.1
ProcessStabilization	The time taken for a process execution to be considered stable whenever a monitored process starts on the device	3.2	n/a	n/a	n/a
ProcessUsage	A daily summary of the launches and terminations of processes. The Process Usage capture source is required by the **Tachyon Powered Inventory** feature (Tachyon connector). **Note** Process Usage capture can generate high disk I/O while capturing process usage on virtual machine hosts with guests starting at the same time.	3.2	n/a	n/a	n/a
SensitiveProcess	Performance metrics for sensitive processes - the metrics executable runs every 4 hours by default	5.0	n/a	n/a	n/a

Source Name	Description	Windows	macOS	Linux	Solaris
	This capture source is required by the **Experience** application.				
Software	Software installs/uninstalls/presence - the Inventory module captures whenever software is installed/uninstalled, and also captures which software is present on a device	2.1	2.1	2.1	2.1
SoftwareInteraction	Software process responsiveness and duration of active interaction.	5.1	n/a	n/a	n/a
SoftwarePerformance	Performance metrics for software - Software performance polling is every 10 seconds by default This capture source is required by the **Experience** application. Aggregated with SoftwarePerformance data: • SoftwarePerformance.DiskUsage - Disk related metrics for each running process • SoftwarePerformance.ProcessNetworkUsage - Network related metrics for each running process.	5.0	n/a	n/a	n/a
TCP	Outbound TCP connections - the Inventory module captures whenever an outbound TCP connection is made	2.1	2.1	2.1	n/a
UserUsage	A daily summary of all the logons and logoffs of users. This capture source is required by the **Tachyon Powered Inventory** feature (Tachyon connector).	3.2	n/a	n/a	n/a

2.6.1.6.4.2 Global capture settings

The table below lists configuration properties that affect all capture sources.

Inventory module setting	Installation default	Description
Module.Inventory.Enabled **Note** This is the only inventory setting in the template configuration file.	true	Determines whether the **Tachyon Activity Record** feature is enabled or disabled. Must be set to **true** or **false**. Must be set to true if using the **Tachyon Powered Inventory** feature (Tachyon connector). If set to **true**, individual capture sources can be enabled or disabled by setting **Module.Inventory.<source>.Enabled** to **true** or **false**. If set to **false** , this setting takes precedence over individual capture source settings with all being disabled.
Module.Inventory.NoEventTracing **Note** This setting does not have an equivalent Windows Installer property and is not in the template configuration file.	false	Controls whether the Inventory module will, on Windows, use a polling-based mechanism to capture data instead of event-based. The Inventory module will use Windows operating system events to capture data, if the host operating system supports it. If this setting is **true**, the Inventory module will instead use a polling-based approach to capture data. This setting is ignored on other operating systems.

Inventory module setting	Installation default	Description
Module.Inventory.AggregationIntervalSeconds **Note** This setting does not have an equivalent Windows Installer property and is not in the template configuration file.	60 (seconds)	Determines the frequency, in seconds, at which the Inventory module will write the capture buffers to the live and aggregated tables. More frequent aggregations will make captured data available for querying sooner, at the cost of more processing on the device. Range is 30 to 600 (10 minutes).

2.6.1.6.4.3 Capture source settings

The table below lists the 8 settings used to configure each capture source. The relevant <source> name needs to be included in each of the setting names (not case-sensitive):

ARP | BootPerformance | DeviceInteraction | DevicePerformance | DeviceResourceDemand | DNS | OperatingSystemPerformance | PerformanceEvent | Process | ProcessStabilization | ProcessUsage | SensitiveProcess | Software | SoftwareInteraction | SoftwarePerformance | TCP | UserUsage

Note

The following settings do not have an equivalent Windows Installer property and are not in the template configuration file.

Capture source setting	Installation default	Description
Module.Inventory.<source>.Enabled Not available for capture source: • SoftwareInteraction	true (all sources)	Controls whether this capture source is active (**true**) and will capture data. To disable capture of this data, use **false**. **Note** Disabling the **Tachyon Activity Record** feature by setting **Module.Inventory.Enabled** to **false**, takes precedence over individual capture source settings.

Capture source setting	Installation default	Description
		The Process Usage capture source is required by the **Tachyon Powered Inventory** feature (Tachyon connector). **Note** Process Usage capture can generate high disk I/O while capturing process usage on virtual machine hosts with guests starting at the same time.
Module.Inventory.<source>.BufferSize Not available for capture sources: • DevicePerformance • DeviceResourceDemand • SoftwarePerformance	1000 (all sources)	Determines the maximum number of capture entries held in memory during an aggregation period. The Inventory module will store data in memory prior to writing it to disk (as determined by the **Module.Inventory.AggregationIntervalSeconds** setting described above). This setting controls the size of the capture buffer available for this data. If this capture buffer is exceeded, older entries will be discarded to make room for newer ones. For example, based on the default values, if more than 1000 DNS lookups occur within 60 seconds. A higher value will allow the Inventory module can capture higher volumes of events at the cost of additional memory use.

Capture source setting	Installation default	Description
		Range is 100 to 10000.
Module.Inventory.<source>.PollIntervalSeconds Not available for capture sources: • DNS • Process • ProcessStabilization • ProcessUsage • TCP • UserUsage	30 (all sources except Software and OperatingSystemPerformance) 120 (2 minutes for Software) 300 (5 minutes for OperatingSystemPerformance)	Determines the frequency, in seconds, at which the capture source will poll for data. This setting is ignored if the Inventory module is using an event-based mechanism to capture data. A lower value (more frequent polls) is likely to capture more data at the cost of additional processing overhead on the device. Range is 5 to 600 (10 minutes) for all sources except for OperatingSystemPerformance which can go up to 86400 (1 day).
Module.Inventory.<source>.AggregationsBeforeGroom	3 (all sources)	Determines the number of aggregation cycles that should occur before old data is removed (groomed) from the Inventory module's live disk-based store. See the three Retention settings below. The Inventory module will store captured data for a limited time before removing it. This setting determines how frequently the grooming operation will be performed. The clean-up operation happens every N aggregation cycles. A lower value (more frequent deletion) will remove old data more quickly at the cost of

Capture source setting	Installation default	Description
		additional processing overhead on the device. Range is 1 to 50.
Module.Inventory.<source>.LiveRetention	5000 (all sources)	Determines the maximum number of capture entries that will be stored in the Inventory module's live disk-based storage. The Inventory module stores detailed (non-aggregate, live) capture entries on disk, as well as aggregated capture entries per hour, day and month (see below). This setting determines the limit of the detailed entries. When the limit is reached, older entries are deleted to make room for newer ones. A higher value allows storage of a longer period of detailed entries at the cost of additional disk space on the device. Storing more data will also cause queries on that data to take longer. Range is 100 to 50000.
Module.Inventory.<source>.HourlyRetention	24 (all sources)	Determines the maximum number of hours/days/months for which aggregated data will be kept in the Inventory module's disk-based storage. The Inventory module will discard data from its hourly/daily/monthly store to make room for newer data.

Capture source setting	Installation default	Description
		A higher value allows a longer record of data to kept at the cost of additional disk space on the device. Storing more data will also cause queries on that data to take longer. Note that these settings are independent of one another – for example, it is not necessary to specify an “hourly” value of 24 or greater to be able to capture “daily” values. A value of zero means “disable data aggregation at this resolution”. Again, since the settings are independent, it is valid to disable hourly data aggregation yet keep daily and monthly aggregation active. Range is 0 (disabled) to 100.
Module.Inventory.<source>.DailyRetention	31 (90 days for ProcessUsage and UserUsage for 5.1 and later)	
Module.Inventory.<source>.MonthlyRetention	12 (all sources)	

2.6.1.6.4.4 Settings unique to specific capture sources

Note

The following settings do not have an equivalent Windows Installer property and are not in the template configuration file.

Capture source setting	Installation default	Description
Module.Inventory.ProcessStabilization.Fuzziness	5	Modifies the margins within

Capture source setting	Installation default	Description
		which a process is considered stable. The default is 5, and the range is 1 to 66 inclusive. This setting should be left unchanged.
Module.Inventory.ProcessStabilization.MonitoredProcesses		This is a comma separated, case insensitive list of executable names (with extensions) of any processes that require stabilization monitoring. By default, this is not set and therefore process stabilization monitoring is disabled. The list should not exceed 15 executables.
Module.Inventory.ProcessUsage.VerboseLogging	false	Enables or disables Process Usage log messages, which typically appear for each data capture refresh. ProcessUsage is used by the Tachyon Powered Inventory feature.
Module.Inventory.UserUsage.VerboseLogging	false	Enables or disables User Usage log messages, which typically appear for

Capture source setting	Installation default	Description
		each data capture refresh. UserUsage is used by the Tachyon Powered Inventory feature.

2.6.1.7 Content Distribution client settings

Installer properties and configuration file settings for the Content Distribution client module of the 1E Client, which is supported only on Windows computers.

Note

Installer properties:

Module.Nomad.Enabled | MODULE.NOMAD.AUTHENTICATEDUSERS | MODULE.NOMAD.BLOCKSIZE | MODULE.NOMAD.CACHECLEANCYCLEHRS | MODULE.NOMAD.CACHECLEANSUBNETLOOKUP | MODULE.NOMAD.CACHEPATH | | MODULE.NOMAD.CACHESTATESYNCINTERVALMINUTES | MODULE.NOMAD.CERTISSUER | MODULE.NOMAD.CERTSUBJECT | MODULE.NOMAD.COMPATIBILITYFLAGS | MODULE.NOMAD.CONTENTPROVIDERONWIFI | MODULE.NOMAD.CONTENTREGISTRATION | MODULE.NOMAD.DEBUG | MODULE.NOMAD.DOREPORTINGENABLED | MODULE.NOMAD.DOWNLOADTIMEOUT | | MODULE.NOMAD.DPCACHECLEANUPENABLED | MODULE.NOMAD.DPNOTAVAILABLECODES | MODULE.NOMAD.ENFORCEQUOTAS | MODULE.NOMAD.GENERATEWEREVENTS | MODULE.NOMAD.HAACKTIMEOUTMINS | MODULE.NOMAD.LOCALSSDSTAGGER | MODULE.NOMAD.LOGNAME | MODULE.NOMAD.LOGPATH | MODULE.NOMAD.MADCAPSCOPE | MODULE.NOMAD.MAXALLOCREQUEST | MODULE.NOMAD.MAXCACHEDAYS | | MODULE.NOMAD.MAXCACHEDAYSTHRESHOLD | MODULE.NOMAD.MAXCACHESIZEMB | MODULE.NOMAD.MAXCONCURRENCY | MODULE.NOMAD.MAXDEVICESFROMAE | MODULE.NOMAD.MAXELECTIONRESPONSELOGGING | MODULE.NOMAD.MAXIMUMMEGABYTE | MODULE.NOMAD.MAXLOGSIZE | MODULE.NOMAD.MAXPACKAGEFAST | MODULE.NOMAD.MAXPACKAGERAS | MODULE.NOMAD.MAXPACKAGESLOW | MODULE.NOMAD.MAXPACKETSPERSECOND | MODULE.NOMAD.MAXPRECACHEDAYS | MODULE.NOMAD.MAXSTATUSFREQUENCY | | MODULE.NOMAD.MAXSTUCKCOUNT | MODULE.NOMAD.MAXSUCACHEDAYS | MODULE.NOMAD.MULTICASTSUPPORT | MODULE.NOMAD.NOHARDLINK | MODULE.NOMAD.NOMADINHIBITEDADSITES | MODULE.NOMAD.NOMADINHIBITEDSUBNETS | | MODULE.NOMAD.P2PDISQUALIFYMAXNUMPEERS | | MODULE.NOMAD.P2PDISQUALIFYMAXWINDOWMINS | MODULE.NOMAD.P2PENABLED | MODULE.NOMAD.P2PHTTPPORT | MODULE.NOMAD.P2PHTTPSPORT | MODULE.NOMAD.P2PPORT | MODULE.NOMAD.P2PSSLSETTINGS | MODULE.NOMAD.PERCENTAVAILABLEDISK | MODULE.NOMAD.PERMITTEDLSZSHARES | MODULE.NOMAD.PERMITUNCACHED | MODULE.NOMAD.PLATFORMURL | MODULE.NOMAD.POSTCOMPLETETIMEOUTHOURS | MODULE.NOMAD.PRECACHEPOLLBATCHSIZE | MODULE.NOMAD.PRECACHEPOLLMINUTES |

MODULE.NOMAD.PRECOMPLETETIMEOUTHOURS | MODULE.NOMAD.RECYCLEDPDELAY | | MODULE.NOMAD.RANDOMIZEREMOTEPATHS | MODULE.NOMAD.SIGSFOLDER | MODULE.NOMAD.SITESSDSTAGGER | | MODULE.NOMAD.SITESSDMINPACKAGESIZEKB | MODULE.NOMAD.SPECIALNETSHARE | MODULE.NOMAD.SSDENABLED | MODULE.NOMAD.SSPBAENABLED | MODULE.NOMAD.STATUSMSGEVENTS | MODULE.NOMAD.SUCCESSCODES | | MODULE.NOMAD.SUPPORTWPAD | MODULE.NOMAD.USEFIPS | MODULE.NOMAD.WAKEUPBATCHSIZE | MODULE.NOMAD.WAKEUPENABLED | MODULE.NOMAD.WAKEUPMINPACKAGESIZEMB | MODULE.NOMAD.WLANBLIPSECS | MODULE.NOMAD.WLANPROFILELIST

Note

Configuration file settings:

Module.Nomad.Enabled

Note

The Content Distribution client module of 1E Client replaces the legacy NomadBranch component of Content Distribution.

When the 1E Client starts, and the Content Distribution client module is enabled, it will only initialize the Content Distribution client module if the OS version is a supported Windows version. The 1E Client will automatically remove any previous installation of NomadBranch, keeping relevant NomadBranch registry settings.

The 1E Client Content Distribution client module is not supported on:

- Non-Windows devices
- Legacy OS (that is OS which Microsoft no longer support including XP, Vista, Server 2008 etc.)

1E Client installers include a **template configuration file** that contains the more important settings with default values that match hard-coded default values. The configuration file is updated during installation and named **1E.Client.conf** in the installation folder along with the 1E Client executable.

After installation, configuration file settings can be managed using 1E Client command-line parameters, Explorer configuration instructions, Guaranteed State policies, Configuration Manager baselines or other means. Registry settings can also be managed by Windows Group Policy.

The following table shows the supported installer properties for the Content Distribution client module of the 1E Client.

Note

Each installer property listed below has a link to its corresponding registry value page.

2.6.1.7.1 Nomad client settings

Note

You must use UPPERCASE when specifying the *name* of any installer property in a **mst** transform file, and preferably when including them in a msiexec command-line.

Names of settings stored in the configuration file are not case-sensitive. Setting names stored in the registry may be case-sensitive and should be specified as shown.

Settings that have numeric values must be set using decimal integers, unless otherwise specified.

<table>
<tr><th>Installer property</th><th>Description</th></tr>
<tr><td>Module.Nomad.Enabled</td><td>Set this property to true to enable the Nomad client module. The default value is false.

Note
If enabled, when the 1E Client starts, it will attempt to automatically remove any previous installations of Nomad Branch.

This setting does not have an associated Nomad registry entry and is stored in the 1E Client configuration file.</td></tr>
<tr><td>MODULE.NOMAD.AUTHENTICATEDUSERS</td><td>Determines which of the built-in security groups is granted read-only permissions to the Nomad cache.

<table>
<tr><th>Registry value</th><th>Default value</th><th>Notes</th></tr>
<tr><td>AuthenticatedUsers</td><td>1</td><td>Grants read-only access to the Nomad cache as follows:

• 0 – Everyone built-in security group and the SMSNomadP2P& Nomad share account. This is the least restrictive option and is not valid with HTTP or HTTPS protocol and is treated as 2 (only the SMSNomadP2P& Nomad share account)

• 1 – Authenticated Users built-in security group and the SMSNomadP2P& Nomad share account

• 2 – Only the SMSNomadP2P& Nomad share account. This account has also been added to NTFS permission settings.</td></tr>
</table>
</td></tr>
</table>

Installer property	Description
	Unauthorised HTTP requests to access the caches are met with a 403 status code. The Nomad share has more information about share permissions and NTFS security. The difference between Authenticated Users and Everyone depends on the OS version, but in general Everyone includes Authenticated Users plus Guest.
MODULE.NOMAD.BLOCKSIZE	Value (in bytes) for the minimum size of each block of data Nomad copies from the package source folder. Click here to expand... Value (in bytes) for the minimum size of each block of data Nomad copies from the package source folder. **Note** Any change to this value requires a manual service restart before it can take effect.

2.6.1.7.1.1 BlockSize

Value (in bytes) for the minimum size of each block of data Nomad copies from the package source folder.

Note

Any change to this value requires a manual service restart before it can take effect.

Registry value	Default value	Notes	Installer property
BlockSize	131072(128KB)	Must be between 4096(4KB) to 4194304(4MB) inclusive. • The default block size is 128KB	MODULE.NOMAD.BLOCKSIZE

Installer property	Description
	• The maximum block size is 4MB • Multicast environments can only use the default block size. If you define a larger value for multicast environments, Nomad automatically resets it to the default. • Clients use the block size defined in the registry and ignore the values from the LSZ

The Dynamic Block Size (DBS) feature increases block size on high-bandwidth links to get maximum efficiency, and reduces it on low-bandwidth links to reduce the impact. Using DBS, Nomad is able to automatically decide the appropriate block size for a given link bandwidth and also adjust it as needed during the download if the link conditions change. As a result, Nomad is far more efficient and faster on all types of connection bandwidths while retaining its minimal impact on other link traffic.

Note

DBS is enabled or disabled by configuring Bit 25 in the CompatibilityFlags registry. Setting Bit 25 disables DBS and clearing Bit 25 enables DBS.

In Nomad 7.0 onwards, the DBS feature is turned off by default for new installations, and not changed for upgrades.

Installer property	Description

Prior to v6.3 the default value of BlockSize registry setting was 32KB (0x8000). From v6.3 onwards the default is 128KB (0x20000).

The installer automatically sets this to 128KB for both fresh installs and upgrades from previous versions. The only exceptions to this are:

- It will use the specified value if the BLOCKSIZE property is used in the installation command line or in a MST transform, when doing a fresh install or upgrade
- It will retain the previous value of BLOCKSIZE if it was set to anything other than 32KB (the older default), when doing an upgrade.

Registry value	Default value	Notes
BlockSize	131072(128KB)	Must be between 4096(4KB) to 4194304(4MB) inclusive. • The default block size is 128KB • The maximum block size is 4MB • Multicast environments can only use the default block size. If you define a larger value for multicast environments, Nomad automatically resets it to the default. • Clients use the block size defined in the registry and ignore the values from the LSZ

The Dynamic Block Size (DBS) feature increases block size on high-bandwidth links to get maximum efficiency, and reduces it on low-bandwidth links to reduce the impact. Using DBS, Nomad is able to automatically decide the appropriate block size for a given link bandwidth and also adjust it as needed during the download if the link conditions change. As a result, Nomad is far more efficient and faster on all types of connection bandwidths while retaining its minimal impact on other link traffic.

Note

Installer property	Description
	DBS is enabled or disabled by configuring Bit 25 in the CompatibilityFlags registry. Setting Bit 25 disables DBS and clearing Bit 25 enables DBS. In Nomad 7.0 onwards, the DBS feature is turned off by default for new installations, and not changed for upgrades. Prior to v6.3 the default value of BlockSize registry setting was 32KB (0x8000). From v6.3 onwards the default is 128KB (0x20000). The installer automatically sets this to 128KB for both fresh installs and upgrades from previous versions. The only exceptions to this are: • It will use the specified value if the BLOCKSIZE property is used in the installation command line or in a MST transform, when doing a fresh install or upgrade • It will retain the previous value of BLOCKSIZE if it was set to anything other than 32KB (the older default), when doing an upgrade.
MODULE.NOMAD.CACHECLEANCYCLEHRS	Determines the number of hours between automatically running the Nomad cache cleaner. Click here to expand... Determines the number of hours between automatically running the Nomad cache cleaner.

Registry value	Default value	Notes
CacheCleanCycleHrs	0 (turned off)	The first automatic cache clean runs randomly between 10 to 60 mins of service start up. Subsequent cache clean cycles run after the number of hours specified. 0 means feature turned off. No cache cleaning cycle would run. Changing this registry entry performs an internal restart. The minimum value is 4. The maximum value is 168 (Once a week)

Installer property	Description
	Please refer to Cache management for details about other cache management settings.
MODULE.NOMAD.CACHECLEANSUBNETLOOKUP	If enabled, sets the cache clean subnet lookup. Click here to expand... If enabled, sets the cache clean subnet lookup.

Registry value	Type	Default value	Notes
CacheCleanSubnetLookup	REG_DWORD	1	Before deleting content, Nomad checks if it is on any other client in the same subnet, and will only delete local content if the same is present on at least one other client on the same subnet. To disable subnet lookup, set the value to 0. Its value can be 0 or 1. The default value is 1, subnet lookup is enabled. New setting introduced in 8.0. Please refer to Cache management for details about other cache management settings.

Installer property	Description
MODULE.NOMAD.CACHEPATH	Determines the value of : • NomadBranch\LocalCachePath - the location of local Nomad package cache Click here to expand LocalCachePath... The location of local Nomad package cache. Registry value: LocalCachePath Default value: %ALLUSERSPROFILE%\1E\NomadBranch\ Notes: There are two registry values called LocalCachePath that are used by Nomad. • The LocalCachePath REG_SZ registry value under the HKLM\Software\1E\NomadBranch key sets the path to the local Nomad package cache. • The LocalCachePath REG_SZ registry value under the HKLM\Software\1E\NomadBranch\NMDS key sets the path to the PBA package cache. The path is created if it does not exist. If the drive letter does not exist, and it is not possible to create the specified path, *%TEMP%* is used. Default values are dependent on OS. **Known issue fixed in latest accumulated hotfix**

Installer property	Description

The value for the installer property CACHEPATH requires a trailing backslash \. When Nomad is installed on a DP this location is also used for the LSZFiles vDir folder. If LocalCachePath does not contain a trailing backslash, then:

- the LSZFILES folder is incorrectly created (LocalCachePathLSZFILES instead of LocalCachePath\LSZFILES)
- IIS vDIR points to wrong folder (LocalCachePathLSZFILES instead of LocalCachePath\LSZFILES)
- LSZGEN fails because it is attempting to store LSZ files to non-existent path (LocalCachePath\LSZFILES)

PBA cache is also derived from the same installer property MODULE.NOMAD.CACHEPATH, but it is stored in the registry value> CachePath in the NomadBranch\NMDS registry key.

- NomadBranch\NMDS\CachePath - the location of the base peer backup assistant (PBS) share where user data is copied to

Click here to expand CachePath...

This value holds the location of the base peer backup assistant (PBS) share where user data is copied to.

Installer property	Description

Registry value	Default value	Notes
CachePath	<NomadCachePath>\NMDS	This REG_SZ registry value is found under the PBA registry key NomadBranch\NMDS. This parameter relies on the folder it points to as being configured as a share. In normal circumstances, this should not be modified from the default value. The MODULE.NOMAD.CACHEPATH installer property also used to configure the location of the Nomad cache, which is stored in the registry value LocalCachePath. The location of the PBA cache is derived from the MODULE.NOMAD.CACHEPATH property, and is stored in the registry value CachePath in the NomadBranch\NMDS registry key.

MODULE.NOMAD.CACHESTATESYNCINTERVALMINUTES

Ensures the cache state of a device held on ContentDistribution is in sync with locally held data. This setting controls the **Content Registration Sync Cycle** feature.

Registry value	Default value	Notes
CacheStateSyncIntervalMinutes	1440 (1day)	Range: from 60 to 525600 (1Year).

The **Content Registration Sync Cycle** is available in the following versions of 1E Client, where the Nomad client registers pending and failed content registrations with ActiveEfficiency or Tachyon Platform. Please refer to Single Site Download: Improved resilience of content registration.

Installer property	Description
	• Nomad 8.0 in 1E Client 5.2 - uses Content Distribution in Tachyon Platform • Nomad 7.1 in 1E Client 5.2 - uses Content Distribution in Tachyon Platform • Nomad 7.0.200 in 1E Client 5.1 - uses ActiveEfficiency • Nomad 7.0.100 in 1E Client 5.0 - uses ActiveEfficiency • Nomad 7.0 in 1E Client 4.1 - uses ActiveEfficiency
MODULE.NOMAD.CERTISSUER	Defines one or more certificate issuers that Nomad will use to select the appropriate PKI certificate for the: • Configuration Manager (CM) client authentication certificate - used when downloading over HTTPS from Distribution Points and when communicating with Management Points during pre-caching • Nomad Server Authentication certificate - used to share content between peers over HTTPS • Client Authentication certificate - used for certificate-based client authentication when sharing content between peers over HTTPS. In most cases Nomad will be able to identify a suitable certificate in the Local Computer Personal certificate store without needing to specify CertIssuer (refer to Peer copy over HTTP or HTTPS: Certificate Selection for more details). You should use CertIssuer if the CM client is not using PKI certificates and there are multiple Client Authentication certificates issued by different Certificate Authorities in the store, and if there is a chance some of those certificates may not be trusted by other peers or CM site systems. Click here to expand... Defines one or more certificate issuers that Nomad will use to select the appropriate PKI certificate for the: • Configuration Manager (CM) client authentication certificate - used when downloading over HTTPS from Distribution Points and when communicating with Management Points during pre-caching • Nomad Server Authentication certificate - used to share content between peers over HTTPS

Installer property	Description

- Client Authentication certificate - used for certificate-based client authentication when sharing content between peers over HTTPS.

In most cases Nomad will be able to identify a suitable certificate in the Local Computer Personal certificate store without needing to specify CertIssuer (refer to Peer copy over HTTP or HTTPS: Certificate Selection for more details). You should use CertIssuer if the CM client is not using PKI certificates and there are multiple Client Authentication certificates issued by different Certificate Authorities in the store, and if there is a chance some of those certificates may not be trusted by other peers or CM site systems.

Registry value	Default value	Notes
CertIssuer	" "	Set this value to the name of the certificate issuer (Certificate Authority (CA)) that Nomad should use to select the appropriate PKI certificate. A case-insensitive substring-within-a-string match is performed. If you have multiple CAs you can specify a: • Common sub-string (e.g. "CORPCA" would work for certificates issued by CORPCA1 or CORPCA2) • Comma-separated list of certificate issuers (both exact names or substrings are acceptable values). For example, "DigiCert,Thawte,Verisign" would work for certificates issued by DigiCert, DigiCert EV, Thawte or Verisign. If you are only using HTTPS for downloading from an HTTPS DP (That is, not using HTTPS for peer-to-peer data transfer) you can leave this blank and set CertSubject instead.

MODULE.NOMAD.CERTSUBJECT	Defines one or more certificate subject names that Nomad uses to select the appropriate PKI certificate for authentication with Configuration Manager (CM) site systems configured to use HTTPS. It does not affect certificate selection for

Installer property	Description

client authentication certificates used for peer-to-peer authentication or for selection of server authentication certificates.

In most cases Nomad will be able to identify a suitable certificate in the Local Computer Personal certificate store without the need to specify CertSubject (refer to Peer copy over HTTP or HTTPS: Certificate Selection for more details).

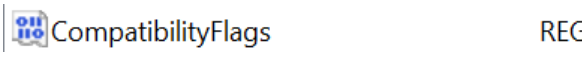
Click here to expand...

Defines one or more certificate subject names that Nomad uses to select the appropriate PKI certificate for authentication with Configuration Manager (CM) site systems configured to use HTTPS. It does not affect certificate selection for client authentication certificates used for peer-to-peer authentication or for selection of server authentication certificates.

In most cases Nomad will be able to identify a suitable certificate in the Local Computer Personal certificate store without the need to specify CertSubject (refer to Peer copy over HTTP or HTTPS: Certificate Selection for more details).

Registry value	Default value	Notes
CertSubject	" "	For downloads over HTTPS from the Distribution Point, set either the CertIssuer or CertSubject registry values. Set this value to the subject name of the certificate that Nomad should use to select the appropriate PKI certificate. The match has the following properties: • case-insensitive • a substring search is done, so if the text is set to ACME it will return certificates where ACME appears anywhere in the certificate's subject. If you have multiple valid subject names you can specify a: • Common sub-string, for example "contoso.com" would work for certificates that have contoso.com anywhere in the subject name

Installer property	Description
	• Comma-separated list of subject names or sub-strings, for example, you can specify multiple subject domain suffixes, for example "contoso.com,abc.in". For the installer property, configure either MODULE.NOMAD.CERTISSUER or MODULE.NOMAD.CERTSUBJECTinstaller properties for HTTPS downloads.
MODULE.NOMAD.COMPATIBILITYFLAGS	Determines different compatibility settings which relate to specific customer related functionality and should not generally be changed from the default value under normal conditions, unless advised.The installer property must be set to sum of the integer values for the required bits. For example, to disable hash value checking (1) and DelegatedLSZ checks and errors (131072), run *msiexec /i 1E.Client-x64.msi MODULE.NOMAD.COMPATIBILITYFLAGS=131073 [other properties] /qn* on the installer command-line. Click here to expand... Determines different compatibility settings which relate to specific customer related functionality and should not generally be changed from the default value under normal conditions, unless advised.

Registry value	Default value	Notes
CompatibilityFlags	0x1E18000A (504889354)	For Nomad in full OS, the registry value is set to the sum of the values for the required bits.  The default value combines the following settings: • *Bit 1 - 0x00000002* - Enable longer values for hashes

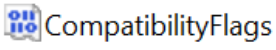
Installer property	Description

- *Bit 3 - 0x00000008* - Fix wrong IPs in election messages
- *Bit 19 - 0x00080000* - Enable full hash generation for SIS content on DPs
- *Bit 20 - 0x00100000* - Abort download on the Nomad client if an LsZ has mismatch is detected
- *Bit 25 - 0x02000000* - Turn off Dynamic Block Size
- *Bit 26 - 0x04000000* - Enable download of Windows 10 Express File Updates
- *Bit 27 - 0x08000000* - Enable download of Software Updates (including Windows 10 feature updates) from Microsoft Update - see note
- *Bit 28 - 0x10000000* - Enable support for byte-range downloads (e.g. Office 365 or delta content for updates) from Microsoft Update - see note

First bit is bit 0. The default in binary is: 0001 1110 0001 1000 0000 0000 0000 1010

Support for downloading updates from Microsoft Update

Setting bits 27 and/or 28 will enable Nomad to download content from Microsoft Update if the update has been deployed with Configuration Manager and the option
If software updates are not avail

Installer property	Description	
		able on distribution point in current, neighbor or site boundary, download content from Microsoft Update has been enabled on the Download Settings tab of the deployment. Nomad will not be used to download updates from Microsoft Update if the update is requested outside of a Configuration Manager Software Update Deployment (e.g. when using Windows Update for Business). **Note** Prior to 1E Client 4.1 (Nomad 7.0) the default was 0x00180000 (1572864): • *Bit 19 - 0x00080000* - Enable full hash generation for SIS content on DPs • *Bit 20 - 0x00100000* - Abort download on the Nomad client if an LsZ has mismatch is detected
0x00100002 (1048578)	For the task sequence action **Install and configure Nomad in Windows PE**, the registry value is set to the sum of the values for the required bits.  The default value combines the following settings: • *Bit 1 - 0x00000002* -	

Installer property	Description
	Enable longer values for hashes • *Bit 20 - 0x00100000* - Abort download on the Nomad client if an LsZ has mismatch is detected **Note** *Bit 1 - 0x00000002* (Enable longer values for hashes) is mandatory. The installer property must be set to sum of the values for the required bits, and given in decimal notation. For example, the following installer command-line uses: • *Default- 0x1E18000A* • *Bit 0 - 0x00000001* - Never check hashes of downloaded content • *Bit 17 - 0x00020000* - Disable DelegatedLSZ

Installer property	Description

checks and errors

- *Sum - 0x1E1A000B* (505020427)

```
> msiexec /i 1E.Client-x64.msi MODULE.NOMAD.COMPATIBILITYFLAGS=505020427 [other properties] /qn
```

Bit	Hex	Decimal	Description
0	*0x0001*	1	Never check hashes of downloaded content.
1	*0x0002*	2	Enable longer values for hashes. This value is auto-enabled when the Configuration Manager client is detected. You must manually configure this setting on any DP that does not have the Configuration Manager client installed. **Note** Prior to 1E Client 4.1 (Nomad 7.0) this was disabled (0) by default.
2	*0x0004*	4	Calculate CRCs as files are downloading.
3	*0x0008*	8	Fix wrong IPs in election messages. On multi-homed machines sometimes the IP from a wrong adapter can get sent in the election messages resulting in peers failing to connect to the master. Enabling this flag causes Nomad to correct such IPs at the

Installer property	Description			
				time when messages are received and thus prevent master connectivity issues.
	4	*0x0010*	16	Determines compatibility with Nomad v3.x caches. Set this option once all Nomad v3.x installations have been upgraded.
	5	*0x0020*	32	Disable all RDC data generation.
	6	*0x0040*	64	Keep Packages that failed the CRC test during P2P or download from DP.
	7	*0x0080*	128	Prevent computers using wireless connections from becoming fill-in multicast masters.
	8	*0x0100*	256	Include LinkLocal IPv4 addresses.
	9	*0x0200*	512	Include LinkLocal IPv6 addresses.
	11	*0x0800*	2048	RESERVED
	12	*0x1000*	4096	Do not automatically jump from HTTP to HTTPS during download from DP.
	13	*0x2000*	8192	Always use HTTPS. (Use this setting when Configuration Manager is configured to use HTTPS-only communication for downloading content from Distribution Points)
	14	*0x4000*	16384	RESERVED
	15	*0x8000*	32768	RESERVED
	16	*0x00010000*	65536	RESERVED (this flag is no longer used; previously this flag disabled a workaround for the issue described in Nomad post-installation tasks: IIS request filtering)

Installer property	Description		
17	*0x00020000*	131072	Disable DelegatedLSZ checks and errors.
18	*0x00040000*	262144	Disable partial download when App-V streaming, i.e. download entire application.
19	*0x00080000*	524288	Enable full hash generation for SIS content when an LsZ file is generated on a DP. If this is not enabled, SIS content is trusted, and corrupted content may be downloaded. Enabled by default.
20	*0x00100000*	1048576	Abort download on the Nomad client if an LsZ hash mismatch is detected. If this is not set, when a Nomad client detects a hash mismatch it will re-request LsZ generation on the DP then try again, and get stuck in a loop if the SIS content is corrupt. Must be set on clients if Bit 19 is set on DPs. Enabled by default.
25	*0x02000000*	33554432	Turn off Dynamic Block Size. This flag is set by default, which means Dynamic Block Size is disabled by default. **Note** Prior to 1E Client 4.1 (Nomad 7.0) this bit was off, meaning **Dynamic Block Size** was enabled by default.
26	*0x04000000*	67108864	Enable download of Windows 10 Express update files. Enabled by default. **Note** This is a new setting in 1E Client 4.1 (Nomad 7.0) and Q20144 for NomadBranch 6.3.201.
27	*0x08000000*	134217728	Enable download of full file software updates from Microsoft Update when

Installer property	Description
	deployed through Configuration Manager. Enabled by default. **Note** This is a new setting in 1E Client 4.1 (Nomad 7.0) and Q20246 for NomadBranch 6.3.201.
	28 *0x10000000* 268435456 Enable download of byte-range software updates (e.g. Express updates, O365 updates) from Microsoft Update when deployed through Configuration Manager. Enabled by default. **Note** This is a new setting in 1E Client 4.1 (Nomad 7.0) and Q20246 for NomadBranch 6.3.201.
	30 *0x40000000* 1073741824 Enable SoftwareUpdate metadata validation. This is not enabled by default. It can be used to resolve rare issues related to SoftwareUpdates where the contents could be updated without any change in its ID or version. Please refer to Resolving SoftwareUpdate metadata validation for more details. **Note** This is a new setting in 1E Client 5.1 (Nomad 7.0.200).
MODULE.NOMAD.CONTENTPROVIDERONWIFI	Determines whether a device on a WLAN can become content provider. By default, only devices connected to a LAN can become content providers when using Single Site Download (SSD). **Note** This setting is only applicable to SSD and has no effect on P2P content transfers on the local subnet. Click here to expand...

Installer property	Description

Determines whether a device on a WLAN can become content provider. By default, only devices connected to a LAN can become content providers when using Single Site Download (SSD).

Note

This setting is only applicable to SSD and has no effect on P2P content transfers on the local subnet.

Registry value	Default value	Notes
ContentProviderOnWifi	0	Values are: • 0 – Only devices connected to a LAN can be content providers • 1 – Devices connected to any network (including WLANs) can be content providers

MODULE.NOMAD.CONTENTREGISTRATION

Determines if content in Nomad's cache (packages, applications, software updates, boot images, etc.) is registered with Content Distribution. Content registration is necessary if a host is to be available as a Single Site Download (SSD) provider or can be woken up if a Nomad peer requires the content locally.

Click here to expand...

Determines if content in Nomad's cache (packages, applications, software updates, boot images, etc.) is registered with Content Distribution. Content registration is necessary if a host is to be available as a Single Site Download (SSD) provider or can be woken up if a Nomad peer requires the content locally.

Registry value	Default value	Notes
Platform\ContentRegistration	0	To enable content registration, update the value to 1 – it is found under the Platform\ContentDistribution To enable SSD when you install Nomad, you must specify the MODULE.NOMAD.SSDENABLED

Installer property	Description
	installer property and ensure the Tachyon client is enabled by specifying SWITCH and BACKGROUNDCHANNELURL installer properties. If MODULE.NOMAD.SSDENABLED is specified during installation, the registry value of ContentRegistration is automatically set to 1. If you want to enable SSD as a provider after installation, then you also need to configure the registry values for SSDEnabled and ContentRegistration, in addition to enabling the Tachyon client. The ContentDistribution registry setting is found under the Platform key. • Nomad app provides visibility of content distribution activity • Single Site Download (SSD) • Single Site Peer Backup Assistant (SSPBA) • High Availability Peer Backup Assistant (HAPBA) • Get Migration Settings task sequence action used to manage computer associations • Nomad Pre-caching • Nomad Download Pause. In legacy versions of Nomad, Platform features were provided using ActiveEfficiency. This required the PlatformURL setting to

Installer property	Description
	be configured. This is no longer required. You will see that the PlatformURL registry is used, but this is configured automatically by Nomad on startup by querying the value that the Tachyon client is using (stored in the 1EClient.conf file).
MODULE.NOMAD.DEBUG	The level of messages logged in the Nomad logs for debugging purposes. The installer property must be set to sum of the integer values for the required bits. For example, to set all three supported debug levels, run: *`msiexec /i 1E.Client-x64.msi MODULE.NOMAD.DEBUG=25 [other properties] /qn`* on the installer command-line. Click here to expand... The level of messages logged in the Nomad logs for debugging purposes.

Registry value	Default value	Notes
Debug	0x09 (9)	See the table below for customer supported values. The default is a combination of *`0x01`* (Minimal logging) and *`0x08`* (Registry changes). For example, to set maximum debugging, set bit 0, 3 and 4, which is a value of 0x19 hexadecimal or 25 decimal. Values on the installer command-line must be provided in decimal. So to set maximum debugging you would use the following installer command-line: `> msiexec /i 1E.Client-x64.msi DEBUG=25 [other properties] /qn`

Bit	Hex	Decimal	Description
0	0x01	1	Minimal logging.
1	0x02	2	RESERVED

Installer property	Description				
		2	0x04	4	RESERVED
		3	0x08	8	Registry changes.
		4	0x10	16	Additional debugging (should only be used if requested by 1E support).
MODULE.NOMAD.DOREPORTINGENABLED	Enables Delivery Optimization monitoring and reporting if ContentRegistration is enabled. Click here to expand... Enables Delivery Optimization monitoring and reporting if ContentRegistration is enabled.				

Registry value	Default value	Notes
DeliveryOptimizationReportingEnabled	0	Enables monitoring of Delivery Optimization downloads and reporting them to Tachyon Platform (ContentDistribution). Delivery Optimization monitoring and reporting is only supported in versions of Windows Server 2019 and Windows 10 Version 1909 onwards. When it is enabled, DO download events get written to .etl files in the Nomad cache folder, for example: NomadDo-20210325-182415.etl. And aggregated information about the downloads gets writtern

Installer property	Description
	to sqlite files **Do.db** and **DoDownloadMonitor.db** in LocalDb folder inside Nomad cache folder.
MODULE.NOMAD.DOWNLOADTIMEOUT	Sets the timeout in seconds after which a job will be cancelled if the download has not been successful. Click here to expand... Sets the timeout in seconds after which a job will be cancelled if the download has not been successful.
MODULE.NOMAD.DPCACHECLEANUPENABLED	Delete all obsolete LSZ files on the DP where the associated content is no longer present in ContentLib. Click here to expand... Delete all obsolete LSZ files on the DP where the associated content is no longer present in ContentLib.

Registry value	Default value	Notes
DownloadTimeout	0	This parameter is associated with the distribution point resilience feature and is used in conjunction with the *RecycleDPDelay* registry value. If a value greater than zero is set, the download timeout will either use this or the Configuration Manager setting depending on which is the smaller value. When the timeout is reached, the job package download is cancelled and a success is sent to the Configuration Manager client with the *ERROR_MAXDURATION* timeout error sent as the package status message. The default is to use the Configuration Manager setting (28 days by default).

Installer property	Description

Registry value	Default value	Notes
DpCacheCleanupEnabled	0 (turned off)	This entry controls the cached LSZ files cleaning feature. When turned on, this feature deletes all LSZ files in a Distribution Point (DP) cache where the associated content is not present in ContentLib. The following table describes the values this entry may be set to: Value: 0 — The feature is turned off. This is the default. Value: 1 (or greater) — The feature is turned on. Please refer to Cache management for details about other cache management settings.

MODULE.NOMAD.DPNOTAVAILABLECODES

Determines which error codes will cause Nomad to retry a download using an alternative distribution point.

For example, the following would set Nomad to the default value on the 1E Client installer command-line:`> msiexec /i 1E.Client-x64.msi MODULE.NOMAD.DPNOTAVAILABLECODES="0x205A,0x205D" [other properties] /qn`

Click here to expand...

Determines which error codes will cause Nomad to retry a download using an alternative distribution point.

Installer property	Description

Registry value	Default value	Notes
DPNotAvailableCodes	0x205A, 0x205D	This registry entry contains a comma-separated list of return codes, see Nomad return codes for a list of the possible ones. If Nomad encounters one of these during download it will attempt a retry from an alternative DP. It gets the list of possible DPs from Configuration Manager. The two return codes set as default are the only ones that are applicable to DP availability: • 0x205A – in valid special package path (set using *--pp*) • 0x205D – DP path not found Under normal circumstances, you would not change this from the default value. You may want to not allow failover to an alternative DP altogether, in which case you would set the value to " " in the registry. Or you may only want to failover if the DP path was not found, in which case you would set the value to 0x205D only. This installer property should be set to a string containing the comma-separated hex values. For example the following sets Nomad to failover to the next DP only when the DP path was not found: *> msiexec /i 1E.Client-x64.msi DPNOTAVAILABLECODES="0x205D" [other properties] /qn*

MODULE.NOMAD.ENFORCEQUOTAS	Determines whether Windows Disk Quotas (if configured) are enforced on the PBA share defined inCachePath. Click here to expand...

Installer property	Description

Determines whether Windows Disk Quotas (if configured) are enforced on the PBA share defined in CachePath.

Registry value	Default value	Notes
EnforceQuotas	0x0 (0)	Enables quotas to be enforced but requires Windows Disk Quotas to be configured. If the size specified in the NMDS_POLL request causes the quota to be exceeded, the request fails and you get disk full error. This registry value is found under the PBA registry key NomadBranch\NMDS.

MODULE.NOMAD.GENERATEWEREVENTS

Determines whether Windows Error Reporting memory dumps should be sent to Microsoft Winqual.

Click here to expand...

Determines whether Windows Error Reporting memory dumps should be sent to Microsoft Winqual.

Registry value	Default value	Notes
GenerateWEREvents	1	If enabled and if Nomad experiences an unexpected failure, a dialog is displayed prompting the user to send the debug information to Winqual which is forwarded to 1E for continued quality improvements. Values are: • 0 disables this feature • 1 enables this feature

MODULE.NOMAD.HAACKTIMEOUTMINS

The time-out period in minutes for the Peer Backup Assistant - High Availability (deprecated) (PBA-HA) task sequence action. If a machine running this action does not receive an acknowledgement message within this period from the PBA host performing the additional backups, the action will fail.

Click here to expand...

Installer property	Description

The time-out period in minutes for the Peer Backup Assistant - High Availability (deprecated) (PBA-HA) task sequence action. If a machine running this action does not receive an acknowledgement message within this period from the PBA host performing the additional backups, the action will fail.

Registry value	Default value	Notes
HAACKTimeoutMins	20	Applies to synchronized backups only. The PBA tost sends the acknowledgement messages back to the machine running the task sequence approximately every 5% of the synchronized copy. This registry value is found under the PBA registry key NomadBranch\NMDS.

MODULE.NOMAD.LOCALSSDSTAGGER

Sets the site SSD query stagger duration (seconds).

Click here to expand...

Sets the site SSD query stagger duration (seconds).

Deployments to large numbers of clients (30,000 or more) generate significant network traffic from 1E Client to Content Distribution that may result in IIS 503 Overload errors on the server, causing content registrations and SSD requests to fail. LocalSsdStagger allows an elected subnet master to wait for a random configurable time before making a local SSD request. All peers in the subnet participating in the election would also synchronize and wait for the same time before copying from master machine.

Registry value	Type	Default value	Notes
LocalSsdStagger	REG_DWORD	5	Sets the local SSD query stagger duration in seconds. The stagger is 0 (disabled) by default. The maximum value that can configured is 600 seconds (10 minutes).

Installer property	Description
	There is no SSD staggering in WinPE. Local SSD happens when only when network broadcast is disabled. **Note** Please consult 1E before changing this value. This setting works in conjunction with SiteSsdStagger.
MODULE.NOMAD.LOGNAME	Name of the Nomad log file. This value is preserved upon upgrade. This property is combined with MODULE.NOMAD.LOGPATH to create registry value LogFileName. The default value is *NomadBranch.log*
MODULE.NOMAD.LOGPATH	Location of the Nomad log file. The path will be created if it does not exist. This value is preserved upon upgrade. Default values are dependent on OS. This property is combined with MODULE.NOMAD.LOGNAME to create the registry value LogFileName. The default location is: *%ALLUSERSPROFILE%\1E\NomadBranch\LogFiles*
MODULE.NOMAD.MADCAPSCOPE	The MADCAP scope for multicast. Click here to expand... The MADCAP scope for multicast. **Warning** The Multicast feature is not supported in the Tachyon 5.2 release. This feature is under consideration for re-design and may be available in future versions of Nomad.

Registry value	Default value	Notes
MultiCastMADCAPScope	SMSNomad	Values may be set using either of the formats in the table below.

Installer property	Description

Format	Description
<ScopeName>	*<ScopeName>* is the name of a scope defined in the DHCP (if you are using the Microsoft implementation of MADCAP). Use this format if you have multiple MADCAP servers. This method uses the time to live settings for the scope.
<MADCAP_ServerIP> *<MADCAP_Scope_IP>* *<TTL>*	• *<MADCAP_ServerIP>* is the IP address of a specific MADCAP server • *<MADCAP_ScopeIP>* is the starting IP address for a MADCAP scope defined in the DHCP (if you are using the Microsoft implementation of MADCAP) • *<TTL>* is the time to live for the multicast packets **Note** Using a TTL greater than 1 is not recommended unless you have ensured that multicast traffic cannot leak back upstream through any intervening routers. The valid range for TTL is a number between 1 and 255

Nomad is also capable of performing control multicast without a MADCAP server installation on the network. In order to use this feature, the *<MADCAP_ServerIP>* must be set to *0.0.0.0*. For example, the following supports MADCAP server not being present, with a scope of *239.0.9.0* and a time to live of *3*.

```
0.0.0.0,239.0.9.0,3
```

MODULE.NOMAD.MAXALLOCREQUEST	Sets the maximum amount of space in MB that can be requested by each PBA client. Click here to expand...

Installer property	Description

Sets the maximum amount of space in MB that can be requested by each PBA client.

Registry value	Default value	Notes
MaxAllocRequest	0xC8 (200)	Located under the PBA registry key NomadBranch\NMDS.

MODULE.NOMAD.MAXCACHEDAYS

When the Nomad cache cleaner runs, delete any application or package content that last triggered Nomad elections before the specified number of days ago.

Click here to expand...

When the Nomad cache cleaner runs, delete any application or package content that last triggered Nomad elections before the specified number of days ago.

Registry value	Default value	Notes
MaxCacheDays	0 (turned off)	Set to delete application or package content that last triggered Nomad elections before the specified number of days from the date the cache cleaner runs. This ensures that only application or package content that have triggered elections recently will be kept in the cache. 0 means that application and package content will not be deleted automatically when the cache cleaner runs. Please refer to Cache management for details about other cache management settings.

MODULE.NOMAD.MAXCA

This is the maximum number of days content is present on a client.

Click here to expand...

<table>
<tr><th>Installer property</th><th>Description</th></tr>
<tr><td>CHEDAYSTHRESHOLD</td><td>This is the maximum number of days content is present on a client.
<table>
<tr><th>Registry value</th><th>Type</th><th>Default value</th><th>Notes</th></tr>
<tr><td>MaxCacheDaysThreshold</td><td>REG_DWORD</td><td>0</td><td>This is the maximum number of days content is present on a client. If it's not zero, then content will be deleted without any other checks once it reaches the threshold. If the threshold has a value greater than zero and less than 30, Nomad uses the threshold of 30 days and creates an associated log.

Default value is 0.

New setting introduced in 8.0.

Please refer to Cache management for details about other cache management settings.</td></tr>
</table></td></tr>
<tr><td>MODULE.NOMAD.MAXCACHESIZEMB</td><td>Provided for backward compatibility only – use PercentAvailableDisk instead. The value (in bytes) for the maximum size the cache is allowed to grow to, before automatic cache cleaning takes place.

Click here to expand...

Provided for backward compatibility only – use PercentAvailableDisk instead. The value (in bytes) for the maximum size the cache is allowed to grow to, before automatic cache cleaning takes place.</td></tr>
</table>

Installer property	Description

Registry value	Default value	Notes
MaxCacheSizeMB	0	There is no maximum value for this property. This method for determining the maximum size of the cache is an alternative to PercentAvailableDisk: • If PercentAvailableDisk has a value greater than zero set its method will be used to control the cache size. • If MaxCacheSizeMB is set to a value greater than zero and PercentAvailableDisk is set to zero thenMaxCacheSizeMB will be used as the method for determining the maximum size of the Nomad cache.

MODULE.NOMAD.MAXCONCURRENCY

Sets the maximum number of concurrent PBA sessions that may be in use on the host.

Click here to expand...

Sets the maximum number of concurrent PBA sessions that may be in use on the host.

Registry value	Default value	Notes
MaxConcurrency	0x3 (3)	Located under the PBA registry key NomadBranch\NMDS.

MODULE.NOMAD.MAXDEVICESFROMAE

The maximum number of devices with the content that Nomad can retrieve from Content Distribution in one call.

Click here to expand...

The maximum number of devices with the content that Nomad can retrieve from Content Distribution in one call.

Installer property	Description

Registry value	Default value	Notes
MaxDevicesFromAE	10	The maximum number of devices (i.e. machines) with the content (package, application or software update) that Nomad can retrieve from Content Distribution in one call. The maximum value is 20.

MODULE.NOMAD.MAXELECTIONRESPONSELOGGING

Defines the number of election responses Nomad will write to the log for a given election.

Click here to expand...

Defines the number of election responses Nomad will write to the log for a given election.

Registry value	Default value	Notes
MaxElectionResponseLogging	By default this REG_DWORD value is not present and all election responses are logged.	Add this REG_DWORD value and set it to the number of responses that Nomad should log for any given election. Setting the value to 0 effectively turns off logging of any election responses.

Note

The value of MaxElectionResponseLogging specifies the number of election replies to be logged per election request. As an example, if MaxElectionResponseLogging = 5 and there are two election requests for the same package at different times, a maximum of 5 election responses will be logged for each elections (up to 10 election replies in total). If there are two concurrent election requests for the same package, the number of maximum election replies logged may vary from 5 to 10. In general, if MaxElectionResponseLogging = *n* and if there are *m* concurrent election requests for the same package, the number of maximum election replies logged may vary from *n* to *m***n*.

Installer property	Description
MODULE.NOMAD.MAXIMUMMEGABYTE	The maximum amount of space (in MB) that can be used for all the PBA shares combined on the host. Click here to expand... The maximum amount of space (in MB) that can be used for all the PBA shares combined on the host. Registry value: MaximumMegaByte Default value: 0 Notes: A non-zero value enables PBA share. This registry value is located under the PBA registry key NomadBranch\NMDS.
MODULE.NOMAD.MAXLOGSIZE	The maximum size (in bytes) of the Nomad log file. Default is 5MB. Click here to expand... The maximum size (in bytes) of the Nomad log file. Default is 5MB. Registry value: MaxLogFileSize Default value: 5242880 Notes: When the log file reaches this size, it is renamed with a *.LO_* extension and a new *.LOG* file is created. The *.LO* file is overwritten each time. **Note** The default has been increased from 1048576 (1MB) to 5242880 (5MB) for Nomad 7.0 onwards (1E Client 4.1). **Note** The installer property name is different to the registry name.
MODULE.NOMAD.MAXPACKAGEFAST	The maximum size (in bytes) of a package that Nomad attempts to cache on a Fast LAN (>500 kbps) connection. Click here to expand...

Installer property	Description
	The maximum size (in bytes) of a package that Nomad attempts to cache on a Fast LAN (>500 kbps) connection. Registry value: MaxPackageSizeFastLAN Default value: 0 Notes: Works in conjunction with the RunUncachedPermittedFastLAN registry value. **Note** The installer property name is different to the registry name.
MODULE.NOMAD.MAXPACKAGERAS	The maximum size (in bytes) of a package that Nomad will attempt to cache on a RAS (<55 kbps) connection. Click here to expand... The maximum size (in bytes) of a package that Nomad will attempt to cache on a RAS (<55 kbps) connection. Registry value: MaxPackageSizeRAS Default value: 0 Notes: **Note** The installer property name is different to the registry name.
MODULE.NOMAD.MAXPACKAGESLOW	Maximum size (in bytes) of a package that Nomad attempts to cache on a Slow LAN (55-500 kbps) connection. Click here to expand... Maximum size (in bytes) of a package that Nomad attempts to cache on a Slow LAN (55-500 kbps) connection.

Installer property	Description

Registry value	Default value	Notes
MaxPackageSizeSlowLAN	0	**Note** The installer property name is different to the registry name.

MODULE.NOMAD.MAXPACKETSPERSECOND

The maximum rate at which multicast packets are sent.

Click here to expand...

The maximum rate at which multicast packets are sent.

Warning

The Multicast feature is not supported in the Tachyon 5.2 release. This feature is under consideration for re-design and may be available in future versions of Nomad.

Registry value	Default value	Notes
MaxPacketsPerSecond	800	Modify this value with caution. If packets are sent too fast, machines will drop packets and multicast will not be effective - too slow and multicast works, but slowly. The default value is indicative of how this should be set.

MODULE.NOMAD.MAXPRECACHEDAYS

When the Nomad cache cleaner runs, delete any pre-cached content that last triggered Nomad elections before the specified number of days ago.

Click here to expand...

When the Nomad cache cleaner runs, delete any pre-cached content that last triggered Nomad elections before the specified number of days ago.

Installer property	Description

Registry value	Default value	Notes
MaxPreCacheDays	0 (turned off)	Set to delete pre-cached content that last triggered Nomad elections before the specified number of days from the date the cache cleaner runs. This ensures that only pre-cached content that has triggered elections recently will be kept in the cache. 0 means that pre-cached content will not be deleted automatically when the cache cleaner runs. Please refer to Cache management for details about other cache management settings.

MODULE.NOMAD.MAXSTATUSFREQUENCY

he minimum interval (in seconds) between sending transfer progress status messages, thereby governing the overall maximum frequency for sending the messages.

Click here to expand...

he minimum interval (in seconds) between sending transfer progress status messages, thereby governing the overall maximum frequency for sending the messages.

Registry value	Default value	Notes
MaxStatusFrequency	3600	Works in conjunction with the ++sm setting on the Nomad properties tab and the StatusMsgEvents registry values.

MODULE.NOMAD.MAXSTUCKCOUNT

Registry value to hold an integer determining the number of times Nomad attempts to copy content and gets stuck before aborting.

Click here to expand...

Installer property	Description

Registry value to hold an integer determining the number of times Nomad attempts to copy content and gets stuck before aborting.

If you update the registry, you must restart the Nomad service for you changes to take effect. We recommend backing up your registry before you do this.

Registry value	Default value	Notes
MaxStuckCount	100	The number of times Nomad attempts to copy content after failure (such as network outages, incomplete LSZ files, hash mismatches, election issues, connecting with peers) before it aborts the operation. The range is 3 to 1000, but if the value is less than 3 or greater than 1000, it sets to the default of 100. **Warning** The MaxStuckCount value is an internal NomadBranch registry value. You should not change this value unless advised by 1E.

Do not use unless advised by 1E.

MODULE.NOMAD.MAXSUCACHEDAYS

When the Nomad cache cleaner runs, delete any software updates that last triggered Nomad elections before the specified number of days ago.

Click here to expand...

When the Nomad cache cleaner runs, delete any software updates that last triggered Nomad elections before the specified number of days ago.

Registry value	Default value	Notes
MaxSUCacheDays	0 (turned off)	Set to delete software updates that last triggered Nomad elections before the

Installer property	Description
	specified number of days from the date the cache cleaner runs. This ensures that only software updates that have triggered elections recently will be kept in the cache. 0 means that software updates will not be deleted automatically when the cache cleaner runs. Please refer to Cache management for details about other cache management settings.
MODULE.NOMAD.MULTICASTSUPPORT	The behavior of local multicast. Click here to expand... The behavior of local multicast. **Warning** The Multicast feature is not supported in the Tachyon 5.2 release. This feature is under consideration for re-design and may be available in future versions of Nomad.

Registry value	Default value	Notes
MulticastSupport	0x0 (0)	All machines in a single branch must be configured using the same value for this parameter. If you are not using multicast, deploy the Nomad branch agent with the MULTICASTSUPPORT property set to 0 to reduce the noise in Nomad logs. Prior to Nomad 7.0 multicast was enabled (0x1) by default. Now it is disabled (0x0) by default.

Installer property	Description

Bit	Hex	Decimal	Description
	0x0	0	**No Multicast**– disables the feature.
0	0x1	1	**Data Only Multicast** – choose this for a standard Nomad multicast. Data refers to the content of the downloaded package. Nomad control communications are broadcast as normal on the local subnet. Select this option for standard functionality.
1	0x2	2	**Control Only Multicast** – control information refers to the communications between Nomad enabled machines, especially for elections. This may be used if there is more than one subnet in a single location to enable a single Nomad master to be elected for all the subnets.
	0x3	3	**Control and Data Multicast** – data and control information is multicast. Select this option if a branch has multiple subnets connected by high speed routers.

MODULE.NOMAD.NOHARDLINK

Determines whether hard links are used between the Nomad cache and the Configuration Manager cache.

Click here to expand...

Determines whether hard links are used between the Nomad cache and the Configuration Manager cache.

Registry value	Default value	Notes
NoHardlink	0	Values are: • 0 – hard links are used. The Nomad cache will link to the Configuration Manager cache

Installer property	Description
	so only a single copy of a package is held locally. • 1 – hard links are not used and results in the content being double-cached For more detail about the Nomad Cache please refer to Nomad cache.
MODULE.NOMAD.NOMADINHIBITEDADSITES	Prevents Nomad from calling an election when it is connected to a specified AD site, meaning that each Nomad client on the listed AD sites will automatically become a Nomad master. This prevents P2P sharing, as each master downloads its own copy of the content. Click here to expand... Prevents Nomad from calling an election when it is connected to a specified AD site, meaning that each Nomad client on the listed AD sites will automatically become a Nomad master. This prevents P2P sharing, as each master downloads its own copy of the content.

Registry value	Default value	Notes
NomadInhibitedADSites	(empty)	A comma-separated list for each AD site to be inhibited. Useful for sites with: • a local DP • a VPN without isolation For example, to inhibit three AD sites called site1, site2 and site3: `site1,site2,site3` Please refer to Design Considerations: Inhibiting subnets and sites.

Installer property	Description
MODULE.NOMAD.NOMAD	Prevents Nomad from calling an election when it is connected to a specified IP subnet, meaning that each Nomad client on the IP subnet automatically

Installer property	Description
INHIBITEDSUBNETS	becomes a Nomad master. This prevents P2P sharing, as each master downloads its own copy of the content. Click here to expand... Prevents Nomad from calling an election when it is connected to a specified IP subnet, meaning that each Nomad client on the IP subnet automatically becomes a Nomad master. This prevents P2P sharing, as each master downloads its own copy of the content. Registry value: NomadInhibitedSubnets Default value: (empty) Notes: A comma-separated list of each subnet to be inhibited in CIDR notation. Useful for sites with either of the following: • a local DP • a VPN without isolation For example, to isolate two subnets: `10.2.0.0/16,192.168.9.0/24` Please refer to Design Considerations: Inhibiting subnets and sites.
MODULE.NOMAD.P2PDISQUALIFYMAXNUMPEERS	Defines the max number of devices which a device will disqualify during a peer-to-peer copy. Click here to expand... Defines the max number of devices which a device will disqualify during a peer-to-peer copy. If you update the registry, you must restart the Nomad service for you changes to take effect. We recommend backing up your registry before you do this. Registry value: P2PDisqualifyMaxNumPeers Default value: 5 Notes: A device does not further disqualify a peer if it has disqualified

Installer property	Description
	P2PDisqualifyMaxNumPeers number of peers within last P2PDisqualifyMaxWindowMins minutes. **Warning** The P2PDisqualifyMaxNumPeers value is an internal NomadBranch registry value. You should not change this value unless advised by 1E. Do not use unless advised by 1E.
MODULE.NOMAD.P2PDISQUALIFYMAXWINDOWMINS	Defines the max number of minutes within which a device will disqualify a peer during a peer-to-peer copy. Click here to expand... Defines the max number of minutes within which a device will disqualify a peer during a peer-to-peer copy. If you update the registry, you must restart the Nomad service for you changes to take effect. We recommend backing up your registry before you do this.

Registry value	Default value	Notes
P2PDisqualifyMaxWindowMins	60	A device does not further disqualify a peer if it has disqualified P2PDisqualifyMaxNumPeers number of peers within last P2PDisqualifyMaxWindowMins minutes. **Warning** The P2PDisqualifyMaxWindowMins value is an internal NomadBranch registry value. You should not

Installer property	Description
	change this value unless advised by 1E. Do not use unless advised by 1E.
MODULE.NOMAD.P2PENABLED	Determines how the Nomad cache is accessed. Please refer to Nomad cache for more details. The installer property must be set to sum of the integer values for the required bits. For example, the following would set Nomad to use connectionless P2P on the 1E Client installer command-line: *> msiexec /i 1E.Client-x64.msi MODULE.NOMAD.P2PENABLED=6 [other properties] /qn* Click here to expand... Determines how the Nomad cache is accessed. Please refer to Nomad cache for more details.

Registry value	Default value	Notes
P2PEnabled	9	The default (Hex 0x0009) configures P2P to use SMB and Net Literal Names. You can set more than one option at the same time by combining the bit values. See the table below for details. **Note** We recommend restarting the Nomad Branch service when you modify this parameter.

Bit	Hex	Decimal	Notes
0	0x0001	1	(Default) Use the SMB protocol to share its own cache, and create the NomadSHR file share upon the start of the Nomad service, unless the CustomShare option has been enabled in SpecialNetShare. When

Installer property	Description			
				P2PEnabled is set in addition to Bit 5 (use HTTP) or Bit 6 (use HTTPS), Nomad will attempt to use HTTPS/HTTP and will fall-back to SMB if HTTPS/HTTP is unavailable on other peers. To disable SMB P2P, set this bit to 0.
		1	0x0002	2	Enable connectionless P2P server.
		2	0x0004	4	Enable connectionless P2P client.
		3	0x0008	8	(Default) Use Net Literal Names when connecting to P2P shares. This causes Nomad to use the Nomad master's IP address when connecting to the share and is recommended when running wirelessly.
		4	0x0010	16	Use FQDN when connecting to P2P shares. Recommended when using a multi-forest environment where computers from different forests may be present in the same subnet. This requires that reverse lookup for IP addresses is correctly configured and running. If this is not available Nomad will revert to using the IP address for connecting to the P2P shares.
		5	0x0020	32	Use the HTTP protocol to share its own cache and access other caches.
		6	0x0040	64	Use the HTTPS protocol to share its own cache and access other caches.
MODULE.NOMAD.P2PHTTPPORT	The HTTP port to use for peer copy. Click here to expand... The HTTP port to use for peer copy.				

Installer property	Description

Registry value	Default value	Notes
P2PHttpPort	5080	Default HTTP port to use for peer copy. If you are using a custom port, ensure that all agents use the same custom port.

MODULE.NOMAD.P2PHTTPSPORT

The HTTPS port to use for peer copy.

Click here to expand...

Registry value	Default value	Notes
P2PHttpsPort	5443	Default HTTPS port to use for peer copy. If you are using a custom port, ensure that all agents use the same custom port.

MODULE.NOMAD.P2PPORT

Port used to broadcast election messages, for connectionless cache access and package status broadcasts.

Click here to expand...

Port used to broadcast election messages, for connectionless cache access and package status broadcasts.

Registry value	Default value	Notes
P2P_Port	1779	

MODULE.NOMAD.P2PSSLSETTINGS

Defines server and client authentication options when using HTTPS for P2P content transfer (i.e. P2PEnabled 0x60 option is set).

Click here to expand...

Defines server and client authentication options when using HTTPS for P2P content transfer (i.e. P2PEnabled 0x60 option is set).

Installer property	Description

Registry value	Default value	Notes
P2PSslSettings	0	The default value (0) configures Nomad to use a self-signed certificate for server authentication and disables certificate-based client authentication. P2PSslSettings is a numeric value where, when represented in binary, each bit represents a configurable option as defined in the table below. You can combine these options to derive the required value, for example setting P2PSslSettings to 3 (0x1 + 0x2) configures Nomad to use a PKI certificate for server authentication and also enables certificate-based authentication. These options are only applicable if the HTTPS protocol has been enabled in the P2PEnabled setting. If you are using PKI certificates you must deploy the certificates to all clients before enabling this option. Refer to Peer copy over HTTP or HTTPS for further details on using HTTPS and associated authentication.

Bit	Hex	Decimal	Notes
0	0x0001	1	If not set (0), use self-signed certificate for server (Master) authentication If set (1), use PKI certificate for server (Master) authentication
1	0x0002	2	Enables certificate-based client authentication (Requires a PKI client authentication certificate)

Note

Installer property	Description
	If this option is enabled and the Configuration Manager client is using self-signed client authentication certificates (or Nomad is being used outside of CM), you should specify CertIssuer to ensure Nomad uses the intended certificate.
MODULE.NOMAD.PERCENTAVAILABLEDISK	The limit on the Nomad cache. Specified as a percentage of the available disk space, it controls the automatic cache cleaning to ensure that the cache does not grow to a size whereby the percentage of available disk space is less than this value. Click here to expand... The limit on the Nomad cache. Specified as a percentage of the available disk space, it controls the automatic cache cleaning to ensure that the cache does not grow to a size whereby the percentage of available disk space is less than this value.

Registry value	Default value	Notes
PercentAvailableDisk	10	By default, the cache will not grow such that less that #UUID146b7586a8d378aba88bc74a4d10ae9110 % of total disk space is available. The maximum value is 80. The cache will not grow beyond 20% of the total available disk space. This method for determining the maximum size of the cache is provided as an alternative to MaxCacheSizeMB: • If PercentAvailableDisk is greater than zero, its method is used to control the cache size • IfMaxCacheSizeMB is greater than zero and PercentAvailableDisk is zero, then MaxCacheSizeMB is used as the method for determining the maximum size of the Nomad cache.

Installer property	Description
MODULE.NOMAD.PERMITTEDLSZSHARES	Restricts Nomad LSZ file generation requests to a list of permitted package source locations. Click here to expand... Restricts Nomad LSZ file generation requests to a list of permitted package source locations.

Registry value	Default value	Notes
PermittedLSZShares	SMSPKG*$ SMS_DP_SMSPKG*$	A list of comma-separated package source locations. Enables increased security and is only used by the Nomad client installed on a distribution point. Nomad LSZ file generation requests will only be completed if the content location is listed. If you are using additional package source locations, you must manually add these to this registry value. *PermittedLSZShares* can incorporate wildcard characters to provide flexible naming convention support. If you leave the registry value blank, security checks on package source locations are not carried out. **Note** When Configuration Manager (specifically Distribution Point servers) is configured to use HTTPS only, you must also add *NOCERT_SMS_DP_SMSPKG*$* and CCMTOKENAUTH_SMS_DP_SMSPKG*$ to the PermittedLSZShares registry value.

<table>
<tr><th>Installer property</th><th>Description</th></tr>
<tr><td>MODULE.NOMAD.PERMITUNCACHED</td><td>Determines where the download package is run from under certain conditions.

Click here to expand...

Determines where the download package is run from under certain conditions.

<table>
<tr><th>Registry value</th><th>Default value</th><th>Notes</th></tr>
<tr><td>RunUncachedPermittedFastLAN</td><td>0</td><td>Works in conjunction with MaxPackageSizeFastLAN (which needs to contain a value value greater than zero). Values are:

• 0 – do not run package from the distribution point.

• 1 – run package directly from the distribution point if there is either insufficient disk space to create the cache, or the maximum package threshold is exceeded but the connection is fast (>500kbps).

To ensure that the un-cached mode works correctly, set the Program Environment Properties to include the Drive mode/Require drive letter option.</td></tr>
</table>
</td></tr>
<tr><td>MODULE.NOMAD.PLATFORMURL</td><td>The URL of the Tachyon Platform, specifically the Tachyon Background Channel, which provides a reverse proxy for the Content Distribution component of Tachyon Platform. Usually of the form https://<BackgroundChannelServer>:<BackgroundChannelPort>/Background/

Click here to expand...</td></tr>
</table>

Installer property	Description

Note

Platform features are now enabled by using the BackgroundChannelUrl instead of PlatformURL.

The URL of the Tachyon Platform, specifically the Tachyon Background Channel, which provides a reverse proxy for the Content Distribution component of Tachyon Platform. Usually of the form *https://<BackgroundChannelServer>:<BackgroundChannelPort>/Background/*

Registry value	Default value	Notes
PlatformURL	(empty)	Located under the following registry keys, depending on the component. • For *NomadBranch*, it is found under *HKLM\Software\1E\NomadBranch\Platform* • For *NomadBranchAdminUIExt* on 64-bit machines, it is found under *HKLM\Software\Wow6432Node\1E\NomadAdminUI\Platform* • For *NomadBranchAdminUIExt* on 32-bit machines, it is found under *HKLM\Software\1E\NomadAdminUI\Platform* **Warning** Do not configure this registry setting, it is automatically configured on service startup. To enable SSD when you install Nomad, you must specify the MODULE.NOMAD.SSDENABLED installer property and ensure the Tachyon client is enabled by specifying SWITCH and BACKGROUNDCHANNELURL installer properties. If MODULE.NOMAD.SSDENABLED is specified during installation, the registry value of ContentRegistration is automatically set to 1. If you want to enable SSD as a provider after installation, then you also need to configure the registry values for SSDEnabled and ContentRegistration, in

Installer property	Description
	addition to enabling the Tachyon client. The ContentDistribution registry setting is found under the Platform key. • Nomad app provides visibility of content distribution activity • Single Site Download (SSD) • Single Site Peer Backup Assistant (SSPBA) • High Availability Peer Backup Assistant (HAPBA) • Get Migration Settings task sequence action used to manage computer associations • Nomad Pre-caching • Nomad Download Pause. In legacy versions of Nomad, Platform features were provided using ActiveEfficiency. This required the PlatformURL setting to be configured. This is no longer required. You will see that the PlatformURL registry is used, but this is configured automatically by Nomad on startup by querying the value that the Tachyon client is using (stored in the 1EClient.conf file).
MODULE.NOMAD.POSTCOMPLETETIMEOUTHOURS	The duration (in hours) after which the PBA share is deleted from the host. Click here to expand... The duration (in hours) after which the PBA share is deleted from the host.

Registry value	Default value	Notes
PostCompleteTimeoutHours	0xA8 (168)	Only applies to a PBA share after the NMDS_COMPLETE command has been run for it, otherwise the PreCompleteTimeoutHours value will apply. The intention is that an incomplete share will only be available for a short period of time,

Installer property	Description
	defined in PreCompleteTimeoutHours. Once the NMDS_COMPLETE command is sent, it will be fixed for this longer time. When the share is deleted the folder and associated user will be removed. This registry value is found under the PBA registry key NomadBranch\NMDS.
MODULE.NOMAD.PRECACHEPOLLBATCHSIZE	The number of notifications a client processes in one pre-cache poll cycle. Click here to expand... The number of notifications a client processes in one pre-cache poll cycle. Registry value: PrecachePollBatchSize Default value: 20 Notes: Range is 1 to 500. If the value is greater than 500, it defaults to 500. If you set the value to 0, it defaults to 20.
MODULE.NOMAD.PRECACHEPOLLMINUTES	The interval (in minutes) between Nomad polling Content Distribution for new pre-cache jobs. Click here to expand... The interval (in minutes) between Nomad polling Content Distribution for new pre-cache jobs. Registry value: PrecachePollMinutes Default value: 0x5A0 (1440) Notes: Nomad clients normally start their polling cycle when the service starts-up, with a random delay to minimize the possibility of concurrent polls from different clients.

Installer property	Description
	The range is 60 - 525600 (1 year). 0 disables polling
MODULE.NOMAD.PRECOMPLETETIMEOUTHOURS	The duration (in hours) after which PBA share is deleted from the host. Click here to expand... The duration (in hours) after which PBA share is deleted from the host.

Registry value	Default value	Notes
PreCompleteTimeoutHours	0x3 (3)	Located under the PBA registry key NomadBranch\NMDS, it only applies to a PBA share after the NMDS_POLL command has been run, but not the NMDS_COMPLETE command. The intention is that an incomplete share will only be available for a short period of time. When the share is deleted the folder and associated user is removed.

Installer property	Description
MODULE.NOMAD.RECYCLEDPDELAY	The delay (in seconds) before restarting retries from the first DP after the whole list of available DPs have been tried. Click here to expand... The delay (in seconds) before restarting retries from the first DP after the whole list of available DPs have been tried.

Registry value	Default value	Notes
RecycleDPDelay	600	It is associated with the distribution point resilience feature and is used in conjunction with DownloadTimeout. The default equates to 10 minutes.

Installer property	Description
MODULE.NOMAD.RANDOMIZEREMOTEPATHS	Allows you to enable and disable the remote paths randomization for CM and pre-cache jobs. Click here to expand... Allows you to enable and disable the remote paths randomization for CM and pre-cache jobs. When Nomad begins content download, its content is pulled from the same distribution point by every client. For example, If a site has four Distribution Points (DP), the first one in the list is always used for downloading. In a very large environment, this can put an unnecessary load on a single DP. Using**RandomizeRemotePaths**Nomad can randomize the content location list.

Registry value	Type	Default value	Notes
RandomizeRemotePaths	REG_DWORD	0	By default, RandomizeRemotePaths is not present in the Nomad registry hive. To change the value, you need to create it and set your desired value. You can enable and disable the remote paths randomization for either Configuration Manager (CM) or pre-cache jobs using the following bits:

Bit	Hex	Decimal	Notes
0	0x0001	1	Enable remote paths randomization for CM jobs.

Installer property	Description				
		1	0x0002	2	Enable remote paths randomization for Pre-cache jobs.

MODULE.NOMAD.SIGSFOLDER

The path to the Configuration Manager signature files.

Click here to expand...

The path to the Configuration Manager signature files.

Registry value	Default value	Notes
SigsFolder	C:\SMSSIG$	Relates to RDC integration and must point to the folder where the signature files are held for Configuration Manager. Wildcards are not allowed. For example: `E:\SMSSIG$` When it is not set, Nomad assumes that signature files location as *`C:\SMSSIG$`*, if it exists.

MODULE.NOMAD.SITESSDSTAGGER

Sets the site SSD query stagger duration (seconds).

Click here to expand...

Sets the site SSD query stagger duration (seconds).

Deployments to large numbers of clients (30,000 or more) generate significant network traffic from 1E Clients to ContentDistribution that may result in IIS 503 Overload errors on the server, causing content registrations and SSD requests to fail. SiteSsdStagger allows an elected subnet master to wait for a random configurable time before making a site SSD request. All peers in the subnet participating in the election would also synchronize and wait for the same time before copying from master machine.

Installer property	Description

Registry value	Type	Default value	Notes
SiteSsdStagger	REG_DWORD	0	Sets the site SSD query stagger duration in seconds. The stagger is 0 (disabled) by default. The maximum value that can configured is 300 seconds (5 minutes). There is no SSD staggering in WinPE. Site SSD happens when broadcast is enabled or if local SSD is enabled and it does not return any devices from ActiveEfficiency. **Note** Please consult 1E before changing this value. This setting works in conjunction with LocalSsdStagger.

MODULE.NOMAD.SITESSDMINPACKAGESIZEKB

Allows you to configure a minimum content size before making an SSD request.

Click here to expand...

Allows you to configure a minimum content size before making an SSD request.

Registry value	Type	Default value	Notes
SiteSSDMinPackageSizeKB	REG_DWORD	0	The default value is 0 which can be changed after installation when it will be an installer property. There is no lower limit for this key, upper limit

Installer property	Description
	is 10240. If the registry value is greater than 10240, the agent will only consider 10240 and will log a warning. Size of content is first taken from Job data, if that's not available it's taken from the LST file, if it's not present there, this key is ignored and an SSD request is made irrespective of size. **Note** This check is for site SSD, not for local SSD.
MODULE.NOMAD.SPECIALNETSHARE	Sets various special feature options related to the Nomad share. The installer property must be set to sum of the integer values for the required bits. For example, to use the computer$ account for access to the Nomad share, and have custom share permissions, you would set the value for the SpecialNetShare registry entry to 129 (0x81 hex). This is shown in the following 1E Client installer command-line: `> msiexec /i 1E.Client-x64.msi MODULE.NOMAD.SPECIALNETSHARE=129 [other properties] /qn` Click here to expand... Sets various special feature options related to the Nomad share.

Registry value	Default value	Notes
SpecialNetShare	0x2060 (8288)	You can set more than one option at the same time by combining the bit values. For example, to have custom share permissions and use the machine account for access to the Nomad share,

Installer property	Description

set the value for SpecialNetShare to 129 (decimal value 1+128 or 0x0081 hex). See The Nomad share for more detail on configuration and security.

The default value in different versions has changed, based on feedback. Upgrading does not change the value unless explicitly set.

Nomad version	Default in MSI
Nomad 8.0 (1E Client 8.0)	0x2060 (8288) • Bit 5: Disables broadcast of download statistics • Bit 6: Enable Nomad FanOut • Bit 13: Use HTTP/S or SMB
Nomad 7.1 (1E Client 5.2) Nomad 7.0 (1E Client 4.1 to 5.1)	0x2020 (8224) • Bit 5: Disables broadcast of download statistics • Bit 13: Use HTTP/S or SMB
Nomad 6.x	0x0000 (0) • No special features enabled.

The default used in all versions of Client Deployment Assistant (and earlier Endpoint Agent Installer) is 0x2070 (8304):

Installer property	Description
	• Bit 4: Enable Nomad hidden share as NomadSHR$ • Bit 5: Disables broadcast of download statistics • Bit 6: Enable Nomad FanOut • Bit 13: Use HTTP/S or SMB

Bit	Hex	Decimal	Description
	0x0000	0	No special features enabled.
0	0x0001	1	Custom Share Permissions: Administrators configure and manage custom share permissions. The service doesn't create the *NomadSHR* share on start-up, leaving the administrator to manually create it and set the permissions. It is also not deleted when the service stops and therefore existing share permissions are preserved.
1	0x0002	2	Enables support for IPv6: If the network supports both IPv6 and IPv4, enable support for both – set bit 1 but not bit 2.
2	0x0004	4	Disables support for IPv4: If the network supports only IPv6, disable IPv4 and set both bit 1 and bit 2.
3	0x0008	8	RESERVED
4	0x0010	16	The Nomad share is hidden and named *NomadSHR$*. When using a hidden share, all Nomad installations must be configured to use this option. See The Nomad share for more detail on configuration and security.
5	0x0020	32	Disables broadcast of download statistics. By default, this is disabled. If enabled, Nomad

Installer property			Description
			broadcasts download statistics to all peers when a download is complete. **Note** Prior to 1E Client 4.1 (Nomad 7.0) this was enabled (0) by default, now it is disabled (1) by default.
	6	0x0040	64	Enables Nomad FanOut.
	7	0x0080	128	The machine account is used when connecting to a peer client. The SMSNomadP2P& account is not created. Please refer to The Nomad share: Use Machine Account. **Note** Will not work if peers exist in untrusted domains or workgroups.
	8	0x0100	256	RESERVED
	9	0x0200	512	RESERVED
	10	0x0400	1024	RESERVED
	11	0x0800	2048	RESERVED
	12	0x1000	4096	RESERVED (deprecated)
	13	0x2000	8192	Use HTTP/S or SMB. Ensure that this is set if Nomad integration is used by Tachyon. HTTP/S is automatically used if CM client is detected. **Note** Prior to 1E Client 4.1 (Nomad 7.0) this was disabled (0) by default, now it is enabled (1) by default. This setting should be enabled in baseline or other policies.

Installer property	Description			
	14	0x4000	16384	Web LSZ generation: enables the Nomad client on Configuration Manager standalone DPs to handle LSZ file generation requests coming from HTTP/HTTPS enabled clients. Used when Nomad clients are configured with either of the following enabled: • Bit13 (0x2000) – Use HTTP/S or SMB • Bit 15 (0x8000) – Use HTTP/S only, not SMB When enabled, the Nomad distribution point client creates a virtual folder called *LSZFILES*. The permissions for this are copied from the Configuration Manager *SMS_DP_SMSPKGX$* share. By default, access to the LSZFILES folder requires SSL to be enabled. This is the case for Internet facing scenarios where local client access certificates will ensure authentication. If you are using HTTP instead of HTTPS, manually disable SSL on the LSZFILES web folder in order for the Nomad LSZ file generation process to work. Only needs to be enabled when using HTTP or HTTPS on standalone DPs; it is not required on site server DPs because Nomad automatically configures Web LSZ generation on them.
	15	0x8000	32768	Use HTTP/S only, not SMB: enables the Nomad client to download content using HTTPS or HTTP depending on the content location provided by Configuration Manager or Tachyon. The Nomad client will not use SMB to download content when this is enabled.
MODULE.NOMAD.SSDENABLED	Enables Single Site Download (SSD). The installer property must be set to sum of the integer values for the required bits. For example, the following will turn the complete SSD functionality on.			

Installer property	Description

```
> msiexec /i 1E.Client-x64.msi MODULE.NOMAD.SSDENABLED=3 [other properties] /qn
```

Click here to expand...

Enables Single Site Download (SSD).

Registry value	Default value	Notes
SSDEnabled	0	You can set more than one option at the same time by combining the bit values. For example, to enable clients to fetch downloads using SSD and provide them to peers, set the value to 3 (decimal value 1+2 or 0x3). To enable clients to fetch downloads using site and local SSD and provide them to peers, set the value to 7. To enable SSD when you install Nomad, you must specify the MODULE.NOMAD.SSDENABLED installer property and ensure the Tachyon client is enabled by specifying SWITCH and BACKGROUNDCHANNELURL installer properties. If MODULE.NOMAD.SSDENABLED is specified during installation, the registry value of ContentRegistration is automatically set to 1. If you want to enable SSD as a provider after installation, then you also need to configure the registry values for SSDEnabled and ContentRegistration, in addition to enabling the Tachyon client. The ContentDistribution registry setting is found under the Platform key. • Nomad app provides visibility of content distribution activity • Single Site Download (SSD) • Single Site Peer Backup Assistant (SSPBA) • High Availability Peer Backup Assistant (HAPBA)

Installer property	Description

- Get Migration Settings task sequence action used to manage computer associations
- Nomad Pre-caching
- Nomad Download Pause.

In legacy versions of Nomad, Platform features were provided using ActiveEfficiency. This required the PlatformURL setting to be configured. This is no longer required. You will see that the PlatformURL registry is used, but this is configured automatically by Nomad on startup by querying the value that the Tachyon client is using (stored in the 1EClient.conf file).

If your network is running over a WLAN or have devices on a wireless network you want to be content providers, set ContentProviderOnWifi=1.

Bit	Hex	Decimal	Description
	0x0	0	SSD is disabled, the Nomad client takes no part in the SSD on the site.
0	0x1	1	SSD is enabled and the Nomad client fetches downloads using SSD. This setting on its own (without provider mode set) should be used with sensitive server weighting. Provider mode is where a peer gets content from another peer but cannot serve it (it cannot act as a master).
1	0x2	2	SSD is enabled and the Nomad client provides downloads to peers. Enabling this bit causes Nomad to register content with Content Distribution. In practice, this is unlikely to be used on its own. This is automatically disabled for WinPE installations (because cached content is only temporary).

Installer property	Description		
	2	0x4	4

Local SSD is enabled and the Nomad client fetches downloads from a local client (also known as a subnet peer master - the term used for local devices which have content but cannot be located during the normal election process because network broadcasts have been disabled) within the subnet.

The local SSD feature was introduced to supplement site SSD for clients on networks such as wireless where broadcasts are disabled, to prevent each client becoming its own master and downloading direct from the DP. In a SSD enabled environment, a master queries Content Distribution to get a list of devices on other subnets within the site that have content. With local SSD enabled, the master also queries for devices having content within local subnet. If any local peers with content are available, then the master downloads from them, otherwise it attempts to download from Site peers (other subnets in the site), and if the master still cannot find any peers, it downloads the content direct from the DP.

In version 7.0 and later, a master skips using local SSD if it sees broadcast messages from peers. This means clients in mixed network environments can be configured with the same SSDEnabled setting (with Local SSD enabled) and clients can move seamlessly between networks. When on a wireless network (where broadcasts are typically disabled) local SSD can be used. On LAN networks (where broadcasts are typically allowed) local SSD would be skipped because a master is elected and sees broadcast activity from peers.

This setting should only be used if networks have broadcasts being disabled (for example wireless networks) and clients are forced to download from the DP as they can't participate in an election.

Local SSD requires that a peer on the local subnet be configured to provide downloads to peers, that is at least one client on the subnet must be configured with Bit 1 enabled. To maintain consistency with typical

Installer property	Description
	Nomad peer sharing behavior where local SSD is not required, configure all clients with *SSDEnabled=7*. You'll also want to set ContentProviderOnWifi=1. When enabled, the elected master: 1. Queries Content Distribution to get a list of local devices having the content. 2. Queries each of those devices to check if they are available and have the content. The list is ordered by percentage of content the device holds. 3. Repeats the same process for devices on other subnets (existing SSD feature). 4. Stores a list of subnets as well as site devices in memory. 5. Cycles through the list in the following order: a. Subnet peer master (fetched from list of local devices from Content Distribution) b. Site master c. DP. To distinguish between a master derived from Content Distribution and an election, the log records: *Connection::SetDownloadSource = SubnetPeer* (an elected peer) instead of *Connection::SetDownloadSource = Peer* (an SSD peer master).
MODULE.NOMAD.SSPBAENABLED	Enables the use of Single Site functionality for PBA data stores. See Single Site peer backup assistant for more details. Click here to expand... Enables the use of Single Site functionality for PBA data stores. See Single Site peer backup assistant for more details.

Installer property	Description

Registry value	Default value	Notes
SSPBAEnabled	0	Has a dependency on the Tachyon Platform PlatformURL. Values are: • 0 – disables single-site integration with ContentDistribution • 1 – enables single-site integration with ContentDistribution

MODULE.NOMAD.STATUSMSGEVENTS

Determines which Nomad events are reported using Configuration Manager status messages.

Click here to expand...

Determines which Nomad events are reported using Configuration Manager status messages.

Registry value	Default value	Notes
StatusMsgEvents	0x0	Nomad can send status messages through Configuration Manager based on specific download events which appear in its deployment status. They are provided mainly for advanced troubleshooting purposes, or for custom reporting solutions. From v7.1 onwards, they are no longer required for the Nomad Dashboard which now gets its status events directly via the Platform Content Distribution feature. However, you may have custom reporting in Configuration Manger that also use these messages, and you can configure this setting accordingly for this purpose. These messages are controlled by the StatusMsgEvents registry value. This is a *REG_SZ* string data type and the format of the parameter

Installer property	Description

must be a 64-bit value. Status messages are only sent when there is an active deployment.

> **Warning**
>
> Status message events should be used with caution as they could impact your Configuration Manager environment when scaled up to tens of thousands of machines.

For example, to set the request started, request completed, started copy and master changed events, update the StatusMsgEvents registry value to *0x80002060*.

- 0x0000000001 – SNO_EVT_START
- 0x0000000002 – SNO_EVT_STOP
- 0x0000000004 – SNO_EVT_ERROR
- 0x0000000008 – SNO_EVT_PAUSED
- 0x0000000010 – SNO_EVT_RESUMED
- 0x0000000020 – SNO_EVT_REQUEST_STARTED
- 0x0000000040 – SNO_EVT_REQUEST_COMPLETED
- 0x0000000080 – SNO_EVT_SERVICE_RESET
- 0x0000000100 – SNO_EVT_STARTED_CACHE_MANAGEMENT
- 0x0000000200 – SNO_EVT_FINISHED_CACHE_MANAGEMENT
- 0x0000000400 – SNO_EVT_STARTED_HASHCHECK

Installer property	Description
	• 0x0000000800 – SNO_EVT_FINISHED_HASHCHECK • 0x0000001000 – SNO_EVT_ELECTION_REQUEST • 0x0000002000 – SNO_EVT_MASTER_CHANGED • 0x0000004000 – SNO_EVT_FILLIN_MASTER_CHANGED • 0x0000008000 – SNO_EVT_MCAST_CENTRALSCHED • 0x0000010000 – SNO_EVT_MCAST_ERROR • 0x0000020000 – SNO_EVT_MCAST_COMPLETE • 0x0000040000 – SNO_EVT_SCHEDULER • 0x0000080000 – SNO_EVT_STARTED_TX_CENTRALMCAST • 0x0000100000 – SNO_EVT_STOPPED_TX_CENTRALMCAST • 0x0000200000 – SNO_EVT_STARTED_TX_ACTIVEMCAST • 0x0000400000 – SNO_EVT_STOPPED_TX_ACTIVEMCAST • 0x0000800000 – SNO_EVT_STARTED_TX_FILLINMCAST • 0x0001000000 – SNO_EVT_STOPPED_TX_FILLINMCAST • 0x0002000000 – SNO_EVT_STARTED_RX_CENTRALMCAST

Installer property	Description

- 0x0004000000 – SNO_EVT_STOPPED_RX_CENTRALMCAST
- 0x0008000000 – SNO_EVT_STARTED_RX_ACTIVEMCAST
- 0x0010000000 – SNO_EVT_STOPPED_RX_ACTIVEMCAST
- 0x0020000000 – SNO_EVT_STARTED_RX_FILLINMCAST
- 0x0040000000 – SNO_EVT_STOPPED_RX_FILLINMCAST
- 0x0080000000 – SNO_EVT_STARTED_COPY
- 0x0100000000 – SNO_EVT_STOPPED_COPY
- 0x0200000000 – SNO_EVT_WORKRATE_CHANGED
- 0x0400000000 – SNO_EVT_WRONG_PKG_VERSION
- 0x0800000000 – SNO_EVT_INFORMATIONAL
- 0x1000000000 – SNO_EVT_FINALSTATS (see notes below)
- 0x2000000000 – SNO_EVT_WAIT
- 0x4000000000 – SNO_EVT_MAX_EVENTID

SNO_EVT_FINALSTATS notes

For success reporting, this message provides feedback on the status of the download. For example, it can show how much data was received using multicast as opposed to peer-to-peer copying. Turning this message on creates an

Installer property	Description

extra status message per machine for each deployment. The format of the status message is:

```
Evt_FinalStats MD100067 1 170 59195038 1
70 59195038 0 59195038 0 0
```

Configuration Manager status messages are made up of insertion strings. The strings for the final stats event are:

InstrStr0	Nomad event string (internal reference)	N/A
InstrStr1	Package Id and Package version	MD100067 1
InstrStr2	Total number of files in package	170
InstrStr3	Total number of package bytes	59195038
InstrStr4	Number of files which are cached	170
InstrStr5	Bytes which are cached	59195038
InstrStr6	Bytes coped from a peer agent (P2P)	0
InstrStr7	Bytes copied from the DP	59195038
InstrStr8	Bytes received via local multicast	0
InstrStr9	Bytes received from a central multicast	0

Installer property	Description
	If the package is already cached and is re-deployed with an unchanged package version, the final stats message will not be re-sent.
MODULE.NOMAD.SUCCESSCODES	A list of Nomad return codes that are translated as success to the Content Transfer Manager (CTM) component of the Configuration Manager client. Click here to expand... A list of Nomad return codes that are translated as success to the Content Transfer Manager (CTM) component of the Configuration Manager client. **Registry value:** SuccessCodes **Default:** 0x206b, 0x2077, 0x103, 0xffffffff, 0x1, 0x70, 0x2050, 0x2051, 0x2052, 0x2053, 0x2054,0x2055, 0x2056, 0x2057, 0x2058, 0x205a, 0x205b, 0x205c, 0x205d, 0x205e, 0x2060, 0x2061,0x2062, 0x2063, 0x2064, 0x2065, 0x2066, 0x2067, 0x2068, **Notes:** This REG_SZ value contains a comma-delimited list of possible Nomad return codes that should be treated as a success and thereby prevent Configuration Manager from attempting to download the content itself or use another Alternate Content Provider (ACP). Any code returned by Nomad that is not on the list will be treated as a failure and trigger the Configuration Manager client to attempt to download the content using alternate means. Nomad also sends a status message to the Configuration Manager site containing its return code. Strictly speaking the Nomad return codes are actually internal status codes, Nomad will only ever return success or failure to the Content Transfer Manager (CTM) component of the Configuration Manager client. When CTM receives a success it passes control to the ExecMgr component of the Configuration Manager client, which attempts to execute the deployment. ExecMgr will fail if Nomad did not download the content and make it available in the Configuration Manager cache. In this case, ExecMgr sends a status message

Installer property	Description		
		0x2069, 0x209A	(e.g. failed deployment) back to the Configuration Manager site. If Nomad generates a return code that is not in the list, it passes a fail to the CTM component which causes the Configuration Manager client to try downloading the content itself using BITS, or use another Alternate Content Provider (ACP). This process may itself succeed or fail depending on the conditions that resulted in the original Nomad return code, and may have an undesirable impact on the network. **Note** The special code 0x9999 can be added to the list, or used on its own, to cause Nomad to always return a success to CTM. As a consequence this code is also known as "prevent failover to BITS". **Note** The SuccessCodes list need not be modified under normal circumstances, other than to add or remove the 0x9999 code. The following table shows the possible Nomad return codes that can be set in the list: **Note** This list is subject to change with each release of Nomad, and provided for reference only.

Installer property	Description

Return Code	Description	
-1	0xFFFFFFFF	Reserved.
1	0x0001	Reserved.
112	0x0070	Insufficient disk space to create the cache.
259	0x0103	Reserved.
8272	0x2050	The download has been suspended by APM.
8273	0x2051	The user has cancelled this download.
8274	0x2052	Invalid command line.
8275	0x2053	Command-line execution failure.
8276	0x2054	Internal Error.
8277	0x2055	The package exceeds the threshold for a RAS connection.
8278	0x2056	The package exceeds the threshold for a Slow LAN connection.

Installer property	Description			
		8279	0x2057	The package exceeds the threshold for a Fast LAN connection.
		8280	0x2058	Reserved.
		8281	0x2059	Unknown transport. Returned when an attempt is made to download a Software Update from an Internet location (like Microsoft Updates).
		8282	0x205A	Invalid special package path (set using --pp).
		8283	0x205B	Incorrect file hash.
		8284	0x205C	Exited due to a kill request.
		8285	0x205D	DP path not found.
		8286	0x205E	The MaxBusyBackOff consecutive event threshold has been exceeded.
		8287	0x205F	The service has stopped.
		8288	0x2060	The advertisement has expired.
		8289	0x2061	Reserved.

Installer property	Description			
		8290	0x2062	This is an unlicensed version of Nomad.
		8291	0x2063	Invalid alternate cache path (set using --cp).
		8292	0x2064	No Configuration Manager job data found in WMI.
		8293	0x2065	Incorrect package hash.
		8294	0x2066	MaxDuration or execution runtime for this program has been exceeded.
		8295	0x2067	Reserved.
		8296	0x2068	Incorrect package version.
		8297	0x2069	Obsolete package version.
		8298	0x206A	The BlockSize has been changed during download.
		8299	0x206B	The "no progress" re-check threshold has been exceeded.
		8300	0x206C	The parent process has terminated.

Installer property	Description			
		8301	0x206D	Duplicate download for the package.
		8302	0x206E	The service was reset. This will occur if certain configuration parameters are changed during a download e.g. NomadInhibitedSubnets
		8303	0x206F	Nomad inhibited.
		8311	0x2077	Internal error LST incomplete.
		8346	0x209A	Client certificate missing. Nomad is configured to use certificate-based client authentication but was unable to find an appropriate certificate.
MODULE.NOMAD.SUPPORTWPAD	Provides support for Web Proxy Auto-Discovery Protocol (WPAD). Click here to expand... Provides support for Web Proxy Auto-Discovery Protocol (WPAD). Nomad always uses System level proxy if it has been set, irrespective of what SupportWPAD has been set to. SupportWPAD was introduced in v7.1 and when disabled it does not change the default behavior, which is: If system level proxy is set then use it, otherwise access directly without proxy. When SupportWPAD is enabled in Nomad, the behavior is:			

Installer property	Description

- If system level proxy is set then use it and do not try WPAD
- If system level proxy is not set then fetch automatic proxy using WPAD and use it
- If system level proxy is not set and failed to get automatic proxy using WPAD then try access directly without proxy.

How to know if a system level proxy has been set

```
netsh winhttp show proxy
```

Registry value	Default value	Notes
SupportWPAD	0	By default, the WPAD feature is disabled. To enable WPAD in Nomad, add registry key 'SupportWPAD' and set it to 1 at registry path HKLM/Software/1E/NomadBranch To enable or disable the WPAD feature in Nomad: • Disable WPAD set SupportWPAD = 0 • Enable WPAD set SupportWPAD= 1 (or non-zero value).

MODULE.NOMAD.USEFIPS

This installer property sets the Nomad EncryptionType registry entry.

Determines the type of encryption used by Nomad to encrypt its communications between Nomad peers.

Click here to expand...

Determines the type of encryption used by Nomad to encrypt its communications between Nomad peers.

Registry value	Default value	Notes
EncryptionType	0x0 (0)	Value are: • 0 – standard Nomad encryption • 1 – FIPS encryption

Installer property	Description
MODULE.NOMAD.WAKEUPBATCHSIZE	The maximum number of machines to wake up in a single call. Click here to expand... The maximum number of machines to wake up in a single call. **Warning** Nomad integration with WakeUp enables Nomad to share content from its devices that are holding particular content, even if those devices are offline. One reason why peers in the local subnet may not respond to the request even though they have content in their caches is that they are offline (shutdown, in hibernate or sleep mode). However, if WakeUp is integrated, the Nomad client would know which offline device has the content and can wake it up when it queried Content Distribution. The wake-up list is maintained by Content Distribution and is the same list that Single Site Download (SSD) uses. Separate lists of peers are returned for the subnet and site. This feature requires Nomad SSD to be enabled, Content Distribution, and a NightWatchman infrastructure. The feature is enabled during the installation of the NightWatchman Management Center. Please refer toIntroducing Nomad for requirements.

Registry value	Default value	Notes
WakeUpBatchSize	10	Sets the maximum number of machines to wake up in one call, for subnet and site separately. (So up to twice this number of requests is sent in total if WakeUp is enabled for both subnet and site.) The next batch is launched, if necessary, after a re-election (usually a periodic election). The value cannot be greater than MaxDevicesFromAE, and hence itself cannot be more than 20.

MODULE.NOMAD.WAKEUPENABLED	Enables WakeUp integration, see Integrating Nomad with WakeUp for more details.

Installer property	Description

Click here to expand...

Enables WakeUp integration, see Integrating Nomad with WakeUp for more details.

Warning

Nomad integration with WakeUp enables Nomad to share content from its devices that are holding particular content, even if those devices are offline. One reason why peers in the local subnet may not respond to the request even though they have content in their caches is that they are offline (shutdown, in hibernate or sleep mode). However, if WakeUp is integrated, the Nomad client would know which offline device has the content and can wake it up when it queried Content Distribution.

The wake-up list is maintained by Content Distribution and is the same list that Single Site Download (SSD) uses. Separate lists of peers are returned for the subnet and site. This feature requires Nomad SSD to be enabled, Content Distribution, and a NightWatchman infrastructure. The feature is enabled during the installation of the NightWatchman Management Center. Please refer toIntroducing Nomad for requirements.

Registry value	Default value	Notes
WakeUpEnabled	0	Determines the status of the WakeUp integration. If configured by the installer, it is disabled (0) by default. If integration is enabled, Nomad attempts to wake up dormant hosts that are known to have the requested content in their caches. The integration has a dependency on the PlatformURL. To enable integration post-installation, for normal usage, set both bits 0 and 1 (0x3)

Bit	Hex	Decimal	Description
	0x0	0	Disables WakeUp integration.

Installer property	Description			
	0	0x1	1	Enables WakeUp integration only for the local subnet.
	1	0x2	2	Enables WakeUp integration only for the site.
		0x3	3	Enables WakeUp integration for the site and the local subnet.

MODULE.NOMAD.WAKEUPMINPACKAGESIZEMB

The minimum size of content (in megabytes) that will cause a request for a wakeup. See Integrating Nomad with WakeUp for more details.

Click here to expand...

The minimum size of content (in megabytes) that will cause a request for a wakeup. See Integrating Nomad with WakeUp for more details.

Warning

Nomad integration with WakeUp enables Nomad to share content from its devices that are holding particular content, even if those devices are offline. One reason why peers in the local subnet may not respond to the request even though they have content in their caches is that they are offline (shutdown, in hibernate or sleep mode). However, if WakeUp is integrated, the Nomad client would know which offline device has the content and can wake it up when it queried Content Distribution.

The wake-up list is maintained by Content Distribution and is the same list that Single Site Download (SSD) uses. Separate lists of peers are returned for the subnet and site. This feature requires Nomad SSD to be enabled, Content Distribution, and a NightWatchman infrastructure. The feature is enabled during the installation of the NightWatchman Management Center. Please refer toIntroducing Nomad for requirements.

Registry value	Default value	Notes
WakeUpMinPackageSizeMB	1024	Any content below this size is downloaded from the DP as downloads from the DP for files this size will likely complete before any wakeups will have had a chance to finish. The value can be 0, in which

Installer property	Description
	case wakeups will always be attempted. For example, if it is set to 512 and size of the content downloaded is 500 MB, a wake-up request (to site or subnet) is not be sent. Similarly, if size of the content is 600 MB, then wake-up requests (to site and subnet, determined by WakeupEnabled) is be sent. **Note** For standalone downloads (using SMSNomad.exe) and under WinPE, there has no effect as the size of the content cannot easily be determined. Wake-up requests are always sent in these instances.
MODULE.NOMAD.WLANBLIPSECS	The duration for temporarily disabling a wireless connection when a wired LAN connection becomes available, to provide time for the OS and Nomad to switch to the LAN connection. This is useful for OS versions and drivers that do not automatically switch to a preferred wired connection. Click here to expand... The duration for temporarily disabling a wireless connection when a wired LAN connection becomes available, to provide time for the OS and Nomad to switch to the LAN connection. This is useful for OS versions and drivers that do not automatically switch to a preferred wired connection. Registry value: WLanBlipSecs Default value: 0 Notes: The value must be 20 seconds or more. Nomad provides extra stability by managing a machine's network connections as they move between a wireless and a wired LAN. Depending on the OS version or other factors, once an SMB or HTTP session is running on a wireless connection, it will remain on wireless even when a wired LAN becomes available. Nomad uses **WLanBlipSecs** to temporarily drop a wireless connection

Installer property	Description

	when it detects a wired LAN connection, to give time for the OS and Nomad to automatically switch to the LAN connection.
	
	For example, if a Nomad master was initiated when a machine was on a wireless connection and a wired connection subsequently became available, Nomad disables the wireless adapter for a long enough period to enable a switchover to the wired connection. As a result of this, the IP address and the share path will change and peers will log error messages until each peer re-establishes its connection to the master and the new share location.
	
	This feature is turned off by default.
	
	Note
	Other applications may be affected when switching from wireless to wired connection.
	
	Irrespective of the **WLanBlipSecs** setting, you can also control which service set identifier (SSID) Nomad connects to by managing a list. To do this, update the NomadBranch WLanProfileList registry value with a comma-delimited list of SSIDs or use the wildcard (*) character for any SSID.
	
	Examples:
	
	`WLanProfileList REG_SZ WIFIGAP,GUEST`
	`WLanProfileList REG_SZ *`

MODULE.NOMAD.WLANPROFILELIST	A list of wireless SSIDs to enable switching from wireless to wired LAN connections. Click here to expand... A list of wireless SSIDs to enable switching from wireless to wired LAN connections. Registry value: WLanProfileList Default value: Notes: A comma-delimited list of wireless SSIDs (* for any all) which enables Nomad to switch form wireless to a wired LAN connection when it becomes available.

2.6.1.8 PXE Everywhere Agent settings

Installer and configuration settings for the PXE Everywhere Agent client module of the 1E Client supported only on Windows computers.

1E Client is available as 32-bit and 64-bit versions, and the correct version must be installed. This means the PXE Everywhere Agent registry location is the same for x86 and x64:

- *HKEY_LOCAL_MACHINE\SOFTWARE\1E\PXEEverywhere*

Note

Registry settings:

AlwaysBootImageId | AlwaysIsMandatory | BindTo | CommsPort | ConfigServerAddress | Debug | DefaultBlockSize | DhcpPort | ElectionWaitSecs | ElectionWeight | EncryptionType | Flags | IgnoreGatewayAddress | IgnoreWireless | LogFileName | LogFormat | MaxBlockSize | MaxLogFilesize | Mode | ReserveSecs | SessionTimeoutSecs | TftpRoot

Note

Installer properties:

Module.PXEEverywhere.Enabled | MODULE.PXEEVERYWHERE.COMMSPORT | MODULE.PXEEVERYWHERE.CONFIGSERVERURL | MODULE.PXEEVERYWHERE.DEBUG | MODULE.PXEEVERYWHERE.DHCPPORT | MODULE.PXEEVERYWHERE.ELECTIONWAITSECS | MODULE.PXEEVERYWHERE.ELECTIONWEIGHT | MODULE.PXEEVERYWHERE.USEFIPS | MODULE.PXEEVERYWHERE.LOGPATH | MODULE.PXEEVERYWHERE.LOGFORMAT | MODULE.PXEEVERYWHERE.MAXLOGFILESIZE | MODULE.PXEEVERYWHERE.MODE | MODULE.PXEEVERYWHERE.RESERVESECS | MODULE.PXEEVERYWHERE.TFTPROOT

Note

Configuration file settings:

Module.PXEEverywhere.Enabled

1E Client installers include a **template configuration file** that contains the more important settings with default values that match hard-coded default values. The configuration file is updated during installation and named **1E.Client.conf** in the installation folder along with the 1E Client executable.

After installation, configuration file settings can be managed using 1E Client command-line parameters, Explorer configuration instructions, Guaranteed State policies, Configuration Manager baselines or other means. Registry settings can also be managed by Windows Group Policy.

2.6.1.8.1 PXE Everywhere Agent installation settings

This table lists the configuration settings visible in the PXE Everywhere screen during an interactive installation of the 1E Client. Other installer properties are available when using a command-line installation or a transform.

Note

You must use UPPERCASE when specifying the *name* of any installer property in a **mst** transform file, and preferably when including them in a msiexec command-line.

Names of settings stored in the configuration file are not case-sensitive. Setting names stored in the registry may be case-sensitive and should be specified as shown.

Settings that have numeric values must be set using decimal integers, unless otherwise specified.

Installer property	Mandatory	Default value	Description
Module.PXEEverywhere.Enabled	No	false	Set this property to **true** to enable the PXE Everywhere Agent client module. The default value is false. **Note** If enabled, when the 1E Client starts it will attempt to automatically remove any previous installations of PXE Everywhere Agent. This setting does not have an associated registry entry and is stored in the 1E Client configuration file.
MODULE.PXEEVERYWHERE.CONFIGSERVERURL	Yes	http://SERVER/PXELite/PXELiteConfiguration.asmx	URL for the PXE Everywhere Central web service in the format: *http://SERVER/PXELite/PXELiteConfiguration.asmx* where *<SERVER>* is the name of the server (or FQDN) where the PXE Everywhere Central web service is installed. **Note** The http prefix to the URL is case-sensitive and must be entered in all lower case letters.

Installer property	Mandatory	Default value	Description
			The URL is not verified by the installer, so you will need to ensure that the correct URL is entered. This setting has an associated ConfigServerAddress registry value.
MODULE.PXEEVERYWHERE.USEFIPS	No	0	You must use the same FIPS encryption setting on all PXE Everywhere Agents. Use of FIPS compliant encryption for communications. • 0 – use default encryption • 1 – use FIPS encryption This setting has an associated EncryptionType registry value.
MODULE.PXEEVERYWHERE.DHCPPORT	No	67	This installer property is set to 2067 if **Enable DHCP Snooping support** is checked during an interactive installation of the 1E Client installer. This is the UDP port on which the PXE Everywhere Agent will listen for PXE requests. If DHCP Snooping is not being used, then this port must be 67 (default), and you do not need to install Responders. When manually installing the PXE Everywhere Agent, if the

Installer property	Mandatory	Default value	Description
			DHCP Snooping option is enabled in the installer UI, the default port is changed from 67 (43 hex) to 2067 (813 hex). If the MODULE.PXEEVERYWHERE.DHCPPORT installer property is used to specify a port other than 67, the installer UI assumes the DHCP Snooping option is enabled. If DHCP Snooping is being used, then DhcpPort on Agents must be the same value as AltPxeServerPort on Responders. The default value of AltPxeServerPort is 2067. If a value other than 2067 is specified as a custom port number on Agents, you will also need to manually create the AltPxeServerPort (and AltPxeClientPort) registry values on Responders. This setting has an associated DhcpPort registry value.

2.6.1.8.2 PXE Everywhere Agent registry settings

This table lists all registry setting and their associated installer properties.

Note

You must use UPPERCASE when specifying the *name* of any installer property in a **mst** transform file, and preferably when including them in a msiexec command-line.

Names of settings stored in the configuration file are not case-sensitive. Setting names stored in the registry may be case-sensitive and should be specified as shown.

Settings that have numeric values must be set using decimal integers, unless otherwise specified.

Registry name	Registry type	Installer property	Mandatory	Default value	Description
AlwaysBootImageId	REG_SZ	This value does not have an installer property.	No	Registry value is not created.	A string value containing a valid package id of a boot image. If specified, do not get boot image ID from PXE Everywhere Central but use this one instead.
AlwaysIsMandatory	REG_DWORD	This value does not have an installer property.	No	Registry value is not created.	Whether the boot image is mandatory (value 1) or not (0). Only relevant in combination with *AlwaysBootImageId*.
BindTo	REG_SZ	This value does not have an installer property.	No	Registry value is not created.	Comma-separated list of IP addresses which PXE Everywhere Agent listens for DHCP (PXE) and TFTP requests. If not present, PXE Everywhere Local listens on all IP addresses. Use this if there is more than one network interface.
CommsPort	REG_DWORD	**MODULE.PXEEVERYWHERE.COMMSPORT**	No	2012	Used for UDP election broadcast messages, this must be opened in the Windows firewall.
ConfigServerAddress	REG_SZ	**MODULE.PXEEVERYWHERE.CONFIGSERVERURL**	Yes	http://SERVER/PXELite/PXELiteConfiguration.asmx	URL for the PXE Everywhere Central web service in the format: *http://SERVER/PXELi*

Registry name	Registry type	Installer property	Mandatory	Default value	Description
					te/PXELiteConfiguration.asmx where *<SERVER>* is the name of the server (or FQDN) where the PXE Everywhere Central web service is installed. **Note** The http prefix to the URL is case-sensitive and must be entered in all lower case letters. The URL is not verified by the installer, so you will need to ensure that the correct URL is entered.
Debug	REG_DWORD	**MODULE.PXEEVERYWHERE.DEBUG**	No	1	The debug level. Leave this at *1* unless 1E Support recommends a change. The range is: • *0x1*: Basic logging • *0x4*: Extra "application-specific" logging

Registry name	Registry type	Installer property	Mandatory	Default value	Description
					• *0x8*: Extra registry logging • *0x10*: Increased general logging The following two bits will perform centralized logging via SOAP calls to the PXE Central Server: • *0x1000*: Logs election results • *0x2000*: Logs TFTP file transfer start and stop (includes statistics).
DefaultBlockSize	REG_DWORD	This value does not have an installer property.	No	Registry value is not created.	Default TFTP block size. 512 if not specified.
DhcpPort	REG_DWORD	**MODULE.PXEEVERYWHERE.DHCPPORT**	No	67	This is the UDP port on which the PXE Everywhere Agent will listen for PXE requests. If DHCP Snooping is not being used, then this port must be 67 (default), and you do not need to install Responders. When manually installing the PXE Everywhere Agent, if the DHCP Snooping

Registry name	Registry type	Installer property	Mandatory	Default value	Description
					option is enabled in the installer UI, the default port is changed from 67 (43 hex) to 2067 (813 hex). If the MODULE.PXEEVERYWHERE.DHCPPORT installer property is used to specify a port other than 67, the installer UI assumes the DHCP Snooping option is enabled. If DHCP Snooping is being used, then DhcpPort on Agents must be the same value as AltPxeServerPort on Responders. The default value of AltPxeServerPort is 2067. If a value other than 2067 is specified as a custom port number on Agents, you will also need to manually create the AltPxeServerPort (and AltPxeClientPort) registry values on Responders.
ElectionWaitSecs	REG_DWORD	**MODULE.PXEEVERYWHERE.ELECTIONWAITSECS**	No	1	Time (in seconds) to wait for responses to the election request before broadcasting the result. Can be any positive integer value above 0.

Registry name	Registry type	Installer property	Mandatory	Default value	Description
Election Weight	REG_DWORD	**MODULE.PXEEVERYWHERE.ELECTIONWEIGHT**	No	50	When set, this manually created registry value determines the likelihood of the machine winning elections, all else being equal. The value must be between 0 and 99 inclusive. The higher the value the the higher the likelihood of winning. If no value is set, a default of 50 is used.
EncryptionType	REG_DWORD	**MODULE.PXEEVERYWHERE.USEFIPS**	No	0	You must use the same FIPS encryption setting on all PXE Everywhere Agents.Use of FIPS compliant encryption for communications. • 0 – use default encryption • 1 – use FIPS encryption
Flags	REG_DWORD	This value does not have an installer property.	No	Registry value is not created.	If set to ***1*** the DHCP listener adds an ASCII terminator character to the bootfile name in the DHCP acknowledgment message. Some HP machines require this.

Registry name	Registry type	Installer property	Mandatory	Default value	Description
					Any value other than **1** is treated as default 0.acknowledgment
IgnoreGatewayAddress	REG_DWORD	This value does not have an installer property.	No	Registry value is not created.	If set to any value other than ***0*** the DHCP listener ignores the gateway address. If not set then assumes default ***0*** .
IgnoreWireless	REG_DWORD	This value does not have an installer property.	No	0	If set to **1** then PXE Everywhere Agent does not bind on wireless adapters. Any value other than 1 is treated as default 0.
LogFileName	REG_SZ	**MODULE.PXEEVERYWHERE.LOGPATH** **Note** This property only specifies the location of the log file.	No	%ALLUSERSPROFILE%\1E\PXEEverywhere PXEEverywhere.log	The location of the PXE Everywhere log file. The path is created if it does not exist. The logfile name is *PXEEverywhere.log*
LogFormat	REG_DWORD	**MODULE.PXEEVERYWHERE.LOGFORMAT**	No	1	Formatting depends on which bits are set: • bit *0 (0x01)* use Configuration Manager-

Registry name	Registry type	Installer property	Mandatory	Default value	Description
					compatible format (default) • bit *3 (0x08)* do no formatting • bit *7 (0x80)* include milliseconds in the timestamp
MaxBlockSize	REG_DWORD	**Note** This value does not have an installer property, but is configurable when deployed using 1E Client Deployment Assistant. Please refer to Installing PXE Everywhere Agents: Preparing a Configuration Manager Application for PXE Everywhere Agent using the	No	Registry value is not created.	Maximum value for the block size (in bytes). PXE Everywhere uses the system MTU to derive the size of TFTP packets. May require limiting when using VPN tunnels. In most cases, this value should not be altered. Default is 8192 (8 kbytes). **Note** The actual block size used for the TFTP protocol is the lesser value of the **tftpBlockSize** and the **MaxBlockSize** registry values. The **tftpBlockSize** value is specified in the

Registry name	Registry type	Installer property	Mandatory	Default value	Description
		1E Client Deployment Assistant.			**CreateBCD.exe** utility command-line, and does not have a registry entry or installer property.
MaxLogFilesize	REG_DWORD	**MODULE.PXEEVERYWHERE.MAXLOGFILESIZE**	No	10485760	Maximum size for the log file in bytes. Once the file reaches the specified size, a copy is made with a *.lo_* extension in the same directory. A new log file will then be created. Default is 10485760 (10 MBytes).
Mode	REG_DWORD	**MODULE.PXEEVERYWHERE.MODE**	No	2	Mode must be one of the following: • 0 – no elections • 1 – the election instigator becomes the master (only to be used for testing) • 2 – with elections (default)
ReserveSecs	REG_DWORD	**MODULE.PXEEVERYWHERE.RESERVESECS**	No	60	Time (in seconds) an election result remains active. 60 if not specified or 0 is

Registry name	Registry type	Installer property	Mandatory	Default value	Description
					specified. Can be any positive integer value.
SessionTimeoutSecs	REG_DWORD	This value does not have an installer property.	No	Registry value is not created.	Timeout for the TFTP listener. 600 if not specified or 0 is specified. Can be any positive integer value.
TftpRoot	REG_SZ	**MODULE.PXEEVERYWHERE.TFTPROOT**	No	*%ALLUSERSPROFILE%\1E\PXEEverywhere\TftpRoot*	Location for the PXE Everywhere Agent *TFTPROOT* directory. If you change the location of *TFTPROOT*, you need to change the location that you copy the additional PXE boot files to.

2.6.1.9 Shopping client settings

Installer properties and configuration settings for the Shopping client module of the 1E Client supported only on Windows computers. This module supports users connecting to the Shopping Portal, and provides the Windows Servicing Assistant (WSA).

> **Note**
>
> Installer properties and Configuration file settings:
>
> Module.Shopping.Enabled | Module.Shopping.AlternativeUrls | Module.Shopping.FirefoxSupportEnabled | Module.Shopping.InitializationFailureSleepSecs | Module.Shopping.LocalhostUrl | Module.Shopping.LoopbackExemptionEnabled | Module.Shopping.OrderTrackingEnabled | Module.Shopping.ShoppingCentralUrl | Module.Shopping.SsoEnabled

Enabling the Shopping client module allows the Windows Servicing Assistant (WSA) feature to be used. There are no additional settings required to enable or configure the WSA feature.

Configuration file settings are the same as the installer properties. There are no registry settings. Configuration file settings can be managed using 1E Client command-line parameters, Explorer configuration instructions, Guaranteed State policies, Configuration Manager baselines or other means.

> **Note**

When the 1E Client starts, if the Shopping module is enabled the 1E Client will automatically remove any previous installation of the 1E Shopping Agent.

The Shopping client module is not supported on:

- Non-Windows devices
- Legacy OS (that is OS which Microsoft no longer support, including XP, Vista, Server 2008 etc.)

2.6.1.9.1 Shopping client settings

The table below lists the settings required to enable the Shopping client required for integration with Shopping v5.5 or later. The Shopping client module must be enabled on all Windows computers that will connect to the Shopping self-service portal.

Note

You must use UPPERCASE when specifying the *name* of any installer property in a **mst** transform file, and preferably when including them in a msiexec command-line.

Names of settings stored in the configuration file are not case-sensitive. Setting names stored in the registry may be case-sensitive and should be specified as shown.

Settings that have numeric values must be set using decimal integers, unless otherwise specified.

Shopping module setting	Installation default	Description
Module.Shopping.Enabled	false	Set the value to **true** to enable the Shopping module. The default value is **false**. Shopping must be enabled so that users of a computer can use the 1E Shopping self-service portal, the Windows Servicing Assistant, and the 1E Virtual Assistant. **Note** If enabled, when the 1E Client starts it will attempt to automatically remove any previous installations of the 1E Shopping Agent.
Module.Shopping.AlternativeUrls **Note**	(blank)	Optional. A list of URLs from which the Shopping module allows launching the WSA wizard. This setting is typically used to launch WSA from a ServiceNow application such as 1E Service Catalog Connect.

Shopping module setting	Installation default	Description
This setting is not in the template configuration file.		Multiple URLs should be separated by pipe characters. For example *https://dev123456.servicenow.com|https://dev987654.servicenow.com* The Shopping client requests this value from the Shopping Central website (admin console setting: AlternativeUrls). If the client fails to connect to the website, it defaults to using this setting and retries later.
Module.Shopping.FirefoxSupportEnabled **Note** This setting is not in the template configuration file.	(blank)	Optional. If this setting is not specified the value defaults to **false**. Set this value to **true** to enable support for the Firefox browser on HTTPS. If enabled, 1E Client Shopping module will create a CA certificate and a certificate with subject 'localhost' signed by the CA certificate and add those certificates to the Trusted Root Certification Authorities. This is required to allow launching the WSA wizard from third party websites like ServiceNow. The Shopping client requests this value from the Shopping Central website (admin console setting: Firefox support enabled). If the client fails to connect to the website, it defaults to using this local setting and retries later.
Module.Shopping.InitializationFailureSleepSecs **Note** This setting is not in the template configuration file.	30	This setting controls the time the client waits before attempting to connect to the website specified in Module.Shopping.ShoppingCentralUrl. If the client module fails to connect during startup, it does not initialize, and will retry at gradually increasing intervals until it is able to connect. Range is 10 to 900, default is 30. The log file may show this setting as InitializationRetryIntervalSecs.
Module.Shopping.LocalhostUrl **Note**	(blank)	Optional. The localhost URL used by the Shopping client module to listen for localhost API calls. For example: *https://localhost:8000/ShoppingClientAgent/MachineInfo*

Shopping module setting	Installation default	Description
This setting is not in the template configuration file.		The Shopping client sets the value of **LocalhostUrl** by calling a server API which returns the value of **1E Client loopback URL** setting in the Shopping Admin Console. However, if the device is in a workgroup, or **Module.Shopping.SsoEnabled** is set to true, or some other reason the API cannot be called, then **Module.Shopping.LocalhostUrl** must be set locally. If set locally, the local setting will override the server setting, and you must ensure it matches the value configured in the Shopping Admin Console. **LocalhostUrl** must be set to **https** if ShoppingCentralUrl is set to **https**, otherwise it can be **http** or **https**. ShoppingCentralUrl — LocalhostUrl http — http or https https — https When **LocalhostUrl** uses **https** the 1E Client Shopping client creates the following certificates on startup, and deletes them when shutting down: • a self-signed certificate issued to **1ECA** added to the machine's Trusted Root Certification Authorities (ROOT) store • a certificate issued by 1ECA issues to **localhost** added to the machine's Personal (MY) store. If using **https** and Firefox browsers are used, then Module.Shopping.FirefoxSupportEnabled must be set to **true**. Shopping client only allows inbound connections to **localhost (127.0.0.1)** which prevents remote access. See Information provided by the Shopping client below for details of localhost API calls.

Shopping module setting	Installation default	Description
Module.Shopping.LoopbackExemptionEnabled	false	Optional. Default value is **false**. Set this value to **true** if users are likely to use Microsoft Edge or other Metro browsers to access the Shopping website. The Shopping client requests this value from the Shopping Central website (admin console setting: Loopback exemption enabled). If the client fails to connect to the website, it defaults to using this local setting and retries later. When users connect to the Shopping Portal, the website needs to get the latest details about the local computer. Shopping may already have details from the Configuration Manager database, but these need to be confirmed and updated. Browser standards only allow websites to get limited information about the user and computer, therefore the website needs to make loopback calls to the local computer via the Shopping client. The following browsers permit loopback calls by default: • All versions of Chrome • All versions of Firefox • Non-Metro UI based Internet Explorer browsers (including legacy Internet Explorer) If your Shopping users are using **Edge** and **Metro Internet Explorer** browsers, you must enable a **Loopback Exemption** to allow these browsers to make loopback calls. Exemption affects the browser as a whole and is not just restricted to the Shopping website. Before enabling this option, check your corporate security policy and be aware of the implications of allowing access between browsers and the local machine. By enabling loopback, you are only setting the Edge/Metro Internet Explorer browsers to the same level of security as other browsers which allow this setting already. If you are running an unattended install, you can use **MODULE.SHOPPING.LOOPBACKEXEMPTIONENABLED** for all OS

Shopping module setting	Installation default	Description
		but it only works on Windows 8, 8.1, 10 and Windows Server 2012 R2 and later. Shopping client only allows inbound connections to **localhost (127.0.0.1)** which prevents remote access.
Module.Shopping.OrderTrackingEnabled **Note** This setting is not in the template configuration file. **Note** New in 1E Client 5.2 Accumulated Hotfix.	(blank)	Add this setting to the configuration file and set to false only if you want to override the Order Tracking feature enabled in the Shopping Admin Console, as described in Shopping Admin Console settings: Order Tracking Enabled. The Console setting, when set to true, globally enables the Order Tracking feature on all clients. You should only use this client setting to override the Console, to disable the feature on a subset of clients. **Tip** This client setting only affects the notification icon (and its popups), it does not affect Order Tracking emails, because they are controlled by the Shopping server. You can control which notifications and emails that users receive using the web administration settings described in Managing Order Tracking. **Note** When using Shopping 6.0, this setting is ignored, and the notification icon is not visible. When using Shopping 6.1 or later, this setting only applies if you have both of the following: • 1E Client 8.0 or 1E Client 5.2 **with the latest hotfix** • Tachyon integration enabled on the Shopping server - to support Shopping 6.1 features: Order Tracking and Tachyon instruction application.
Module.Shopping.ShoppingCentralUrl	(blank)	The URL that the Shopping client module uses to connect to the Shopping Central website.

Shopping module setting	Installation default	Description
		Example: *https://shopping.acme.local/Shopping* This is the URL of the Shopping Central website, comprising: • **scheme** - either http or https • **host header** - DNS Name FQDN - this is the host header configured for the Shopping website, which is normally a DNS Name FQDN • **port number** - you do not have to provide this if using default port 80 or 443 • **path** - this is always /Shopping. **Note** This setting is mandatory when **Module.Shopping.Enabled=true**. **Note** The Shopping client uses **ShoppingCentralUrl** to make the following API calls to obtain configuration settings from the Shopping Central website. <Module.Shopping.ShoppingCentralUrl>/WindowsServicingAssistant/GetTachyonAgentUrl • LocalhostUrl <Module.Shopping.ShoppingCentralUrl>/WindowsServicingAssistant/ModuleConfig • LocalhostUrl • AlternativeUrls • FirefoxSupportEnabled

Shopping module setting	Installation default	Description
		• Loopback ExemptionEnabled
Module.Shopping.SsoEnabled **Note** This setting is not in the template configuration file.	false	Optional. Default value is **false**. Set this value to **true** if environment uses Single Sign On authentication to access Shopping website. When set to true, the Shopping client does not try to connect to the Shopping website and just uses the setting **Module.Shopping.LocalhostUrl** to listen for localhost API calls. When set to true, the **Module.Shopping.LocalhostUrl** must be specified and matches the value configured in the Shopping Admin Console under 1E Client loopback URL settings. The above client request process allows 1E products like Virtual Assistant to use the loopback feature without installing a Shopping website. For example, setting *`Module.Shopping.SsoEnabled=true`* allows the client to use the local value of LocalhostUrl.

2.6.1.9.2 Information provided by the Shopping client

The following localhost API calls can be entered directly in a browser on a device that has the Shopping client module of the 1E Client enabled and correctly configured. If the Shopping Central website binding is **https** then the localhost URL can accept either **http** or **https**, otherwise it can only accept **http**.

When using an Edge or Metro versions of Internet Explorer browser, you must set **Module.Shopping.LoopbackExemptionEnabled=true**.

2.6.1.9.2.1 MachineId

The following table shows example details sent by the Shopping client to the Shopping Central server. The client makes a localhost API call **MachineId** API to get the details, and then uses a server API call to post them to the Shopping Central website, which creates or updates the

machine details in the Shopping database and returns the **MachineId** GUID from the database. Details are shown in the *1E.Client.log*.

This call is made when a user browses to the Shopping Web Portal, and the website uses the loopback feature to query the local computer.

You can test this by entering *https://localhost:8000/ShoppingClientAgent/MachineInfo/MachineId* directly in a browser.

Attribute	Description	Example
HostName	Computername	ACME-WIN1001
HostDomainName	Computer's NetBIOS Domain Name	ACME
AssignedSite	Configuration Manager client Site code	CM1
MacAddress	Computer's MAC Address	20-68-9D-5B-EB-73
OSVersion	OS Version	10.0.15063
OSArchitecture	OS Architecture	64-bit
OSRole	The role of the OS. Values are: • 1 – Workstation • 2 – Domain controller • 3 – Server • 175 - AVD (with latest hotfix)	1
SccmVersion	Configuration Manager client version	5.00.9012.1020
UniqueId	Configuration Manager client GUID	GUID:04804aed-922c-4a4b-9f41-eab6592e7d83
IntuneDeviceId	Intune Device Id	02c967b2-de4d-5ac1-859c-a15cb11b7638

Attribute	Description	Example
TenantId	Tenant Id	6babcaad-604b-40ac-a9d7-9fd97c0b779f
TenantName	Tenant Name	ACME
Fqdn	Fully Qualified Domain Name	ACME-WIN1001.ACME.LOCAL

2.6.1.9.2.2 Fqdn

The following example is JSON returned by the Shopping client when the **Fqdn** API call is made by Windows Servicing Assistant and 1E Virtual Assistant. Details are shown in the *1E.Client.log*.

You can test this by entering
https://localhost:8000/ShoppingClientAgent/MachineInfo/Fqdn into a browser.

```
{"Fqdn":"1EUKCOL1184.ACME.local"}
```

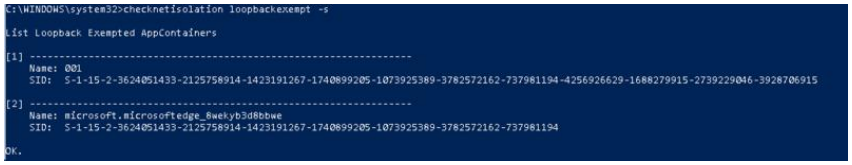
2.6.1.9.3 Checking loopback exemption on Microsoft Edge and Metro Internet Explorer browsers

The following is valid only for Windows 8.1 and Windows 10.

Open a **command-prompt as administrator** on the computer you want to check, then run the following command to verify that loopback exemption was enabled during installation of the 1E Client.

```
CheckNetIsolation LoopbackExempt -s
```

Output should be:



If either of these items are missing, you can manually add them by executing the following commands. Quotes may be required around the name of the app.

For IE:

```
CheckNetIsolation LoopbackExempt -a -n=windows_ie_ac_001
```

For Edge:

```
CheckNetIsolation LoopbackExempt -a -n=Microsoft.MicrosoftEdge_8wekyb3d8bbwe
```

Removing

The exemption from loopback restrictions can also be removed for all apps installed by using the following command:

```
CheckNetIsolation LoopbackExempt –c
```

More information

For more information from Microsoft about CheckNetIsolation please refer to: https://docs.microsoft.com/en-us/previous-versions/windows/apps/hh780593(v=win.10).

2.6.1.10 Wakeup client settings

Installer and configuration settings for the WakeUp client module of the 1E Client supported only on Windows computers.

Note

Note

Installer properties for Windows:

Module.WakeUp.Enabled | Module.WakeUp.ManageFirewallRules | MODULE.WAKEUP.ADDITIONALSUBNETS | MODULE.WAKEUP.AGENTTCPPORT | MODULE.WAKEUP.AGENTTO | MODULE.WAKEUP.ALLOWLASTMANSUSPEND | MODULE.WAKEUP.CERTISSUER | MODULE.WAKEUP.CERTSUBJECT | MODULE.WAKEUP.DEBUG | MODULE.WAKEUP.DELAYCYCLESMSSECS | MODULE.WAKEUP.ENCRYPTIONLEVEL | MODULE.WAKEUP.LASTMANENABLED | MODULE.WAKEUP.LOGFILENAME | MODULE.WAKEUP.LOGPATH | MODULE.WAKEUP.MAGICPACKETDELAY | MODULE.WAKEUP.MAGICPACKETPORT | MODULE.WAKEUP.MAXIMUMFILEAGESECS | MODULE.WAKEUP.MAXLOGFILESIZE | MODULE.WAKEUP.REFRESHHWINFOAFTERHOURS | MODULE.WAKEUP.REFRESHONSUBNETCHANGE | MODULE.WAKEUP.REPEATCOUNT | MODULE.WAKEUP.REPEATDELAY | MODULE.WAKEUP.REPORTING | MODULE.WAKEUP.REPORTINGSERVER | MODULE.WAKEUP.SECUREREPORTINGSERVER | MODULE.WAKEUP.SENDHARDWAREINFO | MODULE.WAKEUP.SPOOLDIR | MODULE.WAKEUP.STAYONFROMSTANDBYMINS | MODULE.WAKEUP.SUBNETOVERRIDE | MODULE.WAKEUP.TCPPORT | MODULE.WAKEUP.USEFIPS | MODULE.WAKEUP.WAKEDISPLAYAFTERSTANDBY | MODULE.WAKEUP.WURESULTDELAY

Note

Note

Configuration file settings:

Module.WakeUp.Enabled | Module.WakeUp.ManageFirewallRules

1E Client installers include a **template configuration file** that contains the more important settings with default values that match hard-coded default values. The configuration file is updated during installation and named **1E.Client.conf** in the installation folder along with the 1E Client executable.

After installation, configuration file settings can be managed using 1E Client reconfiguration, Explorer configuration instructions, Guaranteed State policies, Configuration Manager baselines or other means. Registry settings can also be managed by Windows Group Policy.

Note

The WakeUp client module of the 1E Client replaces the 1E Agent WakeUp components of the 1E Agent and 1E WakeUp Server.

If the WakeUp Server is configured in multi-agent mode (recommended) then the 1E Client must be installed with the WakeUp client module enabled on all in-scope devices.

When the 1E Client starts, and the WakeUp client module is enabled, it will only initialize the WakeUp client module if the OS version is Windows 7 or later. The 1E Client will automatically remove any previous installation of the WakeUp component from the 1E Agent, leaving behind the NightWatchman component, and keeping the WakeUp Agent registry settings. For NightWatchman v7.2.500 onwards the NightWatchman Agent has a separate installer, and its settings continue to be managed by the **NightWatchman Management Center Web Service**.

The WakeUp Server also requires a local WakeUp Agent, and therefore requires the 1E Client to be installed with the WakeUp client module enabled. The WakeUp Server is a 32-bit process and its registry entries are in the 32-bit WOW6432Node area. The 1E Client is a 64-bit process with its registry entries in the 64-bit area. When the 1E Client starts, if the WakeUp client module is enabled the 1E Client will automatically remove any previous installation of the WakeUp Agent component, leaving behind the WakeUp Server component, and moving the existing WakeUp Agent registry settings from the 32-bit to the 64-bit area of the registry.

WakeUp and the WakeUp client module of the 1E Client do not require a full Tachyon infrastructure; only the 1E Client is required, Tachyon Servers are not required. The full Tachyon infrastructure is required only if you are integrating NightWatchman with Tachyon.

The WakeUp client module of the 1E Client is not supported on:

- Non-Windows devices
- Legacy OS (that is OS which Microsoft no longer support including Windows XP, Vista, 7, Server 2008 etc.)

The following legacy WakeUp features from the 1E Agent do not exist in the WakeUp client module:

- 1E WakeUp Agent service - all WakeUp Agent features are now implemented as the WakeUp client module in the 1E Client service
- Computer Health feature - is now obsolete

2.6.1.10.1 WakeUp client installation settings

The table below lists the configuration properties required to enable the WakeUp client required for integration with NightWatchman Enterprise v7.2.500 or later.

Note

You must use UPPERCASE when specifying the *name* of any installer property in a **mst** transform file, and preferably when including them in a msiexec command-line.

Names of settings stored in the configuration file are not case-sensitive. Setting names stored in the registry may be case-sensitive and should be specified as shown.

Settings that have numeric values must be set using decimal integers, unless otherwise specified.

1E Client configuration setting	Installation default	Description
Module.WakeUp.Enabled	false	Set this property to **true** to enable the WakeUp client module. The default value is **false**. Enabling this will also cause any installation of the 1E Agent's WakeUp component to be uninstalled the first time the 1E Client is started, leaving the NightWatchman component if that was installed. **Note** When **true** then you must also specify either the name of the NightWatchman Management Center reporting server, or that reporting is turned off. For details of these and all other installer properties please refer to /document/preview/647736#UUID-b588cdab-ae07-3331-ceb1-c8c6ed63aa1e.
Module.WakeUp.ManageFirewallRules	true	Set this property to **true** to enable the Windows firewall domain rule. The default value is **true**. A Windows firewall domain rule called **1E Client** is removed/added each time the 1E Client is stop/started.

2.6.1.10.2 WakeUp client registry settings

The table below lists additional settings for the WakeUp client module, which may be specified during installation of the 1E Client as Windows installer properties in upper-case. They are stored in the registry in mixed-case. They are not stored in the 1E Client configuration file, and **cannot** be reconfigured after installation using 1E Client command-line parameters. The registry values can be updated via group policy object (GPO) administrative templates or other means.

Note

The table indicates where installer properties have a different name to the registry setting. In some cases this is for backwards compatibility with previous 1E Agent installer properties.

In the descriptions below, the term WakeUp Agent is used to describe the WakeUp client module of the 1E Client. The terms Primary Agent and Alternate Agent are WakeUp roles.

Note

You must use UPPERCASE when specifying the *name* of any installer property in a **mst** transform file, and preferably when including them in a msiexec command-line.

Names of settings stored in the configuration file are not case-sensitive. Setting names stored in the registry may be case-sensitive and should be specified as shown.

Settings that have numeric values must be set using decimal integers, unless otherwise specified.

1E Client installer property	Installation default	Description	Registry name	Registry type
MODULE.WAKEUP.ADDITIONALSUBNETS	**Note** The registry value is not created unless the installation property is specified.	Used only in dedicated agent mode. It enables the dedicated WakeUp Agent to register to awaken multiple subnets. It requires that directed subnet broadcasts are enabled in the routers between the agent and remote subnets. It takes a comma delimited list of subnets. Its use and format are described in WakeUp documentation for NightWatchman Enterprise: Configuring network access control security.	\AdditionalSubnets	REG_SZ
MODULE.WAKEUP.AGENTTCPPORT **Note**	1776	The listening port used by the WakeUp Server to communicate with the WakeUp Agents. Default value is **1776** (decimal). **Note**	\AgentTCP_Port	REG_DWORD

1E Client installer property	Installation default	Description	Registry name	Registry type
The registry name is different to the installer property name (it has an underscore).		The **AgentTCP_Port** value must be different to the TCP_Port value, and must be the same for the WakeUp Server and all Agents.		
MODULE.WAKEUP.AGENTTO		Set to enable Dedicated Agent mode. This parameter should be set to the FQDN (recommended) or NetBIOS name of the WakeUp Server. Default is empty to enable Multi-Agent mode. Dedicated Agent mode does not have Multi-Agent features.	\AgentTo	REG_SZ
MODULE.WAKEUP.ALLOWLASTMANSUSPEND	1	Set to **0** if you want to allow a Primary or Alternate Agent to respect Microsoft power schemes and go to sleep. Set to **1** (default) to prevent a Primary or Alternate Agent going to sleep. **Note** The value of this property is the opposite to what its name implies.	\AllowLastManSuspend	REG_DWORD

1E Client installer property	Installation default	Description	Registry name	Registry type
MODULE.WAKEUP.CERTISSUER		Specify the text used to search for a client certificate in the client certificate store. Either MODULE.WAKEUP.CERTISSUER or MODULE.WAKEUP.CERTSUBJECT is mandatory when all the following are true: • **HTTPS** communications is being used • MODULE.WAKEUP.SECURERREPORTINGSERVER is configured • SSL Settings for the **NightWatchman Management Center Web Service** is configured to require a client certificate If this property is used, it will use the first certificate it finds where the specified text matches the certificate's Issuer CN.	\Reporting\HTTPS\CertIssuer	REG_SZ
MODULE.WAKEUP.CERTSUBJECT		Specify the text used to search for a client certificate in the client certificate store. Either MODULE.WAKEUP.CERTISSUER or MODULE.WAKEUP.CERTSUBJECT is mandatory when all the following are true:	\Reporting\HTTPS\CertSubject	REG_SZ

1E Client installer property	Installation default	Description	Registry name	Registry type
		• **HTTPS** communications is being used • MODULE.WAKEUP.SECURERREPORTINGSERVER is configured • SSL Settings for the **NightWatchman Management Center Web Service** is configured to require a client certificate If this property is used, it will use the first certificate it finds where the specified text matches the certificate's Subject CN.		
MODULE.WAKEUP.DEBUG	13	Sets the level of debug information output to the WakeUp Agentlog file. Default value is **13** (decimal). Range is 1 to 255 (decimal). You should only change this value if requested by 1E Support, and reset it back to **13** when investigation is completed.	\Debug	REG_DWORD
MODULE.WAKEUP.DELAYCYCLESMSSECS	16	Delay (in seconds) before the WakeUp Agent performs a policy refresh after receiving a policy refresh instruction from the WakeUp Server via the Primary Agent. This delay allows time for the ConfigMgr Management Point to be updated in instances where	\DelayCycleSMSSecs	REG_DWORD

1E Client installer property	Installation default	Description	Registry name	Registry type
		Advertisements are newly created. Default value is **16**.		
MODULE.WAKEUP.ENCRYPTIONLEVEL	0	The encryption level used in communications between WakeUp Agents and WakeUp Servers. This does not affect encryption used for WakeUp Reporting. • **0** – Disable WakeUp encryption (default) • **2** – Enable WakeUp encryption • **3** – Enable FIPS encryption **Note** If the MODULE.WAKEUP.USEFIPS installer property is set to **1** it will override the MODULE.WAKEUP.ENCRYPTIONLEVEL installer property and sets the **EncryptionLevel** registry value to **3**, and also uses FIPS for WakeUp Reporting by setting the **UseFipsComplianceEncryption** registry value to **1**. When configuring this option you will need to ensure that the same setting is made	\EncryptionLevel	REG_DWORD

1E Client installer property	Installation default	Description	Registry name	Registry type
		for all WakeUp Agents and WakeUp Servers. Care is required when migrating Agents from Off (**0**) to On (**2**) or the other way round, then the WakeUp Servers will need be configured to support both, by temporary use of of partial/mixed encryption (**1**). Once you are sure all Agents are configured to the same setting, then you should change the WakeUp Server to match the Agents' setting. WakeUp does not support partial/mixed use of FIPS (**3**) and EncryptionLevel (**0/2**) therefore all NightWatchman and WakeUp Servers and Agents must be configured to use FIPS from the outset, or all changed at the same time. EncryptionLevel and FIPS settings used by WakeUp do not affect other 1E Client communications.		

1E Client installer property	Installation default	Description	Registry name	Registry type
MODULE.WAKEUP.LASTMANENABLED	1	Determines if the WakeUp last man standing functionality is turned on or off. • **0** – turns last man standing functionality off • **1** – turns last man standing functionality on (default)	\LastManEnabled	REG_DWORD
MODULE.WAKEUP.LOGFILENAME **Note** The registry name is the same as the installer property name but contains a combination of LOGPATH and LOGFILENAME installer properties.	WakeUpAgt.log	The name of the WakeUp Agent log file. This combines with LOGPATH to give the LogFileName registry value.	\LogFileName	REG_SZ
MODULE.WAKEUP.LOGPATH	%ALLUSERSPROFILE%\1E\Agent	The location of the WakeUp Agent log file. This combines	**Note** See LOG	

1E Client installer property	Installation default	Description	Registry name	Registry type
Note See LOGFILENAME.		with LOGFILENAME to give the LogFileName registry value.	FILENAME	
MODULE.WAKEUP.MAGICPACKETDELAY	1	The delay (in milliseconds) between the WakeUp Agent sending subsequent Magic Packets. Default value is **1**.	\MagicPacketDelay	REG_DWORD
MODULE.WAKEUP.MAGICPACKETPORT **Note** The registry name is different to the installer property name (it has an underscore).	1776	The UDP port used to send wake up broadcasts. Default value is **1776** (decimal).	\MagicPacket_Port	REG_DWORD
MODULE.WAKEUP.MAXIMUMFILEAGESECS	1209600 (14 days)	Sets the maximum age (in seconds) for the Agent to retain reporting information locally when the **NightWatchman Management Center Web Service** cannot be contacted. By default, this is set to **1209600** seconds (14 days). Any files older than that will not be submitted to the **NightWatchman Management Center Reporting** and will be	\Reporting\MaximumFileAgeSecs	REG_DWORD

1E Client installer property	Installation default	Description	Registry name	Registry type
		deleted instead. This value need not be modified under normal circumstances.		
MODULE.WAKEUP.MAXLOGFILESIZE	1048576 (1MB)	Maximum size (in bytes) for the WakeUp Agent log file. There are 5 rollover files numbered 1 (newest) to 5 (oldest) with the rollover number included as n.log (In previous versions of WakeUp the .LOG file was renamed with a .LO_ extension and a new .LOG file is created. The .LO_ file is overwritten each time.)	\MaxLogFilesize	REG_DWORD
MODULE.WAKEUP.REFRESHHWINFOAFTERHOURS	720 (30 days)	The frequency (in hours) for hardware inventory details to be sent to the NightWatchman server if WakeUp reporting is enabled (default) and MODULE.WAKEUP.SENDHARDWAREINFO=ON. Range is from 24 to 999. The default is **720** (30 days). If the NightWatchman Agent is also installed, it will send hardware inventory more frequently.	\Hardware\RefreshHwInfoAfterHours	REG_DWORD
MODULE.WAKEUP.REFRESHONSUBNETCHANGE	ON	Triggers the local ConfigMgr client to do a Hardware Inventory Cycle when the WakeUp Agent detects a change of subnet. The client in turn, updates the ConfigMgr Site inventory, thereby enabling the	\RefreshOnSubnetChange	REG_SZ

1E Client installer property	Installation default	Description	Registry name	Registry type
		Site's WakeUp Server to have the latest subnet details. • **ON** – monitor subnet changes on both physical and wireless connections (default). • **IGNOREWIRELESS** – only monitor subnet changes on physical connections. • **OFF** – no action is taken when the subnet changes. **Tip** This is particularly useful where laptops move between offices. Typically, Wake-On-LAN is not supported over wireless, therefore **IGNOREWIRELESS** avoids the overhead of triggering a ConfigMgr hardware inventory for wireless changes. Use **OFF** only if you are sure computers will not change subnet, and you can rely on the normal ConfigMgr inventory cycle. The WakeUp system relies on having the latest subnet details in order to wake computers. The WakeUp Agent updates the NightWatchman database with		

1E Client installer property	Installation default	Description	Registry name	Registry type
		all subnet changes, because the NightWatchman server is designed to support frequent updates.		
MODULE.WAKEUP.REPEATCOUNT	0	Number of times to repeat sending Magic Packets. Default is **0**. **Note** If you suspect that your network is prone to dropping datagram packets you should try different configurations for ***RepeatCount*** and *RepeatDelay* . Otherwise, these should be left at their default values.	\RepeatCount	REG_DWORD
MODULE.WAKEUP.REPEATDELAY	0	Delay (in milliseconds) before resending a repeated Magic Packet. Default is **0**. **Note** If you suspect that your network is prone to dropping datagram packets you should try different configurations for *RepeatCount* and ***RepeatDelay*** . Otherwise, these should be left at their default values.	\RepeatDelay	REG_DWORD

1E Client installer property	Installation default	Description	Registry name	Registry type
MODULE.WAKEUP.REPORTING	ON	Enables WakeUp reporting. Sets whether the Agent sends reporting messages to the **NightWatchman Management Center Web Service**. May be set to one of the following values: • **ON** – reporting is enabled and messages are forwarded to the NightWatchman server. It is mandatory to specify one of the following: MODULE.WAKEUP.REPORTINGSERVER or MODULE.WAKEUP.SECUREREPORTINGSERVER • **OFF** – no information is reported to the server. **Tip** When installing the 1E Client on a WakeUp Server, set **MODULE.WAKEUP.REPORTING=OFF** so that the server does not appear as a client in the NightWatchman Management Center Admin Console. This will only disable Agent reporting whilst the WakeUp Server will have reporting enabled for reporting statistics.	\Reporting	REG_SZ

1E Client installer property	Installation default	Description	Registry name	Registry type
MODULE.WAKEUP.REPORTINGSERVER **Note** The registry name is different to the installer property name. The supplied value is converted into a full URL.		Set this parameter to the FQDN (recommended) or NetBIOS name of the server hosting the NightWatchman Management Center Web Service. **Warning** Mandatory when WakeUp reporting is enabled (default) and using **HTTP** for communications. **Tip** If **HTTP** is not using standard port 80 then specify the port number as part of the server name: MODULE.WAKEUP.REPORTINGSERVER="ACMESERVER.ACME.COM:8080"	\Reporting\HTTP\ServiceUrl	REG_SZ
MODULE.WAKEUP.SECUREREPORTINGSERVER **Note** The registry name is different to the installer property name. The supplied value is		Set this parameter to the FQDN (*required*) or NetBIOS name of the server where the NightWatchman Management Center Web Service component secure site has been installed. **Warning** Mandatory when WakeUp reporting is enabled (default) and using **HTTPS** for communications. **Tip**	\Reporting\HTTPS\ServiceUrl	REG_SZ

1E Client installer property	Installation default	Description	Registry name	Registry type
converted into a full URL.		If **HTTPS** is not using standard port 443 then specify the port number as part of the server name: MODULE.WAKEUP.SECUREREPORTINGSERVER="ACMESERVER.ACME.COM:7433"		
MODULE.WAKEUP.SENDHARDWAREINFO **Note** The registry name is different to the installer property name.	ON	Enables hardware information messages to be sent to the NightWatchman server, if MODULE.WAKEUP.REPORTING=ON. See also MODULE.WAKEUP.REFRESHHWINFOAFTERHOURS.	\Modules\HwInfoAgt	REG_SZ
MODULE.WAKEUP.SPOOLDIR **Note** The registry name is different to the installer property name.	%ALLUSERSPROFILE%\1E\Reporting\WakeUp\	The location of the WakeUp spooler directory, where Reporting messages are stored before being sent to the **NightWatchman Management Center Web Service**. The location should not need to be modified under normal circumstances. Default value is%ALLUSERSPROFILE%\1E\Reporting\WakeUp\	\Reporting\SpoolerDirectory	REG_SZ
MODULE.WAKEUP.STAYONFROMSTANDBYMINS	0	Set this to the number of minutes the Wakeup Agent keeps the OS awake after a	\StayOnFromStandbyMins	REG_D

1E Client installer property	Installation default	Description	Registry name	Registry type
		wakeup. This is to allow sufficient window of time for multiple jobs to run. If set to less than or equal to **0** (default) then the WakeUp Agent will keep the OS awake for 20 minutes. Set this this value to more than **20** to keep the OS awake for longer.		WORD
MODULE.WAKEUP.SUBNETOVERRIDE	**Note** The registry value is not created unless the installation property is specified.	Contains a list of all unauthenticated subnets that correspond to the authenticated subnets for which the Agent is responsible. Its use and format are described in WakeUp documentation for NightWatchman Enterprise: Configuring network access control security.	\SubnetOverride	REG_SZ
MODULE.WAKEUP.TCPPORT **Note** The registry name is different to the installer property name	1777	The listening port used by the WakeUp Agents to communicate with the WakeUp Server. Default value is **1777** (decimal). **Note** The **TCP_Port** value must be different to the **AgentTCP_Port** value, and must be the same for the	\TCP_Port	REG_DWORD

1E Client installer property	Installation default	Description	Registry name	Registry type
(it has an underscore).		WakeUp Server and all Agents.		
MODULE.WAKEUP.USEFIPS **Note** The registry name is different to the installer property name.	0	Set to **1** to force the WakeUp agent to use a FIPS-compliant algorithm for: • WakeUp Reporting to the **NightWatchman Management Center Web Service** by setting **UseFipsComplianceEncryption** registry value to 1. • Communication between WakeUp Agents and WakeUp Servers. It will override the MODULE.WAKEUP.ENCRYPTIONLEVEL installer property and set the **EncryptionLevel** registry value to 3. If enabled, then all components in the NightWatchman and WakeUp system must have FIPS enabled. EncryptionLevel and FIPS settings used by WakeUp do not affect other 1E Client communications.	\Reporting\UseFipsComplianceEncryption	REG_DWORD
MODULE.WAKEUP.WAKEDISPLAYAFTERSTANDBY	0	Set to **1** to force the display to come on (assuming it has	\WakeDisplayAfterStandBy	REG_D

1E Client installer property	Installation default	Description	Registry name	Registry type
		power) after it has been woken up. This feature works in conjunction with MODULE.WAKEUP.STAYONFROMSTANDBYMINS.		WORD
MODULE.WAKEUP.WURESULTDELAY	0	The time (in seconds) the WakeUp Primary Agent allows for responses to magic packets before it tries to pings devices that have not yet responded with a WASAWAKE or JUSTWOKE and then report NOAGENT or FAILED to the WakeUp Server for reporting purposes. This is especially useful when trying to wake devices that do not have the WakeUp client module enabled. The delay should be set to how long it normally takes for devices to start up. If set to **0** the WakeUp Server determines the time, but this can be overridden by changing the value on the WakeUp Primary Agent. In multi-agent mode, this effectively means all Agents.	\WUResultDelay	REG_DWORD

The following table is for WakeUp client module registry values that do not have Windows installer properties, and are not stored in the 1E Client configuration file.

Warning

These registry values are reserved for use by the WakeUp client module and must not be modified.

Registry name	Registry type	Description
\AgentRegInfo	REG_SZ	Used by the Primary and Alternate Agent to store information it has registered with the WakeUp Server.
\AltAgentMacAddress	REG_BINARY	Used by the Primary and Alternate Agent to store each other's MAC address details.
\InstallationDirectory	REG_SZ	Used as a record of the installation folder, for backwards compatibility.
\MiniAgentTo	REG_SZ	Used by the Primary and Alternate Agent to store the NetbiosName of the 1E Wakeup Server.
\PatchLevel	REG_SZ	Used to indicate the version of the most recent software patch installed.
\TachyonAgentVersion	REG_SZ	Used as a record of the 1E Client version that created the registry settings.

2.6.2 1E Client command-line parameters

Command-line interface (CLI) parameters available to the 1E Client executable.

Some CLI actions invoke the 1E Client itself, whereas others are used to control execution of the 1E Client. Normally a user does not have to be aware of the options, but they can be useful for testing and debugging.

If **1E.Client.exe** is run without a CLI parameter, it will output a usage message showing the options and syntax.

The syntax shown below shows all parameters starting with - but you can use **/** instead. CLI parameters are mutually exclusive unless noted otherwise.

When running these commands from a console, run as administrator (Windows) or prefix the commands with *sudo* (non-Windows).

> **Tip**
>
> A popular use of the CLI is to reconfigure settings in the 1E Client configuration file using the **-reconfigure** and**-restart**parameters.
>
> For further guidance on using the **-reconfigure** parameter, please refer to Reconfiguring 1E Client.

2.6.2.1 Command-line parameters

2.6.2.1.1 -console

Instead of running the 1E Client as a service or daemon, run it as a console application. To stop the 1E Client, press *ctrl-C*.

> **Warning**
>
> This mode is for testing and should not be used unless advised by 1E.

2.6.2.1.2 -runservice

This is the normal invocation of the 1E Client to run it as a service or daemon.

> **Warning**
>
> Do not use this mode from the command line.

2.6.2.1.3 -uninstall[=module1,module2,...]

Run the uninstall action on all (by default) or the specified modules. Case is not significant.

Most modules use the default uninstall action which does nothing, but a few such as Nomad perform important tasks.

This CLI action checks that the 1E Client service/daemon is not currently running, and aborts if it is, because it is not safe to uninstall a module that is active.

2.6.2.1.4 -getdbkey

In rare circumstances 1E Support may ask for a copy of the Tachyon persistent storage database files for diagnostic purposes. This option gives an encrypted form of the DB's key.

> **Warning**
>
> Do not use this option unless requested by 1E Support.
>
> **Note**
>
> Because the DB is generated and encrypted by the 1E Client runs using the system account, you must fetch the key in the same context. On Windows the SysInternals *psexec* command is convenient for this, as follows:

```
psexec -s 1E.Client.exe -getdbkey
```

2.6.2.1.5 -reconfigure name1=value1 ...

This is a convenient way to change settings in the 1E Client configuration file. One or more name=value pairs should be specified, and the configuration file will be updated. A value can be empty, although that is only valid for a few configuration settings. Case of the name-part is not significant, but the case of the value is preserved when it is written to the configuration file.

> **Warning**

You can change only configuration file settings using this method, you must use other methods to change registry settings. For further guidance, please refer to Reconfiguring 1E Client.

Note

Any name=value pair can be added to the configuration file, no validation is done. If a key with the name does not already exist in the configuration file, it will be added to the file and a warning output (in case the name has been misspelled).

This CLI action can be used in combination with **-start** and **-restart** (and **-stop** although that is not very useful).

Note

The 1E Client will not pick up the new configuration value(s) until it is restarted.

2.6.2.1.5.1 Examples

Set the *Switch* and *BackgroundChannelUrl* values, then restart the 1E Client (after a random stagger interval) to pick up the new values.

On Windows:

```
"C:\Program Files\1E\Client\1E.Client.exe" -reconfigure Switch=ACME-DMZ01.ACME.LOCAL:4000 BackgroundChannelUrl=https://ACME-DMZ01.ACME.LOCAL:443/Background/ -restart
```

On Linux and Solaris:

```
/usr/sbin/1E.Client -reconfigure Switch=ACME-DMZ01.ACME.LOCAL:4000 BackgroundChannelUrl=https://ACME-DMZ01.ACME.LOCAL:443/Background/ -restart
```

On macOS:

```
cd /Library/Application Support/1E/Client # Do not prefix cd with sudo
./1E.Client -reconfigure Switch=ACME-DMZ01.ACME.LOCAL:4000 BackgroundChannelUrl=https://ACME-DMZ01.ACME.LOCAL:443/Background/ -restart
```

2.6.2.1.6 -stdin

Read configuration values from standard input rather than the configuration file. This is only used with **-console** when debugging.

Warning

This mode is for testing and should not be used unless advised by 1E.

2.6.2.1.7 -stop [-immediate]

Stop the 1E Client service or daemon if it is running. If **-immediate** is given, the 1E Client will shut down immediately (or as soon as possible to preserve instruction integrity), otherwise it will happen after a random number of seconds in a range between the *ConnectionRetryTimeInSecondsMin* and *ConnectionRetryTimeInSecondsMax* configuration

values. This is to prevent flooding, for example, the Switch with offline messages, depending on which client options have been enabled.

2.6.2.1.8 -start [-immediate]

Start the 1E Client service or daemon if it is not already running. If **-immediate** is given, the 1E Client will start immediately, otherwise it will happen after a random number of seconds in a range between the *ConnectionRetryTimeInSecondsMin* and *ConnectionRetryTimeInSecondsMax* configuration values. This is to prevent flooding, for example, the Switch with online messages, or Nomad content registration messages, depending on which client options have been enabled.

2.6.2.1.9 -restart [-immediate]

Stop the 1E Client service or daemon if it is running, then start it. If **-immediate** is given, this will happen immediately, otherwise it will happen after a random number of seconds in a range between the *ConnectionRetryTimeInSecondsMin* and *ConnectionRetryTimeInSecondsMax* configuration values. This is to prevent flooding, for example, the Switch with offline and online messages, or Nomad content registration messages, depending on which client options have been enabled.

2.6.3 Log files

Details of 1E Client log files.

> **Tip**
>
> This page is a reference of log file names and location. If you are here to troubleshoot then please refer to Troubleshooting instead.

2.6.3.1 1E Client logs

> **Note**
>
> Upgrades retain the location and configuration of log files.

2.6.3.1.1 Log file locations

1E Client logs on Windows

%ALLUSERSPROFILE%\1E\Client\1E.Client.log (used by 1E Client and Tachyon features, and Shopping client)

%ALLUSERSPROFILE%\1E\Client\NomadBranchUninstall-YYYY_MM_HHTMM_HH_SS_000Z.log

1E Client logs on macOS

/Library/Logs/1E.Client.Daemon.log (shows any service start errors)

/Library/Logs/1E.Client.log (shows the current operation of the 1E Client)

1E Client logs on other non-Windows platforms

/var/log/1E/Client/1E.Client.log

Nomad client log

%ALLUSERSPROFILE%\1E\NomadBranch\LogFiles\NomadBranch.log

PXE Everywhere Agent log

%ALLUSERSPROFILE%\1E\PXEEverywhere\PXEEverywhere.log

Shopping WSA client log

%ALLUSERSPROFILE%\1E\Client\WSA.log

WakeUp client log

%ALLUSERSPROFILE%\1E\Agent\WakeUpAgt.log

> **Note**
>
> By default, Windows resolves %ALLUSERSPROFILE% as C:\ProgramData\

2.6.3.1.2 Configuration

1E Client log

The **LogPath** setting is stored in the **1E.Client.Conf** file and determines the full path and filename of the 1E Client log file.

The 1E Client log is shared by:

- 1E Client
- Tachyon client features
- Shopping client module (only available on Windows OS)

To change the logging level, please refer to LoggingLevel in the 1E.Client.CONF file.

The following are not configurable in this version:

- Maximum size of 5MB
- 5 rollover files numbered 1 (newest) to 5 (oldest) with the rollover number included as n.log

Nomad client log

LogFileName registry is configurable using MODULE.NOMAD.LOGPATH and MODULE.NOMAD.LOGNAME installer properties.

- MaxLogFileSize is configurable using MODULE.NOMAD.MAXLOGSIZE. Default is 5242880 (5MB).
- When the log file reaches its maximum size, it is renamed with a .LO_ extension and a new .LOG file is created. The .LO_ file is overwritten each time.

PXE Everywhere Agent log

LogFileName registry is configurable using MODULE.PXEEVERYWHERE.LOGPATH installer property, with the default filename PXEEverywhere.log.

- MaxLogfileSize is configurable using MODULE.PXEEVERYWHERE.MAXLOGFILESIZE. Default is 1048576 (1MB).
- When the log file reaches its maximum size, it is renamed with a .LO_ extension and a new .LOG file is created. The .LO_ file is overwritten each time.
- The logfile format is configurable using MODULE.PXEEVERYWHERE.LOGFORMAT default (1) is Configuration Manager-compatible format.

Shopping WSA client log

Not configurable using installer properties. Configurable by modifying the Log4Net settings in the WSA.exe.config file, located in %ProgramFiles%\1E\Client\Extensibility\WSA folder.

WakeUp client log

LogFileName registry is configurable using MODULE.WAKEUP.LOGPATH and MODULE.WAKEUP.LOGFILENAME installer properties.

- MaxLogFileSize is configurable using MODULE.WAKEUP.MAXLOGFILESIZE. Default is 1048576 (1MB).
- 5 rollover files numbered 1 (newest) to 5 (oldest) with the rollover number included as n.log
- In previous versions of WakeUp the .LOG file was renamed with a .LO_ extension and a new .LOG file is created. The .LO_ file is overwritten each time.

2.6.4 1E Client release information

2.6.4.1 1E Client 8.1 Release Notes – last updated 02-August-2022

These notes contain late-breaking information about 1E Client that you need to have to successfully install and use the product. For the most up-to-date information please see the online readme. You should read these release notes and the online documentation for 1E Client thoroughly before installing the software.

2.6.4.1.1 New features in 1E Client 8.1

2.6.4.1.1.1 Tachyon client for Tachyon v8.1

- The status of all Guaranteed State rules is reported after a configurable number of days, even if the rule status has not changed
- New module called Policy to give better visibility into what the current status of Guaranteed State rules:
  - /document/preview/739118#UUID-1de33ffb-d4e6-aab8-88c6-4bbfbd5b7034_id_PolicyForceStatusReport-ForceStatusReport - trigger the 1E Client to force-send all policy status messages on restart
  - /document/preview/739119#UUID-dbc9eec3-1781-f814-2efa-8af6b0fc1a2b_id_PolicyGetEventSubscriptions-GetEventSubscriptions - get event subscriptions in current policy
  - /document/preview/739120#UUID-f0f824b7-163a-72e0-2c9c-6cd39f7a0f05_id_PolicyGetRuleEvaluationHistory-GetRuleEvaluationHistory ([ruleId]) - get the evaluation history for one rule or all rules
  - /document/preview/739121#UUID-b55da451-c425-a143-6e01-37f100c0b543_id_PolicyGetRules-GetRules - get rules in current policy (with current status)
  - /document/preview/739122#UUID-daf92ecb-8959-48fc-1b3e-fd6e9a7abd3b_id_PolicyGetStatistics-GetStatistics - get policy-related statistics/perf counters
  - /document/preview/739123#UUID-d5b70c1f-8194-d25e-337b-f1ce3cbc8a3e_id_PolicyGetSummary-GetSummary - get a summary of the current policy
  - Policy.Invalidate () - reset the 1E Client's policy to null/empty, which will force a renegotiation of the policy (immediately if connected to Switch, or when it does eventually connect)
- New methods:
  - /document/preview/739176#UUID-65c8a3bf-3714-442a-4c5c-19b77d5e93af_id_StorageList-Delete
- New SQL functions:
  - /document/preview/739230#UUID-4fd278df-907a-b131-c131-e2449af777af_id_HASHSTRING-HASHSTRING, /document/preview/739234#UUID-3d29f21e-8d41-cc2a-e2cd-efc8f7639fe8_id_NEWID-NEWID

- Deprecated methods: FileContent.GetTorrentAnnounceUris, FileContent.GetTorrentDescribedFiles, FileContent.GetTorrentInfo
- Support for Solaris operating systems has been deprecated
- Will not install on Windows XP and Server 2003
- Now uses C++ 14, OpenSSL 3.0.0 7 Sep 2021, SQLite 3.36.0

Note

Only Tachyon client features are supported by the 1E Client on non-Windows devices.

2.6.4.1.1.2 Shopping client for Shopping v6.1

- Shopping 6.1 client is the Shopping module in 1E Client 8.1
- No changes - only hotfixes.

2.6.4.1.1.3 WakeUp client for NightWatchman Enterprise v7.3

- WakeUp 7.3 client is the WakeUp module in 1E Client 8.1
- No changes - only hotfixes.

2.6.4.1.1.4 Content Distribution client for Content Distribution v8.1

- NomadBranch 8.1 client is the Content Distribution module in 1E Client 8.1
- Set Nomad as Download Program - cloud-based services to support Work From Anywhere (WFA) users are becoming more critical to the way enterprises work, there is an increased reliance on Cloud Distribution Points for distributing content.
- Enhancements:
  - Improvements to the Client authentication criteria to authenticate with a DP (or any download source)
  - Download reporting now includes Top status bar, for Bandwdith Protection Reporting.

2.6.4.1.1.5 PXE client for PXE Everywhere v8.1

- PXE Everywhere Agent is a client module of 1E Client 8.1, available for x64 and x86 platforms
- There are no other changes in this version other than hotfixes.

2.6.4.1.2 Online help

Tachyon comes with online help that shows you how to install, configure and use the product. Click the following link to view the help:

- Introducing 1E Client

For support queries, please:

- Use https://support.1e.com/ where you can search the KB or submit a support case.
- Contact support@1e.com.

2.6.4.1.3 Known issues

Current known issues related to installation of the 1E Client can be found on the Known issues page of the 1E Client documentation.

2.6.4.2 1E Client Release History

2.6.4.2.1 Web Release-8.1 (19-Apr-2022)

2.6.4.2.1.1 1E Client 8.1.2.62 - 1E Client Non-Windows 8.1.2.62 - TIMS 8.1.2.62

2.6.4.2.1.1.1 Features and enhancements

For new features in this release please refer to the top of the page.

2.6.4.2.1.1.2 Contained fixes - 1E Client

- Q22096 - Shopping - High CPU utilization caused by Shopping client UI (TFS 245631)
- Q22068 - Content download from Cloud DP does not work when Enhanced HTTP is enabled in CM 2107 (TFS 248101)
- Q22062 - High priority announcements are treated exactly the same as standard priority (TFS 247010)
- Q22056 - Superfluous informational message in NomadBranch log (TFS 249059)
- Q22054 - Failing to decrypt content while downloading from Cloud Distribution Points (TFS 247202)
- Q22040 - Incorrect OS reported by 1E Client when installed on Windows 11 device (TFS 247897)
- Q21994 - 1E Client - Force policy status reporting after X days (TFS 246032)
- Q21992 - Guaranteed State dashboards and detail reports may show a discrepancy for the current compliance state of a rule. (TFS 246358)
- Q21990 - 1E Client Fast File Find returning incomplete results (TFS 246923)
- Q21988 - 1E Client fails to capture output from masqueraded process (TFS 246874)
- Q21942 - 1E Client reporting Windows 10 2009 H2 differently due to OS changes (TFS 246371)
- Q21930 - Nomad precache content status is not in sync with Content Download DB (TFS 244875)
- Q21928 - Nomad download over enhanced HTTP fails with CM 2107 (TFS 245217)
- Q21874 - SoftwarePerformance data for Office executables is not captured (TFS 245425)
- Q21872 - 1E Client unable to connect to Tachyon due to Cross-Signing Certificates (TFS 237025)
- Q21870 - Allow Real-Time Control Center to display info surveys (TFS 245204)
- Q21868 - Device.GetDisks is reporting DiskStatus = Not Available on real physical devices (TFS 245612)
- Q21866 - 1E Client can log potentially sensitive data in plain-text at TRACE level (TFS 246162)
- Q21806 - Shopping notifications do not appear after upgrade to 1E Client 8.0 . (TFS 245391)

2.6.4.2.1.1.3 Contained fixes - TIMS

- None

2.6.4.2.2 Web Release-8.0 (29-Oct-2021)

2.6.4.2.2.1 1E Client 8.0.4.261 - 1E Client Non-Windows 8.0.4.261 - TIMS 8.0.4.261

2.6.4.2.2.1.1 Tachyon client for Tachyon v8.0

Real-Time Control Center - updated Client UI in notification area to support Experience Engagements (Announcements and Surveys), and ITSM Support Tickets

New methods:

Device.GetDisks, FileSystem.PathExists, Interaction.ShowAnnouncement, Storage.GetRemote

Updated methods:

Agent.GetDiagnostics, Network.GetIpAddresses, OperatingSystem.ControlService, OperatingSystem.GetProcesses, NativeServices.RunWmiInstanceMethod, NativeServices.RunWmiQuery, NativeServices.RunWmiStaticMethod, Security.UnquarantineDevice, Storage.Set

New capture sources for Tachyon Activity Record:

BootPerformance, SoftwarePerformance.DiskUsage, SoftwarePerformance.ProcessNetworkUsage

Support for the SQLite JSON extension (), allowing JSON data to be queried through SCALE

TAGS installer property for Windows devices - see Tachyon client settings

Support added for the following Operating Systems:

Windows 10 21H1

Fedora 34

openSUSE Leap 15.2

Red Hat Enterprise Linux 7.9

Red Hat Enterprise Linux 8.3

SUSE Linux Enterprise 15.2

> **Note**
>
> Only Tachyon client features are supported by the 1E Client on non-Windows devices.

2.6.4.2.2.1.2 Shopping client for Shopping v6.1

Shopping 6.1 client is the Shopping module in 1E Client 8.0

Client-side Order Tracking feature - configurable on the Shopping server - to provide toast notifications and 1E Shopping UI popup in the notification area.

2.6.4.2.2.1.3 WakeUp client for NightWatchman Enterprise v7.3

WakeUp 7.3 client is the WakeUp module in 1E Client 8.0

No changes - only hotfixes.

2.6.4.2.2.1.4 Nomad client for Nomad v8.0

NomadBranch 8.0 client is the Nomad module in 1E Client 8.0

New registry setting SiteSSDMinPackageSizeKB to set the minimum size of content before making SSD request

Installer changes:

Integrating Nomad with WakeUp

Enable Nomad FanOut as a default - default value of SpecialNetShare has changed to 0x2060 (8288)

Platform features enabled by using the BackgroundChannelUrl instead of PlatformURL

Enhancements to CacheCleaner functionality to better support remote users as part of the Working From Anywhere initiative.

2.6.4.2.2.1.5 PXE client for PXE Everywhere v8.0

PXE Everywhere Agent is a client module of 1E Client 8.0, available for x64 and x86 platforms

Bootshim.efi folder renamed from **BootPrograms** to **NetworkBootPrograms** (1E\Client\Extensibility\PXEEverywhere\NetworkBootPrograms)

There are no other changes in this version other than hotfixes.

2.6.4.2.2.1.6 Contained fixes - 1E Client

Q21786 - Nomad - Automatic CacheClean updates (TFS 244966)

Q21784 - Nomad is not doing any DP load balancing (TFS 234960)

Q21782 - Nomad failing download content requested by VMware Workspace One (TFS 244963)

Q21724 - Nomad - Get Migration Settings step is not using correct MAC address to query CM computer association (TFS 241912)

Q21706 - WSA- Nomad download jobs coming from WSA fail to download from Cloud DP (TFS 231049)

Q21704 - Shopping Order Tracking feature is always enabled (TFS 240467)

Q21694 - Nomad - CDSSync doesn't report complete download data (TFS 236909)

Q21692 - Nomad isn't honouring Job timeout (TFS 237633)

Q21690 - Nomad crashing on multiple devices (TFS 235899)

Q21670 - Notifications are not issued when the machine and Shopping are logged in with another same user. (TFS 236754)

Q21632 - Shopping Order Tracking (TFS 165266)

Q21630 - Guaranteed State Check Rule for FileSystem.GetFileDetails stopping 1E Client service (TFS 234123)

Q21628 - Nomad fails during byte-range download if ContentRegistration is disabled (TFS 235180)

Q21602 - Standardize Nomad date logging (TFS 231355)

Q21600 - Nomad hash errors on 3rd party software update downloads via WUMU (TFS 230142)

Q21470 - Agent - Client is released from Quarantine after device is hard powered off without a graceful shutdown (TFS 228018)

2.6.4.2.2.1.7 Contained fixes - TIMS

None

2.6.4.2.3 Web Release-5.2 (26-Mar-2021)

2.6.4.2.3.1 1E Client 5.2.5.479 - 1E Client Non-Windows 5.2.5.478 - TIMS 5.2.5.479

2.6.4.2.3.1.1 Features and enhancements

2.6.4.2.3.1.2 Tachyon client for Tachyon v5.2

New methods: Inventory.GetTables, Network.GetWiFiNetworks

Updated methods: Network.GetConnections, OperatingSystem.GetSummary

New TimeoutSecs parameter in: FileSystem.FindFileByName, FileSystem.FindFileBySizeAndHash, FileSystem.FindDirectoryByName

New policy trigger: DirectoryChange

New installer property for Windows devices: DataRoot

Support for TPM (Trusted Platform Module) based client certificates on Windows

OsLocale and OSInstallUtc included in online messages to Switch to support the Location tile in the Details panel of Tachyon Platform 5.2 - Device View: Overview

Support for Nomad client changes, including use of event policy system, and sharing certificate details

Improved Downloading Tachyon client content and Nomad integration

Description removed from Experience Surveys in Client UI (Interaction module)

Additional installation script for deploying client on macOS when using tachyon.pfx certificate file as an alternative to using the macOS key store

Support added for following Operating Systems:

Windows 10-20H2

macOS on Apple M1 architecture.

> **Note**
>
> Only Tachyon client features are supported by the 1E Client on non-Windows devices.

2.6.4.2.3.1.3 Shopping client for Shopping v6.0

Shopping 6.0 client is the Shopping module in 1E Client 5.2

Adding support for Single sign-on (SSO) environment and Workgroup devices to respond with machine details on Shopping website.

2.6.4.2.3.1.4 WakeUp client for NightWatchman Enterprise v7.3

WakeUp 7.3 client is the WakeUp module in 1E Client 5.2

No changes - only hotfixes.

2.6.4.2.3.1.5 Nomad client for Nomad v7.1

NomadBranch 7.1 client is the Nomad module in 1E Client 5.2

ActiveEfficiency features are now provided by Content Distribution on Tachyon Platform 5.2

Client status messages are sent via Tachyon event policy system - Content Distribution uses these instead of StatusMsgEvents using Configuration Manager

New client settings:

DeliveryOptimizationReportingEnabled - monitoring of Delivery Optimization downloads and reporting them to Content Distribution - disabled by default

SupportWPAD - provides support for Web Proxy Auto-Discovery Protocol (WPAD) - disabled by default.

2.6.4.2.3.1.6 PXE client for PXE Everywhere v4.0.100

PXE Everywhere Agent 4.0.100 is the PXE Everywhere module in 1E Client 5.2

No changes - only hotfixes.

2.6.4.2.3.1.7 Tachyon Instruction Management Studio (TIMS) v5.2

For more information about TIMS, please refer to Tachyon SDK - Getting started with TIMS.

Multiple tabs

Default instruction type for a new instruction is now Action rather than Question

Validation error when %global% or %environment% variables are used in fragments (InstructionType fix, check, and precondition).

2.6.4.2.3.1.8 Contained fixes - 1E Client

Q21416 - WSA - VPN username goes missing if the WSA wizard is relaunched without cancelling (TFS 227164)

Q21408 - Agent - Client - User service instances remain after the associated user session is logged off (TFS 222272)

Q21406 - Agent - HTTP download - File 4GB+ causes unhandled exception and failure if Nomad is used (TFS 226892)

Q21386 - Nomad does not work as ACP after CM Client upgrade to 5 00 9040 1015 (CB 2010) (TFS 221969)

Q21374 - Nomad - Fails to retrieve content locations from the MP if there are no boundary groups except the default (TFS 220818)

Q21370 - WSA – Validate WiFi VPN Credentials step fails on non-English machines in WSA task sequence (TFS 221362)

Q21368 - Agent - Methods - FileSystem Find methods can consume significant machine memory (TFS 220092)

Q21366 - Agent - Methods - Correctly handle logging of error messages when Http.Post method contains the '%' symbol within the Body parameter (TFS 220574)

Q21364 - Agent - Interaction - Interaction module establishes TCP listener even if module is disabled (TFS 220906)

Q21358 - PXE boot may fail if multiple network cards are present in the system (TFS 215056)

Q21346 - WSA compatibility scan fails for non-english machines (TFS 220588)

Q21330 - Nomad - Failing to get patches from WUMU (TFS 212827)

Q21328 - Enabling the PXE Module in the 1E Client 5.1 creates an additional 1E.Client.log in C:/Temp folder (TFS 218205)

Q21324 - Fix shopping module dll signing with correct signature (TFS 219781)

Q21280 - Agent - Experience shows processes with unrealistically high Processor Time % (TFS 216267)

Q21278 - 1E Client Shopping module will not initialize when Shopping is configured for SSO (TFS 201787)

Q21222 - Agent - Client with specific locale settings not reporting in experience (TFS 215037)

Q21220 - Agent – 1E Client UI notification icon shows Poke with DEBUG or TRACE level logging (TFS 213480)

Q21218 - Agent - Methods - NativeServices.RunCommand no longer strips trailing whitespace in Output (TFS 216457)

Q21141 - PXE boot fails when the windows firewall is enabled (TFS 212739)

2.6.4.2.3.1.9 Contained fixes - TIMS

Q21230 - Agent - Client with specific locale settings not reporting in experience

Q21226 - Agent – 1E Client UI notification icon shows Poke with DEBUG or TRACE level logging

Q21224 - Agent - Methods - NativeServices.RunCommand no longer strips trailing whitespace in Output

2.6.4.2.4 Web Release-5.1 (18-Aug-2020)

2.6.4.2.4.1 1E Client 5.1.0.922 - 1E Client Non-Windows 5.1.0.922 - TIMS 5.1.0.922

2.6.4.2.4.1.1 Tachyon client for Tachyon v5.1

User surveys and notifications, and notification area icon called 1E Client UI. This is used by Tachyon Experience, please refer to:

Tachyon Experience 1.3 - Getting feedback via User Sentiment Surveys: What the end-user sees

Tachyon Experience 1.3 - Getting feedback via General Purpose Surveys: What the end-user sees

Tachyon Experience 1.3 - Getting feedback via General Purpose Surveys: Do not disturb...

Support for user-centric features (user session reporting). This is used by Tachyon Experience, please refer to Tachyon Experience - Users page

Support for Telemetry. Please refer to Tachyon 5.2 - Telemetry data, and Tachyon 5.2 - Tachyon Setup: Telemetry for more details.

A TemporaryDirectory configuration setting has been added that can override the default location for 1E Client temporary file storage

Device information has been extended to include:

physical MAC address

inbound IP address (for NAT scenarios)

primary user (also displayed in Devices information popup from the Devices table in Explorer)

Support for VDI features (device resource demand reporting) - this is a preview feature that is not enabled by default.

New modules: Interaction

New methods: Security.QuarantineDevice, Security.ModifyQuarantineWhitelist, Users.GetPrimaryUser

Support added for following Operating Systems:

macOS – Catalina v10.15

CentOS 8.1

Debian 10.4

Fedora 32

openSUSE Leap 15.1

RHEL 8.1

SLES 15.1

Ubuntu 18.04

Only Tachyon client features are supported by the 1E Client on non-Windows devices.

2.6.4.2.4.1.2 Shopping client for Shopping v6.0

Shopping 6.0 client is the Shopping module in 1E Client 5.1

WSA - Support for nested Task Sequences

WSA - Autofill WiFi passcode on Connection page if available

WSA - Option to disable the Location page

2.6.4.2.4.1.3 WakeUp client for NightWatchman Enterprise v7.2.500 and v7.3

WakeUp 7.3 client is the WakeUp module in 1E Client 5.1

Creates a firewall exception for WakeUp with the name **1E Client (WakeUp)** that is port specific.

2.6.4.2.4.1.4 Nomad client for Nomad v7.0.200

NomadBranch 7.0.200 client is the Nomad module in 1E Client 5.1

Certificate-based client authentication for Nomad P2P communication

Configuration Manager Enhanced HTTP support

Support for multiple Certificate Authorities

Improved PKI client certificate selection logic

VMWare Workspace One support

Handling download content for "expired" offer

Improved handling of updated Software Update content

Option to reduce election notifications in Nomad logs

2.6.4.2.4.1.5 PXE client for PXE Everywhere v4.0

PXE Everywhere Agent 4.0 is a client module of 1E Client 5.1

PXE Everywhere Static Responder (to support DHCP Snooping) now has its own installer.

2.6.4.2.4.1.6 Contained fixes:

Q20741 - PXE Boot fails on Microsoft Surface Pro systems (TFS 195659)

Q21094 - Agent - Handle leak in ConvertNonStandardExecutableName (TFS 209269)

Q21092 - Agent - Infrastructure - Additional TachyonGUID/device generated if WMI is not available (TFS 207251)

Q21088 - Unable to download Pre-cache Content from Cloud DP on VPN clients (TFS 207646)

Q21070 - Add Shopping v6 Support to 1EClient (TFS 200984)

Q21060 - 1E Client (WakeUp) rule created multiple times in Windows Defender Firewall (TFS 201823)

Q21048 - CertIssuer - specifying issuer name sub string does not work for selecting Server Auth PKI cert for Nomad P2P / PBA over HTTPS (TFS 204608)

Q21020 - Support pre-caching on internet clients using AE on internet and content distributed on CDP or IBCM based DP. (TFS 203685)

Q21018 - Nomad failing to download the content in first attempt (from CMG) and succeeding in second attempt after 10 min (TFS 200803)

Q21004 - Agent - Experience - Operating System service failure - report the extra fields (TFS 200866)

Q21002 - Agent - Infrastructure - Reading output from child processes may fail (TFS 200539)

Q21000 - Agent - Experience - Better INFO logging and log ERROR if PdhOpenQuery() fails (TFS 200100)

Q20998 - Agent - Experience - .tmp files are being reported under Software->Product and Executable column (TFS 200571)

Q20996 - Agent - Experience - Client should report Processor queue length averaged across number of cores (TFS 200097)

Q20972 - Nomad fails a download when similar expired deployment is present (TFS 172581)

Q20970 - Nomad Task Sequence steps fail if Nomad module is not initialized (TFS 197292)

Q20968 - If using SMB to download content from DP in WinPE, the login to the DP share failed and Nomad failed to download the content. (TFS 200073)

Q20966 - The Pre-stage Content Using Nomad step failed to download content over SMB if the SMB path had a backslash at the end (TFS 199950)

Q20964 - If enhanced http was enabled, the Pre-stage Content Using Nomad step failed to download the content. (TFS 200380)

2.6.4.2.5 Web Release-5.0 (19-Mar-2020)

2.6.4.2.5.1 1E Client 5.0.0.745 - 1E Client Non-Windows 5.0.0.745 - 1E Client Android 5.0.0.745 - TIMS 5.0.0.745

2.6.4.2.5.1.1 Tachyon client for Tachyon v5.0

Uses OpenSSL 1.1.1c for secure communication with the Switch and Background Channel

Tachyon.Performance.Metrics.exe is now included in the 1E Client, previously included in the Windows Endpoint Performance Integrated Product pack

Tachyon activity record and storage features enhanced to include:

Software Performance

Operating System Performance

Performance data

New modules: Http.post, Device.GetLocation, Device.SetLocation

Now uses SQLite 1.29.0

Windows support confirmed for Windows 10 1909

Non-Windows now supports Red Hat v8.0 and v6.0

MacOS now supports Catalina 10.15.1

2.6.4.2.5.1.2 Shopping client for Shopping v5.6

Shopping 5.6 client is the Shopping module in 1E Client 5.0

No changes - only hotfixes

2.6.4.2.5.1.3 WakeUp client for NightWatchman Enterprise v7.2.500 and v7.3

WakeUp 7.3 client is the WakeUp module in 1E Client 5.0

Now creates WakeUp firewall exception with name '1E Client (WakeUp)' and it's now port specific.

2.6.4.2.5.1.4 Nomad client for Nomad v7.0.100

NomadBranch 7.0.100 client is the Nomad module in 1E Client 5.0

No changes - only hotfixes.

2.6.4.2.5.1.5 Contained fixes:

Q20775 - Agent - GetInboundMappedDriveHistory default columns does not contain 'Port' (TFS 198528)

Q20773 - Agent - Some patches pending reboot have a GUID but no KB ID or Title. (TFS 198284)

Q20739 - WakeUp - Improved logging for WakeUpAgt.exe at debug level (TFS 195904)

Q20737 - Tachyon - Agent - Network.GetArpEntries() shows incorrect CIDR mask (TFS 195491)

Q20733 - Nomad local SSD is not working (TFS 192409)

Q20705 - WSA IPU doesn't fire Task Sequence after upgrade to SCCM 1906 (TFS 186332)

Q20694 - Nomad - when an LST is created for a cloud DP a zero byte file causes download failure (TFS 187014)

Q20682 - Nomad - LSZGEN fails on long file path with Nomad SECure enabled (TFS 187318)

Q20680 - Nomad - LSZGEN issues on DP when CACHEPATH installer property has no trailing backslash (TFS 187334)

Q20678 - Nomad - Physical path in the LSZFILES virtual directory in IIS is not updated when LocalCachePath is changes after installation (TFS 188203)

Q20676 - Nomad downloads previous version of content (TFS 145160)

Q20674 - Nomad - Captive Portal Web page (eg Logon Page from Public Wifi) may cause issues with Nomad Downloads (TFS 156478)

Q20672 - Nomad fails to download updated task sequence references with ConfigMgr Pre-download option (TFS 182309)

Q20670 - Nomad service failure on PBA host with hidden share enabled during PBA backup (TFS 169339)

Q20666 - Nomad - PBA Size estimation doesn't update TS progress bar (TFS 184347)

Q20664 - Nomad not failing package on CRC failure (TFS 136381)

Q20662 - Nomad Status Message Improvements (TFS 107195)

Q20660 - Nomad service may fail whilst running cachecleaner manually (TFS 164341)

Q20658 - Nomad - Unable to download 0365 updates with Nomad (TFS 159484)

Q20624 - WSA doesn't fire Task Sequence after upgrade to SCCM 1906 (TFS 186332)

Q20612 - WSA wireless check (Readiness check) fails if the device connects to both wired and wireless networks (TFS 185832)

Q20592 - Nomad - 1EClient Nomad Module's install fails if Windows Firewall service is disabled or in stopped state (TFS 185011)

Q20590 - Tachyon - Agent- Methods - FileSystem.GetVersionInfo should return data even if OriginalFileName is missing, and should return SuccessNoContent instead of an error if it fails (TFS 184879)

Q20588 - Tachyon - Agent - 1E Client service terminates unexpectedly after a Patch.Deploy failure response using SCCM (TFS 185003)

Q20586 - Tachyon - Agent - Patch.Deploy returns 2 rows on success and none on failure if the PatchSpec is a GUID (TFS 184668)

Q20558 - WSA support in a multi domain environment (TFS 182470)

Q20556 - Tachyon - Agent - exception in Patch.List() while awaiting a reboot to install patches (TFS 183650)

Q20506 - WSA support for FireFox in WSA-ServiceNow (TFS 176154)

Q20504 - WSA support for ServiceNow integration with WSA in Shopping (TFS 176084)

Q20502 - Tachyon - Agent - Initial policy evaluation should be asynchronous (TFS 180719)

Q20500 - Tachyon - Agent - Exclusivity control for Scripting.Run* and NativeServices.RunCommand methods (TFS 180718)

Q20498 - Tachyon - Agent - Reduce noisiness of logging when Nomad is used (TFS 180717)

Q20496 - Tachyon - Agent - Nomad download should check Tachyon Agent cache first (TFS 180714)

2.6.4.2.6 Web Release-4.1 (21-JUN-2019)

2.6.4.2.6.1 1E Client 4.1.0.267 - 1E Client Non-Windows 4.1.0.267 - 1E Client Android 4.1.0.267 - TIMS 4.1.0.267

Tachyon Agent renamed as 1E Client

Enhancements:

Optimize ProcessUsage Minutes storage

Improvements to 1E Client on macOS

Reading certificates from the macOS keystore

DMG file installations

Agent Historic Data Capture feature renamed as Tachyon Activity Record

WSA enhancements:

Applications page includes all installed, normalized applications

Allow conditional download of Windows 10 upgrade packages

Check Windows 10 version readiness checks before upgrading

Perform In-place Upgrade compatibility check in WSA readiness checks

Allow Windows Servicing Assistant to exclude user state migration

Required for environments where TLS 1.0 is disabled.

1E module library renamed as Nomad, replacing NomadBranch client, and extended to support Nomad 7.0

Nomad provides an efficient file transfer mechanism that integrates with Microsoft Systems Center Configuration Manager, providing a host of features that maximize download efficiency and minimize WAN link bandwidth usage, and reduction in the number of servers.

2.6.4.2.6.1.1 Contained fixes:

Q20428 - Tachyon - Device.GetOutboundPrinters() crashes when handling empty registry values (TFS 173720)

Q20390 - Nomad - Allow WSA to exclude data backup (TFS 129030)

Q20384 - Nomad - Cache cleaner unable to remove content when cache already exceeded configured size (TFS 164413)

Q20382 - Nomad O365 download from untrusted forest not using Network Access Account (NAA) (TFS 169177)

Q20368 - Nomad - Active Efficiency Web service logs exception if FQDN is missing from client data (TFS 165641)

Q20350 - Nomad - Same "disqualified" master keeps winning elections. (TFS 163708)

Q20322 - Nomad - Don't download content to USB if it's already in the Nomad cache (TFS 129581)

Q20314 - Nomad - HTTP Proxy causes failures while downloading from Windows Update (TFS 165017)

Q20310 - Nomad Service Failure while logging disqualification details (TFS 163707)

Q20266 - Nomad - SMSTSNomad fails if the Nomad service is slow to start (TFS 154961)

Q20262 - Nomad - NMDS ExtraReplyDelayMS setting capped at 5000 (TFS 154089)

Q20260 - Nomad download logs CopyLoopWait CopyError: Missing File(s) (TFS 127424)

Q20256 - Nomad failing to download SU from Cloud Distribution Points (TFS 154773)

Q20254 - Nomad - TLS 1.2 compliance testing and fixes for Nomad (TFS 151453)

Q20252 - Nomad - CTM DP order with neighboring boundary group DPs (TFS 153928)

Q20250 - Nomad O365 downloads fail when requested range does not exist. (TFS 151169)

Q20248 - Nomad - Active Efficiency Nomad sync is failing with a "Arithmetic overflow error converting expression to data type bigint." error (TFS 71746)

Q20246 - Nomad - Cannot download software updates from Windows Update (TFS 120735)

Q20198 - Nomad - LSZ downloads fail when package contains files with Unicode names. (TFS 154033)

Q20196 - Nomad - Ignore Local SSD if machine is in a NomadInhibitedSubnet (TFS 127086)

Q20194 - Nomad - SSD queries may connect on inhibited subnets if the master moves (TFS 131988)

Q20192 - Nomad - Active Efficiency experiencing database deadlocks at high utilization (TFS 135419)

Q20144 - Nomad - Express Update support for Nomad (from on premises DP) (TFS 146643)

Q20142 - Nomad - RDC doesn't work in some cases (TFS 145476)

Q20138 - Nomad - SMSTSNomad does not set cache priority correctly (TFS 131034)

Q20136 - Nomad - Issues working Nomad HTTP with WINHTTP Proxy (TFS 125541)

Q20134 - Nomad - Disqualifications sent when too many connections reached over HTTP(S) (TFS 129719)

Q20132 - Nomad - Slow Nomad downloads from DP when BranchCache is enabled (TFS 109497)

Q20130 - NomadBranch Range Overlap Exception (TFS 116165)

Q20128 - Nomad Not Sending Error Status Messages (TFS 102476)

Q20056 - NomadBranch fails on NMDS_FIND HTTPPull when trying to restore a PBA user state backup; (TFS 143320)

2.6.4.3 1E Client features by release

A list of features organized by the release they were implemented in. Links through to the features have been provided for convenience.

Each release includes new or enhanced functions and methods in the Agent language (SCALE). Please refer to Tachyon SDK - Functions and Methods Reference for more details.

2.6.4.3.1 New features in 1E Client 8.1

2.6.4.3.1.1 Tachyon client for Tachyon v8.1

The status of all Guaranteed State rules is reported after a configurable number of days, even if the rule status has not changed

New module called Policy to give better visibility into what the current status of Guaranteed State rules:

/document/preview/739118#UUID-1de33ffb-d4e6-aab8-88c6-4bbfbd5b7034_id_PolicyForceStatusReport-ForceStatusReport - trigger the 1E Client to force-send all policy status messages on restart

/document/preview/739119#UUID-dbc9eec3-1781-f814-2efa-8af6b0fc1a2b_id_PolicyGetEventSubscriptions-GetEventSubscriptions - get event subscriptions in current policy

/document/preview/739120#UUID-f0f824b7-163a-72e0-2c9c-6cd39f7a0f05_id_PolicyGetRuleEvaluationHistory-GetRuleEvaluationHistory ([ruleId]) - get the evaluation history for one rule or all rules

/document/preview/739121#UUID-b55da451-c425-a143-6e01-37f100c0b543_id_PolicyGetRules-GetRules - get rules in current policy (with current status)

/document/preview/739122#UUID-daf92ecb-8959-48fc-1b3e-fd6e9a7abd3b_id_PolicyGetStatistics-GetStatistics - get policy-related statistics/perf counters

/document/preview/739123#UUID-d5b70c1f-8194-d25e-337b-f1ce3cbc8a3e_id_PolicyGetSummary-GetSummary - get a summary of the current policy

Policy.Invalidate () - reset the 1E Client's policy to null/empty, which will force a renegotiation of the policy (immediately if connected to Switch, or when it does eventually connect)

New methods:

/document/preview/739176#UUID-65c8a3bf-3714-442a-4c5c-19b77d5e93af_id_StorageList-Delete

New SQL functions:

/document/preview/739230#UUID-4fd278df-907a-b131-c131-e2449af777af_id_HASHSTRING-HASHSTRING, /document/preview/739234#UUID-3d29f21e-8d41-cc2a-e2cd-efc8f7639fe8_id_NEWID-NEWID

Deprecated methods: FileContent.GetTorrentAnnounceUris, FileContent.GetTorrentDescribedFiles, FileContent.GetTorrentInfo

Support for Solaris operating systems has been deprecated

Will not install on Windows XP and Server 2003

Now uses C++ 14, OpenSSL 3.0.0 7 Sep 2021, SQLite 3.36.0

Note

Only Tachyon client features are supported by the 1E Client on non-Windows devices.

2.6.4.3.1.2 Shopping client for Shopping v6.1

Shopping 6.1 client is the Shopping module in 1E Client 8.1

No changes - only hotfixes.

2.6.4.3.1.3 WakeUp client for NightWatchman Enterprise v7.3

WakeUp 7.3 client is the WakeUp module in 1E Client 8.1

No changes - only hotfixes.

2.6.4.3.1.4 Content Distribution client for Content Distribution v8.1

NomadBranch 8.1 client is the Content Distribution module in 1E Client 8.1

Set Nomad as Download Program - cloud-based services to support Work From Anywhere (WFA) users are becoming more critical to the way enterprises work, there is an increased reliance on Cloud Distribution Points for distributing content.

Enhancements:

Improvements to the Client authentication criteria to authenticate with a DP (or any download source)

Download reporting now includes Top status bar, for Bandwdith Protection Reporting.

2.6.4.3.1.5 PXE client for PXE Everywhere v8.1

PXE Everywhere Agent is a client module of 1E Client 8.1, available for x64 and x86 platforms

There are no other changes in this version other than hotfixes.

2.6.4.3.1.6 Tachyon Instruction Management Studio (TIMS) v8.1

For more information about TIMS, please refer to Tachyon SDK - Getting started with TIMS.

No changes - only hotfixes.

2.6.4.3.2 1E Client 8.0

2.6.4.3.2.1 Tachyon client for Tachyon v8.0

Real-Time Control Center - updated Client UI in notification area to support Experience Engagements (Announcements and Surveys), and ITSM Support Tickets

New methods:

Device.GetDisks, FileSystem.PathExists, Interaction.ShowAnnouncement, Storage.GetRemote

Updated methods:

Agent.GetDiagnostics, Network.GetIpAddresses, OperatingSystem.ControlService, OperatingSystem.GetProcesses, NativeServices.RunWmiInstanceMethod, NativeServices.RunWmiQuery, NativeServices.RunWmiStaticMethod, Security.UnquarantineDevice, Storage.Set

New capture sources for Tachyon Activity Record:

BootPerformance, SoftwarePerformance.DiskUsage, SoftwarePerformance.ProcessNetworkUsage

Support for the SQLite JSON extension (), allowing JSON data to be queried through SCALE

TAGS installer property for Windows devices - see Tachyon client settings

Support added for the following Operating Systems:

Windows 10 21H1

Fedora 34

openSUSE Leap 15.2

Red Hat Enterprise Linux 7.9

Red Hat Enterprise Linux 8.3

SUSE Linux Enterprise 15.2

> **Note**
>
> Only Tachyon client features are supported by the 1E Client on non-Windows devices.

2.6.4.3.2.2 Shopping client for Shopping v6.1

Shopping 6.1 client is the Shopping module in 1E Client 8.0

Client-side Order Tracking feature - configurable on the Shopping server - to provide toast notifications and 1E Shopping UI popup in the notification area.

2.6.4.3.2.3 WakeUp client for NightWatchman Enterprise v7.3

WakeUp 7.3 client is the WakeUp module in 1E Client 8.0

No changes - only hotfixes.

2.6.4.3.2.4 Nomad client for Nomad v8.0

NomadBranch 8.0 client is the Nomad module in 1E Client 8.0

New registry setting SiteSSDMinPackageSizeKB to set the minimum size of content before making SSD request

Installer changes:

Integrating Nomad with WakeUp

Enable Nomad FanOut as a default - default value of SpecialNetShare has changed to 0x2060 (8288)

Platform features enabled by using the BackgroundChannelUrl instead of PlatformURL

Enhancements to CacheCleaner functionality to better support remote users as part of the Working From Anywhere initiative.

2.6.4.3.2.5 PXE client for PXE Everywhere v8.0

PXE Everywhere Agent is a client module of 1E Client 8.0, available for x64 and x86 platforms

Bootshim.efi folder renamed from **BootPrograms** to **NetworkBootPrograms** (1E\Client\Extensibility\PXEEverywhere\NetworkBootPrograms)

There are no other changes in this version other than hotfixes.

2.6.4.3.3 1E Client 5.2

2.6.4.3.3.1 Tachyon client for Tachyon v5.2

New methods: Inventory.GetTables, Network.GetWiFiNetworks

Updated methods: Network.GetConnections, OperatingSystem.GetSummary

New TimeoutSecs parameter in: FileSystem.FindFileByName, FileSystem.FindFileBySizeAndHash, FileSystem.FindDirectoryByName

New policy trigger: DirectoryChange

New installer property for Windows devices: DataRoot

Support for TPM (Trusted Platform Module) based client certificates on Windows

OsLocale and OSInstallUtc included in online messages to Switch to support the Location tile in the Details panel of Tachyon Platform 5.2 - Device View: Overview

Support for Nomad client changes, including use of event policy system, and sharing certificate details

Improved Downloading Tachyon client content and Nomad integration

Description removed from Experience Surveys in Client UI (Interaction module)

Additional installation script for deploying client on macOS when using tachyon.pfx certificate file as an alternative to using the macOS key store

Support added for following Operating Systems:

Windows 10-20H2

macOS on Apple M1 architecture.

> **Note**
>
> Only Tachyon client features are supported by the 1E Client on non-Windows devices.

2.6.4.3.3.2 Shopping client for Shopping v6.0

Shopping 6.0 client is the Shopping module in 1E Client 5.2

Adding support for Single sign-on (SSO) environment and Workgroup devices to respond with machine details on Shopping website.

2.6.4.3.3.3 WakeUp client for NightWatchman Enterprise v7.3

WakeUp 7.3 client is the WakeUp module in 1E Client 5.2

No changes - only hotfixes.

2.6.4.3.3.4 Nomad client for Nomad v7.1

NomadBranch 7.1 client is the Nomad module in 1E Client 5.2

ActiveEfficiency features are now provided by Content Distribution on Tachyon Platform 5.2

Client status messages are sent via Tachyon event policy system - Content Distribution uses these instead of StatusMsgEvents using Configuration Manager

New client settings:

DeliveryOptimizationReportingEnabled - monitoring of Delivery Optimization downloads and reporting them to Content Distribution - disabled by default

SupportWPAD - provides support for Web Proxy Auto-Discovery Protocol (WPAD) - disabled by default.

2.6.4.3.3.5 PXE client for PXE Everywhere v4.0.100

PXE Everywhere Agent 4.0.100 is the PXE Everywhere module in 1E Client 5.2

No changes - only hotfixes.

2.6.4.3.3.6 Tachyon Instruction Management Studio (TIMS) v5.2

For more information about TIMS, please refer to Tachyon SDK - Getting started with TIMS.

Multiple tabs

Default instruction type for a new instruction is now Action rather than Question

Validation error when %global% or %environment% variables are used in fragments (InstructionType fix, check, and precondition).

2.6.4.3.4 1E Client 5.1

2.6.4.3.4.1 Tachyon client for Tachyon v5.1

User surveys and notifications, and notification area icon called 1E Client UI. This is used by Tachyon Experience, please refer to:

Tachyon Experience 1.3 - Getting feedback via User Sentiment Surveys: What the end-user sees

Tachyon Experience 1.3 - Getting feedback via General Purpose Surveys: What the end-user sees

Tachyon Experience 1.3 - Getting feedback via General Purpose Surveys: Do not disturb...

Support for user-centric features (user session reporting). This is used by Tachyon Experience, please refer to Tachyon Experience.

Support for Telemetry. Please refer to Tachyon 5.2 - Telemetry data and Tachyon 5.2 - Tachyon Setup: Telemetry for more details.

A TemporaryDirectory configuration setting has been added that can override the default location for 1E Client temporary file storage

Device information has been extended to include:

physical MAC address

inbound IP address (for NAT scenarios)

primary user (also displayed in Devices information popup from the Devices table in Explorer).

Support for VDI features (device resource demand reporting) - this is a preview feature that is not enabled by default.

New modules: Interaction

New methods: Security.QuarantineDevice, Security.ModifyQuarantineWhitelist, Users.GetPrimaryUser

Support added for following Operating Systems:

macOS – Catalina v10.15

CentOS 8.1

Debian 10.4

Fedora 32

openSUSE Leap 15.1

RHEL 8.1

SLES 15.1

Ubuntu 18.04

Note

Only Tachyon client features are supported by the 1E Client on non-Windows devices.

2.6.4.3.4.2 Shopping client for Shopping v6.0

Shopping 6.0 client is the Shopping module in 1E Client 5.1

WSA - Support for nested Task Sequences

WSA - Autofill WiFi passcode on Connection page if available

WSA - Option to disable the Location page

2.6.4.3.4.3 WakeUp client for NightWatchman Enterprise v7.2.500 and v7.3

WakeUp 7.3 client is the WakeUp module in 1E Client 5.1

Creates a firewall exception for WakeUp with the name **1E Client (WakeUp)** that is port specific.

2.6.4.3.4.4 Nomad client for Nomad v7.0.200

NomadBranch 7.0.200 client is the Nomad module in 1E Client 5.1

Certificate-based client authentication for Nomad P2P communication

Configuration Manager Enhanced HTTP support

Support for multiple Certificate Authorities

Improved PKI client certificate selection logic

VMWare Workspace One support

Handling download content for "expired" offer

Improved handling of updated Software Update content

Option to reduce election notifications in Nomad logs

2.6.4.3.4.5 PXE client for PXE Everywhere v4.0

PXE Everywhere Agent 4.0 is a client module of 1E Client 5.1

PXE Everywhere Static Responder (to support DHCP Snooping) now has its own installer.

2.6.4.3.5 1E Client 5.0

2.6.4.3.5.1 Tachyon client for Tachyon v5.0

Uses OpenSSL 1.1.1c for secure communication with the Switch and Background Channel

Tachyon.Performance.Metrics.exe is now included in the 1E Client, previously included in the Windows Endpoint Performance Integrated Product pack

Tachyon activity record and storage features enhanced to include:

Software Performance

Operating System Performance

Performance data

New modules: Http.post, Device.GetLocation, Device.SetLocation

Now uses SQLite 1.29.0

Windows support confirmed for Windows 10 1909

Non-Windows now supports Red Hat v8.0 and v6.0

MacOS now supports Catalina 10.15.1

2.6.4.3.5.2 Shopping client for Shopping v5.6

Shopping 5.6 client is the Shopping module in 1E Client 5.0

No changes - only hotfixes

2.6.4.3.5.3 WakeUp client for NightWatchman Enterprise v7.2.500 and v7.3

WakeUp 7.3 client is the WakeUp module in 1E Client 5.0

Now creates WakeUp firewall exception with name '1E Client (WakeUp)' and it's now port specific.

2.6.4.3.5.4 Nomad client for Nomad v7.0.100

NomadBranch 7.0.100 client is the Nomad module in 1E Client 5.0

No changes - only hotfixes.

2.6.4.3.6 1E Client 4.1

Tachyon Agent renamed as 1E Client

Enhancements:

Optimize ProcessUsage Minutes storage

Improvements to 1E Client on macOS

Reading certificates from the macOS keystore

DMG file installations

Agent Historic Data Capture feature renamed as Tachyon Activity Record

WSA enhancements:

Applications page includes all installed, normalized applications

Allow conditional download of Windows 10 upgrade packages

Check Windows 10 version readiness checks before upgrading

Perform In-place Upgrade compatibility check in WSA readiness checks

Allow Windows Servicing Assistant to exclude user state migration

Required for environments where TLS 1.0 is disabled.

1E module library renamed as Nomad, replacing NomadBranch client, and extended to support Nomad 7.0

Nomad provides an efficient file transfer mechanism that integrates with Microsoft Systems Center Configuration Manager, providing a host of features that maximize download efficiency and minimize WAN link bandwidth usage, and reduction in the number of servers.

3 1E Client Deployment Assistant

1E Client Deployment Assistant (CDA) is a wizard that assists with deployment of 1E Client, guiding you through common settings for clients and deployments.

3.1 Introducing 1E Client Deployment Assistant

1E Client Deployment Assistant (CDA) is a wizard that assists with deployment of 1E clients, guiding you through common settings for clients and deployments.

CDA is available as a zip file which you can download from support.1e.com/ .

You use the wizard to do the following:

Create a MST transform file for each MSI containing your chosen settings

Create a text file that contains the command-line for deploying each MSI

Optionally allow deployment of an MSP patch file for each MSI

Optionally connect to Microsoft Endpoint Configuration Manager to:

Create applications and packages

Create deployments and collections for the applications

Distribute source files to Distribution Points.

The wizard creates an answer file which records the chosen settings (the wizard uses a template answer file which controls the default settings seen in the wizard).

You can download the latest Accumulated Hotfix MSP for each client, from the 1E Support Portal. The zip that you download may already contain an MSP file for each client. You should remove this if you have alternate methods of deploying patches.

If you are using Configuration Manager, you must run the wizard on a computer that has the Configuration Manager console installed. Windows ADK (with WinPE add-on) is also required locally if CDA is used to configure a deployment of PXE Everywhere .

To start the wizard, run **1EClientDeploymentAssistant.exe** (using Run as Administrator) which prompts for the following:

Connection to a local or remote Configuration Manager site server

The URLs of Configuration Manager application and package content shares where source files must be copied to.

1E Client Deployment Assistant 8.1 contains the following product versions:

1E Client 8.1.2.62 (includes modules for Nomad , PXE Everywhere , Shopping/WSA , WakeUp)

1E NightWatchman Agent 7.3.0.774

3.2 Implementing

Everything you need to know and things to consider when you deploy the 1E Client using the CDA.

3.2.1 Preparation

A list of requirements and preparation steps before Running the wizard.

3.2.1.1 Download the 1E Client Deployment Assistant

Download the **1EClientDeploymentAssistant.v9.0.x.x.zip** from the https://support.1e.com/ .

When you unzip the file, the contents of the folder are:

1E Client Deployment Assistant Release Information.html

1E_License_Agreement.rtf - the text for the 1E license agreement displayed in the CDA wizard

1EClientDeploymentAssistant.exe - executable that runs the CDA wizard

1EClientDeploymentAssistant.exe.config - configuration file for the executable, mainly used for debugging

1EClientDeploymentAssistantWizard.dll - library supporting the executable

AppImport.xml - the answer file that provides default settings for clients and deployments

GenerateMST.exe - creates MST transform files for the installers

GenerateMST.exe.config - controls the behavior of the GenerateMST.exe application

licenses.txt - edit this file if you want to provide default values for the clients that require licensing (required only for 1E NightWatchman Agent)

Microsoft.Deployment.Compression.Cab.dll - WiX tool used to create the .cab files

Microsoft.Deployment.Compression.dll - WiX tool used to create the .cab files

SACommon.dll - common utilities used in the solution accelerators

Wix Toolset source.zip - files related to the Wix toolkit

The zip file also contains the following folders:

Agent Installation Files - contains the client **.msi** installer files, **.msp** accumulated hotfix files, and base **.mst** transform files

Images - contains Client Deployment Assistant.png

> **Note**
>
> In this documentation, Configuration Manager (CM) means either Microsoft Endpoint Configuration Manager (MECM), or its predecessor Microsoft System Center Configuration Manager (SCCM).

3.2.1.2 To run CDA

3.2.1.2.1 Host computer

The host computer used to run the CDA wizard can be the Configuration Manager site server or another computer that has the following installed:

Configuration Manager console

Microsoft ADK with WinPE addon - only if the CDA wizard is used to create PXE Everywhere applications

It will need to have .Net Framework v4.8 Runtime installed, a check when the wizard runs checks for this being installed, and will if not already installed, provide a link to https://dotnet.microsoft.com/en-us/download/dotnet-framework/net48?cid=getdotnetframework where you will need to download and run the .Net Framework v4.8 Runtime. The link is provided should you wish to install this prior to running the wizard. The installation does require a reboot to complete.

If you are installing PXE Everywhere you must install the **Deployment Tools** feature from the Microsoft Assessment and Deployment Kit (ADK), and the **WinPE addon**. The user running the CDA wizard must have local administrator privileges because the CDA wizard uses *dism.exe* to mount a PXE *.wim* file in order to extract boot image files. Start the wizard using Run as Administrator.

> **Note**
>
> To download and install the Windows ADK go to https://docs.microsoft.com/en-us/windows-hardware/get-started/adk-install. Starting with Windows 10, version 1809, WinPE is an add-

on to the ADK, previously it was included in the ADK. First install the ADK, and then install the WinPE addon. Approximately 7GB disk space is required.

3.2.1.2.2 Domain Accounts

Installer account - used to run the CDA wizard on the host computer, must have local administrator rights on the host computer. If you run the CDA wizard on the Configuration Manager site server, the installer account must also have at least the Application Administrator role in Configuration Manager. Start the wizard using Run as Administrator.

Configuration Manager user - If you run the CDA wizard on a remote computer (other than the Configuration Manager site server), you must specify the user account that will create objects in Configuration Manager. This can be the same as the Installer account or any other domain user account that has at least an Application Administrator role in Configuration Manager

If the **Installer account** and **Configuration Manager user** are different accounts then you must specify the **Configuration Manager user** in the Configuration Manager connection screen.

3.2.1.2.3 Configuration Manager site

Connection to a Configuration Manager site is required even if you only want to use the CDA wizard to create the MST transform files. The site must have software distribution features enabled.

> **Tip**
>
> CDA helps create everything you need to deploy clients and agents in your Configuration Manager environment. If you prefer, you can use CDA in a lab or other environment to create the Configuration Manager application and/or package content (including MST transform files). Then you can copy the content to your production environment and manually create your deployments.
>
> If you don't want CDA to create objects in Configuration Manager then you can use Microsoft's Orca to edit the base MST transform files supplied with CDA, and manually create your deployments.
>
> Orca is a Microsoft tool for creating and editing Windows Installer packages (MSI) and merging modules (MST transforms). It is available from the Windows Installer Development Tools - https://docs.microsoft.com/en-us/windows/desktop/msi/orca-exe.

3.2.1.2.4 Application and Package content source shares

The CDA wizard requires you to specify share names that Configuration Manager uses as application and package content source shares. The CDA wizard creates folders in each share and copies files to them, and Configuration Manager will copy the files and distribute them to Distribution Points. Typically, you will already have these shares, or you can create new ones.

Each content source share must have at least the following share permissions and NTFS security:

Read access by the Configuration Manager site server computer$ account

Write access by the installer account used to run the CDA wizard.

The UNC of each content source share must be provided in the General settings screen. For example, your applications UNC may be: *\\acme-server\dsl$\Applications* and your packages UNC may be: *\\acme-server\dsl$\Packages*.

3.2.1.2.5 Configuration Manager Distribution Point Group

You must have at least one **Distribution Point Group** defined in Configuration Manager if you want to enable the **Distribute Content** option in the General settings screen. This option causes Configuration Manager to distribute application and package source to the Distribution Points after the wizard has been run.

3.2.1.3 Licenses.txt file

A license file is required to run CDA, even if it has incorrect license keys. A default file is supplied in the release root folder which can be modified to include your own license key(s), which is useful if you don't want to type them manually each time you run CDA.

At this time a license key is only required for **1E NightWatchman Agent**, therefore if you are not using the Agent then please use the default file.

The file format is a simple name=value pair with one license per line where the name is the name of the application as it appears in the answer file. For example, the contents of the file will look like this:

```
1E NightWatchman Agent=ACMEXX-5555-6666-JKLM-NOPQ
```

You must update this file if you intend to use the CDA wizard in unattended mode.

If the license file does not exist or if you have not updated it with the license for a particular client agent, you will need to manually type the license key into the **Agent selection** screen in the CDA wizard.

> **Note**
>
> 1E license keys have the format: <name>-<4Chars>-<4Chars>-<4Chars>-<4Chars>
>
> A license key may be reported as invalid if hyphens or other characters have been converted into symbols or Unicode, which can happen if copy+pasted.

> **Note**
>
> 1E Client does not have a license key. Even so, you must adhere to the terms of your license agreement.

3.2.1.4 Infrastructure requirements

When using the CDA wizard you will be required to enter details of your server infrastructure. The following table describes the server infrastructure required if you intend to deploy the corresponding clients or agents.

Server	Used by	Requirements
Tachyon Platform	Tachyon and other client settings Nomad client settings	If you intend to use Tachyon, the Tachyon client screen in the CDA wizard requires details of the Tachyon **Switch** and **Background Channel**. These are normally installed on a single Tachyon server and therefore use the same **DNS Name**. Large environments (over 50,000) may have a Tachyon **Master Stack** server and one or more separate **Response Stack** servers. These may share the same **DNS Name** or have different **DNS Names**. The names required by the Tachyon client screen will depend on the design of your Tachyon system. The Tachyon Master Stack server requires a license obtained from 1E, but details of this are not required by the CDA wizard. For 1E Client 5.2 onwards, Nomad client uses the Content Distribution feature of Tachyon platform, which replaces ActiveEfficiency Server used by earlier versions of Nomad client. You must enable the client if you want Nomad to use any of the following Nomad features. Although not a requirement for generally using Nomad, Tachyon platform must be installed and available before you can use certain Nomad features. The following Nomad features use Content Distribution and require Tachyon platform and Tachyon features of 1E Client to be enabled: Nomad app provides visibility of content distribution activity Single Site Download (SSD) (SSD) Single Site PBA (SSPBA) High Availability PBA (HAPBA) (HAPBA) Get Migration Settings task sequence action used to manage computer associations Nomad Pre-caching Nomad Download Pause.

Server	Used by	Requirements
		The following features were provided in versions of Nomad older than 7.1: 1E Client Health - now provided by the Guaranteed State feature of the Tachyon platform Nomad Dashboard - now provided by Nomad app feature of the Tachyon platform. Nomad can also be used to provide content distribution features for clients, as well as Configuration Manager.
PXE Everywhere Central	PXE Everywhere settings	The CDA wizard requires the URL of the PXE Everywhere Central web service when deploying PXE Everywhere Local client. PXE Everywhere Central is installed on a Configuration Manager Site server, or other Windows server.
NightWatchman Management Center	Tachyon and other client settings 1E NightWatchman Agent settings	NightWatchman Management Center server is required if implementing NightWatchman or WakeUp solutions. The CDA wizard requires the name of the NightWatchman web server (specifically the web server hosting the AFWebService).
WakeUp Server	Tachyon and other client settings	If implementing WakeUp, or Nomad integration with WakeUp, then you require a WakeUp Server. If you have Configuration Manager, you require a WakeUp Server on each Site server that has clients reporting into it. If you do not have Configuration Manager, you require one or more independent WakeUp Servers. Ideally, you would install the WakeUp Server before deploying the 1E Client with the WakeUp client module enabled, but that is not a prerequisite for using the CDA wizard.
Shopping Central	Tachyon and other client settings	The CDA wizard requires the URL of the Shopping Central self-service portal when configuring the Shopping client module of the 1E Client. A Shopping solution requires a Shopping Central server on a web server, and a Shopping Receiver installed on each Configuration Manager Site

Server	Used by	Requirements
		server that has a client reporting to it, and on a CAS if using Shopping for OS Deployment. You can deploy the 1E Client without Tachyon servers or Tachyon license. If users are using Edge or Metro browsers, then you must enable the loopback feature option in the CDA wizard. This feature implements a mechanism for passing information between the Shopping client, the browser's secure sandboxed environment and the local machine. This mechanism affects these browsers as a whole and is not just restricted for use by Shopping. **Note** Before enabling the **Edge/Windows App browser support** option, check your security policy on enabling loopback and be aware of the implications of allowing access between browsers and the local machine.

3.2.1.5 Configuration Manager objects

For each 1E Client, the CDA wizard allows you to choose whether to create the following objects in Configuration Manager:

Application and Deployment Type

Package and Program

Device Collection and Deployment for the Application(these are not created for packages, because packages are generally used only in Task Sequences).

Please refer to Configuration Manager objects for more detail on these objects.

Each 1E Client agent has **Specify application and/or package information** screen with the following options:

Installation Files Directory	Mandatory	Tells the CDA wizard where to locate the 1E Client source files that you extracted when you unzipped the 1E Client Deployment Assistant (CDA) files. These are used to create Configuration Manager applications and packages.
Create Application	Optional	Determines if an application for the client is created in Configuration Manager.

		You must check **Create Application** and/or **Create Package** option to enable and click on the **Next** button. If this option is not checked, then the CDA Wizard will not copy files and create an MST transform in the **Application Content Source** specified in the General settings screen.
Create Application Deployment	Optional	Only enabled if you choose **Create Application** and determine whether a required deployment type for the application is created in Configuration Manager.
Create/Select Device Collection	Mandatory if **Create Application Deployment** is enabled	The device collection is used to deploy the application. If specified, then the CDA wizard will also create a deployment for the application's deployment types and the specified collection. A default name is suggested, which you can change. If the name you entered for **Create/Select Device Collection** does not exist, one is created. You must manually populate the created device collection after running the CDA wizard. You can click **Browse** to choose from a list of existing collections that you have access to using Configuration Manager RBAC. If you do this, you will not have the option to associate the device collection with a **Limiting Collection**.
Limiting Collection	Mandatory if **Create Application Deployment** is enabled	If you are creating a new device collection, you must also choose an associated **Limiting Collection**. This limits administrators to populating the new device collection with devices only from the selected **Limiting Collection**. By default, this is **All Systems**, but you can click **Browse** to choose from a list of existing collections that you have access to using Configuration Manager RBAC.
Create Package	Optional	Determines if a legacy package and associated install and uninstall programs for the client are created in Configuration Manager.

You must check **Create Application** and/or **Create Package** options to enable and click on the **Next** button.

If this option is not checked, then the CDA wizard will not copy files and create an MST transform in the **Package Content Source** specified in the General settings screen.

> **Note**
>
> Packages are created primarily for use in Task Sequences, therefore the CDA wizard sets the **Allow this program to be installed from the Ins tall Package task sequence without being depl oyed** property, and does not create collections or deployments.
>
> Do not use this option unless you require a package to be created. You can re-run CDA wizard later to create one if required.

3.2.2 Running the wizard

Steps for running the CDA wizard interactively, with details of common deployment and configuration options for each client agent.

1E Client Deployment Assistant 8.1 creates objects for the following 1E products:

1E Client 8.1.2.62 (includes modules for Nomad , PXE Everywhere, Shopping/WSA, WakeUp)

1E NightWatchman Agent 7.3.0.774

Before you run the CDA wizard, ensure you have reviewed the requirements and completed the preparation steps listed on the Preparation page.

3.2.2.1 Running the wizard in interactive mode

3.2.2.1.1 Start

Start the wizard using **Run as administrator**.

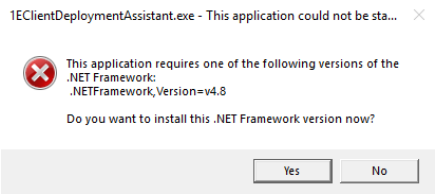
In the folder where you unzipped the 1E Client Deployment Assistant, right-click **1EClientDeploymentAssistant.exe** and from the context menu, choose **Run as administrator**.

If you do not already have .NET Framework v4.8 Runtime installed on the device before the Welcome screen is displayed, a popup is displayed prompting you to install the .NET Framework. This takes you to the https://dotnet.microsoft.com/en-us/download/dotnet-framework/net48?cid=getdotnetframework page where you should download and run the .Net Framework v4.8 Runtime. You must reboot after after installation, after which you can restart the 1E Client Deployment Assistant.

.NET Framework v4.8 is required by:

1E Client Deployment Assistant

1E Client.

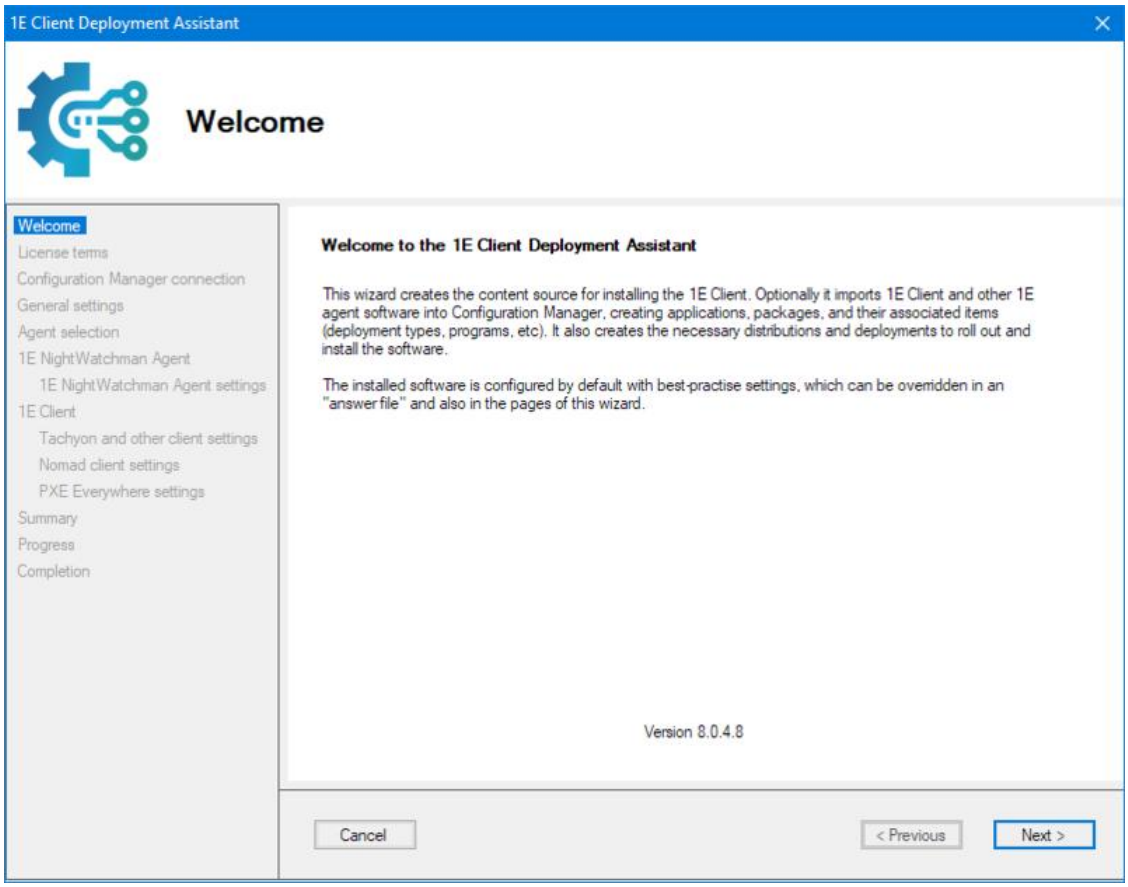


Note

The pictures on this page may not show the latest versions of 1E products.

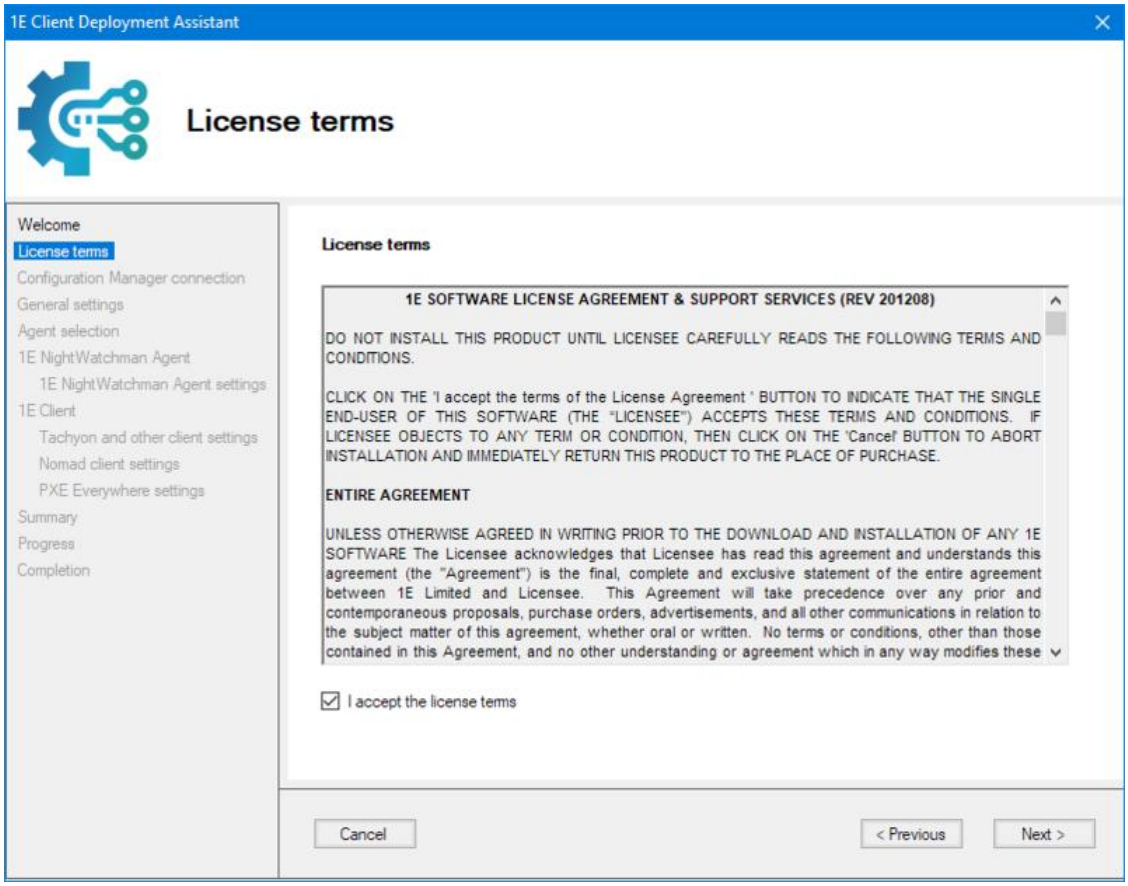
3.2.2.1.2 Welcome

On the **Welcome** screen click **Next**.



3.2.2.1.3 License terms

Check **I accept the license terms** and click **Next**.



3.2.2.1.4 Configuration Manager connection

Choose the Configuration Manager site server to connect to:

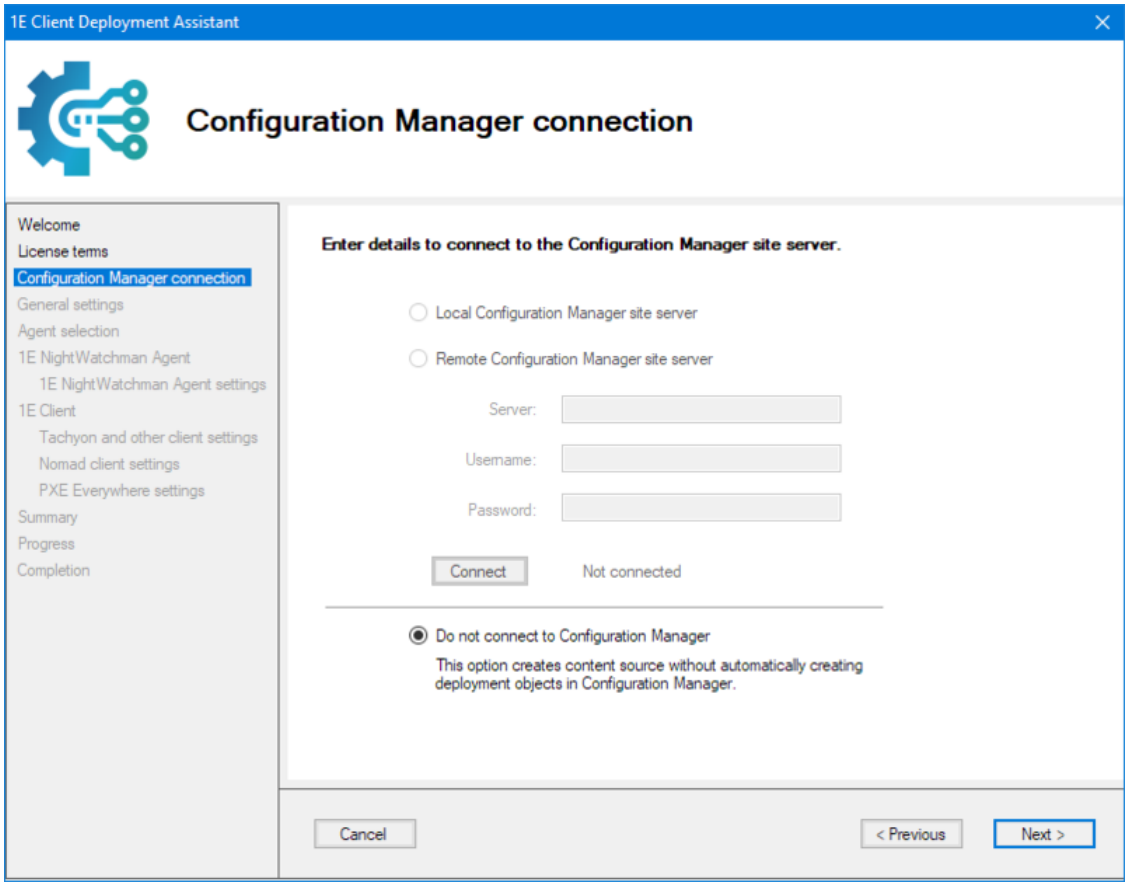
Local Configuration Manager Site Server – use this if the CDA wizard is being run on a Configuration Manager site server

Remote Configuration Manager Site Server – use this option to specify the location of a remote site server and the account used to authenticate the user

> **Note**
>
> If you have selected either of the above Configuration Manager options, click **Connect** and confirm **Connected**.
>
> To automatically create applications or packages in Configuration Manager, you must run CDA on site server or another computer that has the Configuration Manager console installed.

Do not connect to Configuration Manager- this option allows you to create content source without automatically creating deployment objects in Configuration Manager.

Click **Next**.



3.2.2.1.5 General settings

Review the following and click **Next** when completed.

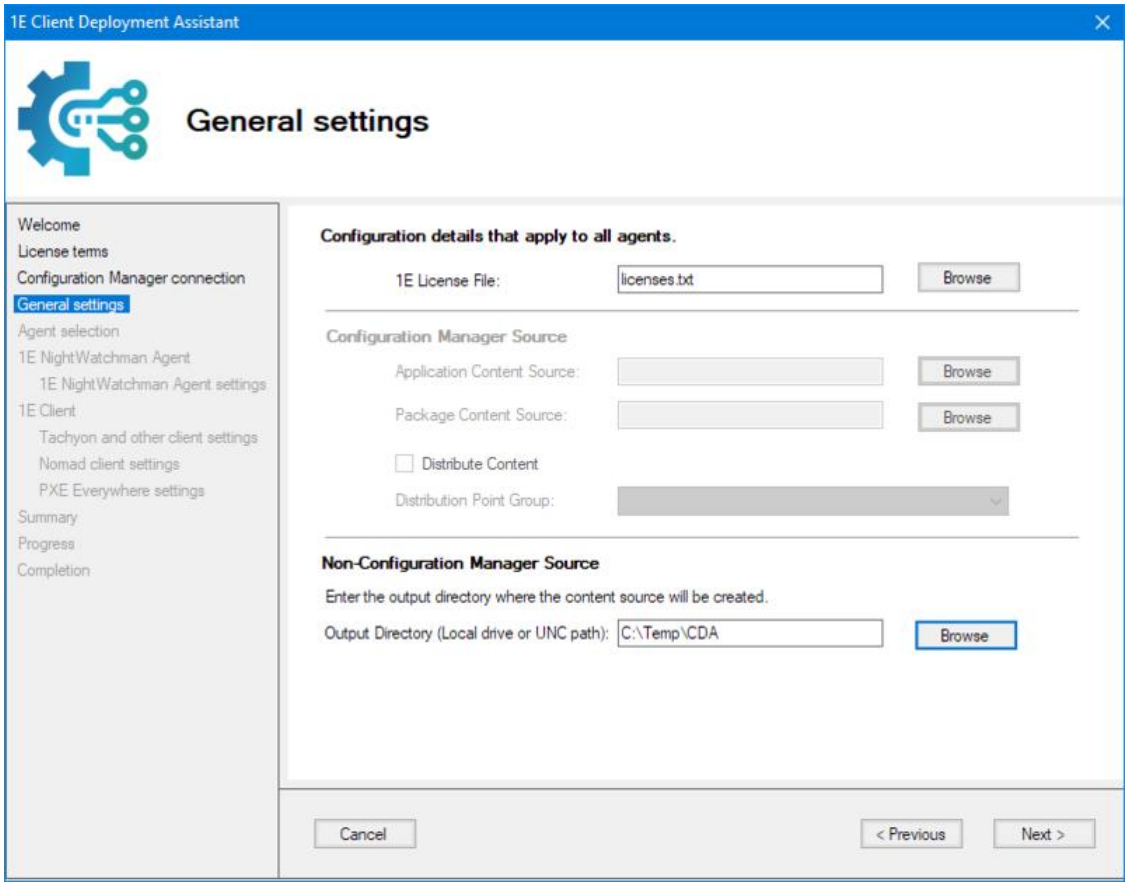
1E License File	Mandatory	If you wish to use a license file other than the default *license.txt* file, then select your own file by using the **Browse** button. A license file is required to run CDA, even if it has incorrect license keys. A default file is supplied in the release root folder which can be modified to include your own license key(s), which is useful if you don't want to type them manually each time you run CDA. At this time a license key is only required for **1E NightWatchman Agent**, therefore if you are not using the Agent then please use the default file.

		For guidance on how to add a license to the file, please see Licenses.txt file. **Warning** After you have moved to the Agent selection screen and the license keys have been validated, you cannot return to this screen and choose a different license file. You can either restart the CDA wizard and select the correct file, or manually enter new keys. The license file is ignored if the AppImport.xml answer file is pre-populated with license keys.
Application Content Source	Mandatory if using Configuration Manager	Enter the UNC of the Configuration Manager **Application Content Source** share where the wizard saves content source for use by Configuration Manager applications. The wizard will create 1E folders below it. For example, your applications UNC may be: `\\acme-server\dsl$\Applications`.
Package Content Source	Mandatory if using Configuration Manager	Enter the UNC of the Configuration Manager **Package Content Source** share where the wizard saves content source for use by Configuration Manager packages. The wizard will create 1E folders below it. For example, your packages UNC may be: `\\acme-server\dsl$\Packages`.
Distribute Content	Optional	Check this option if you want Configuration Manager to distribute application and package source to the distribution points after the wizard has been run. **Warning** Do not use this option if you need to add additional files to the application and/or package content, for example MST

		transform files based on the files created by the wizard as described in Advanced configuration. You will need to update the content and then manually instruct Configuration Manager to distribute. When enabled, a warning is displayed indicating **Distribution is enabled**, which can be helpful if this option had been enabled in the AppImport.xml answer file.
Distribution Point Group	Mandatory if **Distribute Content** is enabled.	Select a **Distribution Point Group**.
Output directory	Mandatory if not using Configuration Manager.	You can enter a local drive, or a UNC path of a network share, where the wizard will save the content source that will be created by the Wizard.

Note

In the previous version of CDA, this screen included a URL for the ActiveEfficiency Server, which was only used by Nomad. In this release instead, it uses Content Distribution, a component of the Tachyon platform. Therefore, ActiveEfficiency Server is no longer required, except as an optional component of a 1E Shopping solution, and there is no requirement to provide a URL.



3.2.2.1.6 Agent selection

Check each of the clients and agents you want to deploy and then click Next.

If you have not already added your NightWatchman Agent license key to the Licenses.txt file, or AppImport.xml file, then you can type a license key. You can override the license key displayed. Only the format of the license key is validated.

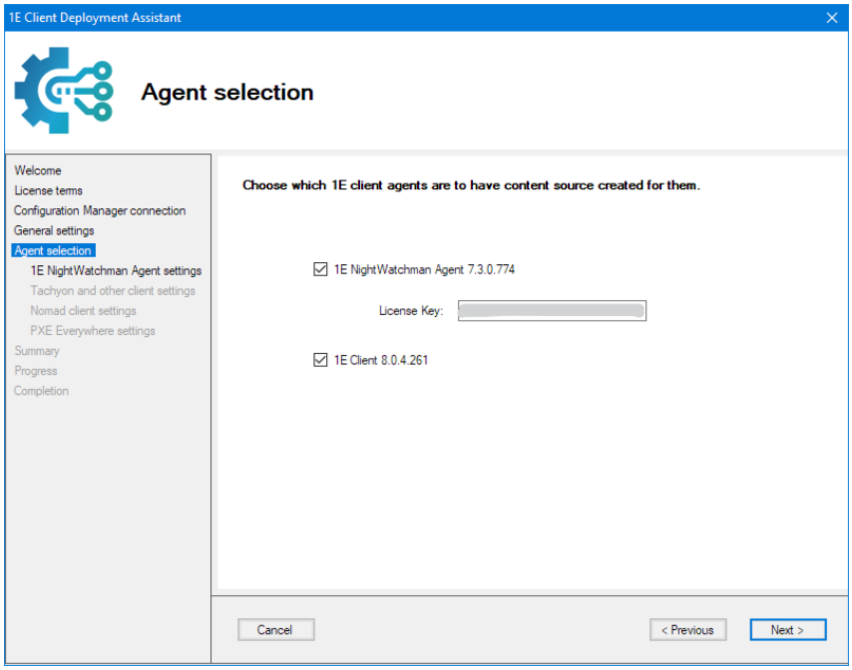
Note

1E license keys have the format: <name>-<4Chars>-<4Chars>-<4Chars>-<4Chars>

A license key may be reported as invalid if hyphens or other characters have been converted into symbols or Unicode, which can happen if copy+pasted.

Note

1E Client (1E Client, Shopping, WakeUp, Nomad, and PXE Everywhere) does not require a license key.



3.2.2.1.7 1E NightWatchman Agent application and package information

Review the following and click **Next** when completed.

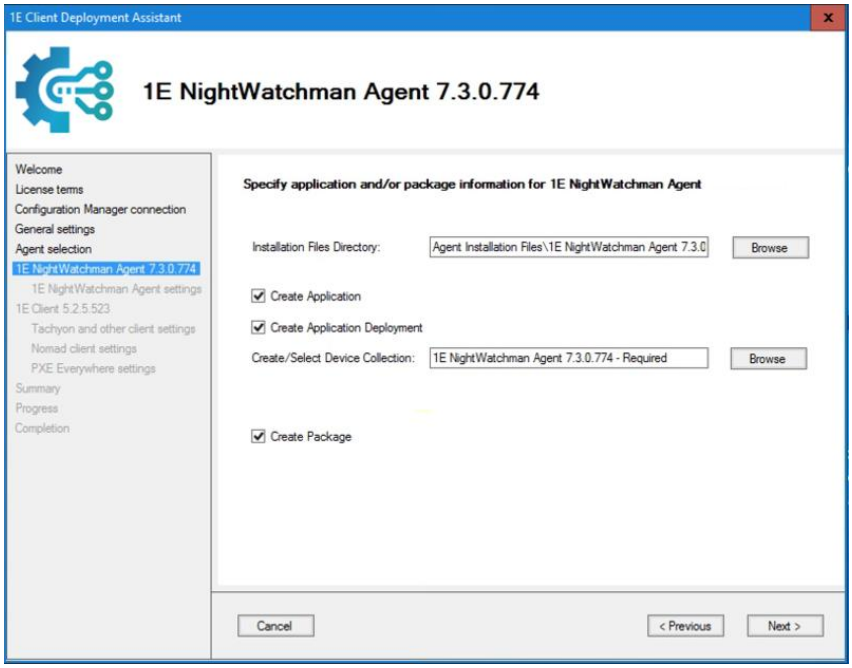
Installation Files Directory	Mandatory	Tells the CDA wizard where to locate the 1E Client source files that you extracted when you unzipped the 1E Client Deployment Assistant (CDA) files. These are used to create Configuration Manager applications and packages.
Create Application	Optional	Determines if an application for the client is created in Configuration Manager. You must check **Create Application** and/or **Create Package** option to enable and click on the **Next** button. If this option is not checked, then the CDA Wizard will not copy files and create an MST transform in the **Application Content Source** specified in the General settings screen.
Create Application Deployment	Optional	Only enabled if you choose **Create Application** and determines whether a required deployment type for the application is created in Configuration Manager.
Create/Select Device Collection	Mandatory if **Create Applicati**	The device collection used to deploy the application. If specified, then the CDA wizard will also create a

	on Deployment is enabled	deployment for the application's deployment types and the specified collection. A default name is suggested, which you can change. If the name you entered for **Create/Select Device Collection** does not exist, one is created. You must manually populate the created device collection after running the CDA wizard. You can click **Browse** to choose from a list of existing collections which you have access to using Configuration Manager RBAC. If you do this, you will not have the option to associate the device collection with a **Limiting Collection**.
Limiting Collection	Mandatory if **Create Application Deployment** is enabled	If you are creating a new device collection, you must also choose an associated **Limiting Collection**. This limits administrators to populating the new device collection with devices only from the selected **Limiting Collection**. By default, this is **All Systems**, but you can click **Browse** to choose from a list of existing collections which you have access to using Configuration Manager RBAC.
Create Package	Optional	Determines if a legacy package and associated install and uninstall programs for the client are created in Configuration Manager. You must check **Create Application** and/or **Create Package** options to enable and click on the **Next** button. If this option is not checked, then the CDA wizard will not copy files and create an MST transform in the **Package Content Source** specified in the General settings screen. **Note** Packages are created primarily for use in Task Sequences, therefore the CDA wizard sets the **Allow this program to be installed from the Install Package task sequence without being deployed** property, and does not create collections or deployments.

Do not use this option unless you require a package to be created. You can re-run CDA wizard later to create one if required.

Note

In previous versions the 1E Agent included WakeUp and NightWatchman. WakeUp is now included in the 1E Client, and NightWatchman is a separate client agent.



3.2.2.1.8 1E NightWatchman Agent settings

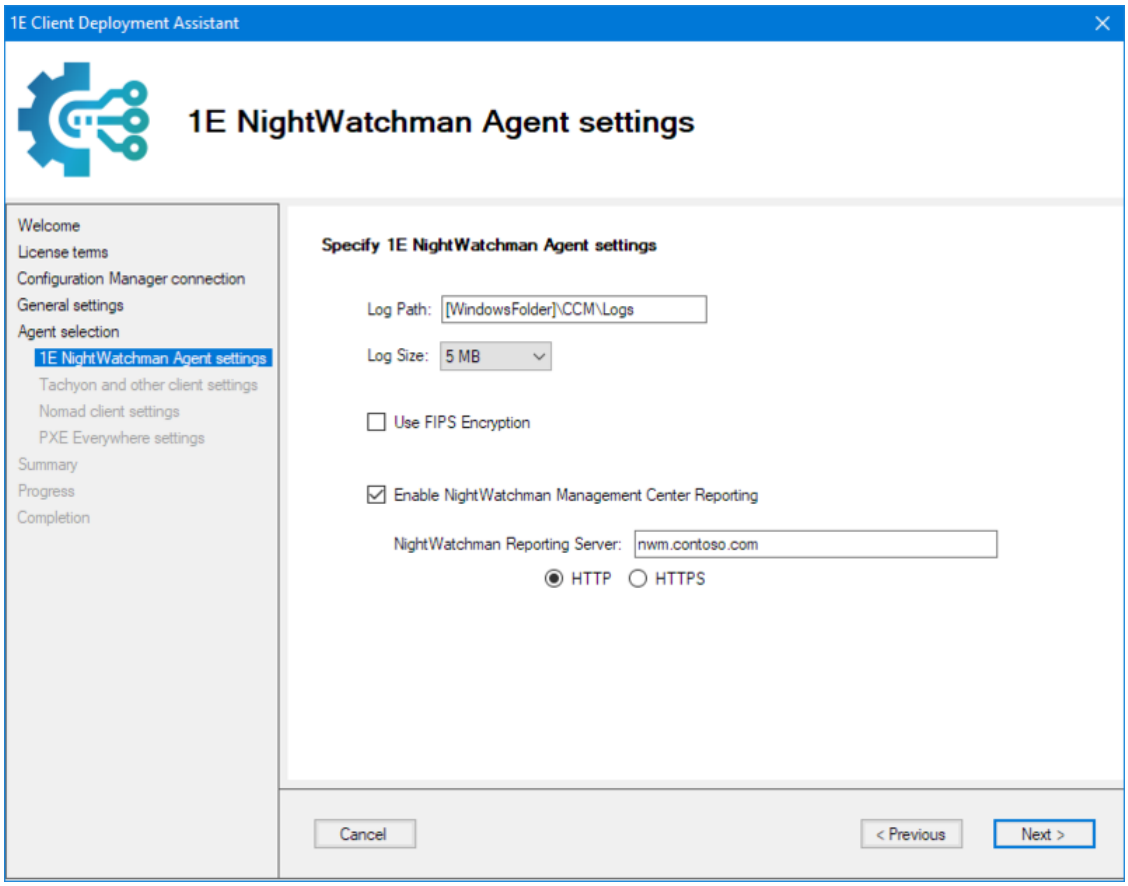
Review the following and click **Next** when completed.

Log Path	Mandatory	The path to the 1E NightWatchman Agent logs. The default path keeps the log files together with the Configuration Manager client logs. It uses *[WindowsFolder]* which is a Windows installer property name that refers to the Windows folder.

Log Size	Mandatory	The size of for the NightWatchman Agent log files. We recommend 5 MB.
Use FIPS Encryption	Optional	Check this option to enable the FIPS Encryption for NightWatchman and WakeUp. **Warning** You must use the same FIPS setting on all WakeUp clients, all WakeUp Servers, and on the NightWatchman Management Center server(s). Please ensure you use the same setting if you have previously deployed NightWatchman or 1E Agent, unless you are sure you want to change it.

Enable NightWatchman Management Center Reporting	Optional	Check this option if you have a NightWatchman Management Center server installed, and want NightWatchman to report power state changes and retrieve policy settings.
NightWatchman Reporting Server	Mandatory if **NightWatchman reporting** is enabled	Enter the name of the NightWatchman Management Center server in the format: *<serverFQDN>* Where **serverFQDN** is normally a DNS alias. The installer uses this name in the ServiceURL registry value for the WakeUp client, and references the AFWebService. **Warning** Please ensure you use the same setting if you have previously deployed NightWatchman or 1E Agent, unless you are sure you want to change it.

Select either the **HTTP** or **HTTPS** protocol.



3.2.2.1.9 1E Client application and package information

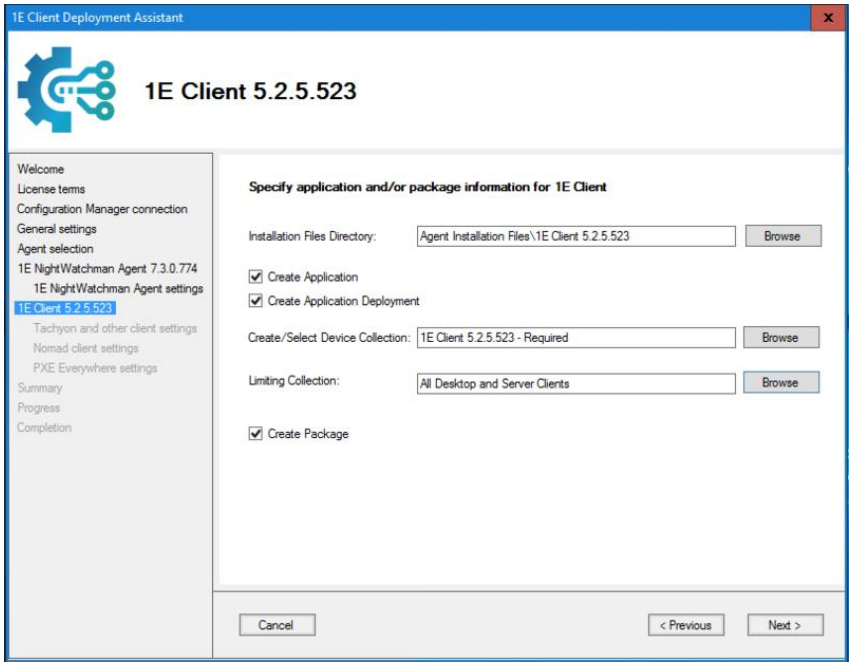
Review the following and click **Next** when completed.

Installation Files Directory	Mandatory	Tells the CDA wizard where to locate the 1E Client source files that you extracted when you unzipped the CDA files. These are used to create Configuration Manager applications and packages.
Create Application	Optional	Determines if an application for the client is created in Configuration Manager. You must check **Create Application** and/or **Create Package** option to enable and click on the **Next** button. If this option is not checked, then the CDA Wizard will not copy files and create an MST transform in the

		Application Content Source specified in the General settings screen.
Create Application Deployment	Optional	Only enabled if you choose **Create Application** and determines whether a required deployment type for the application is created in Configuration Manager.
Create/Select Device Collection	Mandatory if **Create Application Deployment** is enabled	The device collection used to deploy the application. If specified, then the CDA wizard will also create a deployment for the application's deployment types and the specified collection. A default name is suggested, which you can change. If the name you entered for **Create/Select Device Collection** does not exist, one is created. You must manually populate the created device collection after running the CDA wizard. You can click **Browse** to choose from a list of existing collections which you have access to using Configuration Manager RBAC. If you do this, you will not have the option to associate the device collection with a **Limiting Collection**.
Limiting Collection	Mandatory if **Create Application Deployment** is enabled	If you are creating a new device collection, you must also choose an associated **Limiting Collection**. This limits administrators to populating the new device collection with devices only from the selected **Limiting Collection**. By default, this is **All Systems**, but you can click **Browse** to choose from a list of existing collections which you have access to using Configuration Manager RBAC.
Create Package	Optional	Determines if a legacy package and associated install and uninstall programs for the client are created in Configuration Manager. You must check **Create Application** and/or **Create Package** options to enable and click on the **Next** button. If this option is not checked, then the CDA wizard will not copy files and create an MST transform in the

Package Content Source specified in the General settings screen.

> **Note**
>
> Packages are created primarily for use in Task Sequences, therefore the CDA wizard sets the **Allow this program to be installed from the Install Package task sequence without being deployed** property, and does not create collections or deployments.
>
> Do not use this option unless you require a package to be created. You can re-run CDA wizard later to create one if required.



3.2.2.1.10 Tachyon and other client settings

Review the following and click **Next** when completed.

Enable 1E	Optional	Check this option to enable Tachyon real-time client features of 1E Client to be used.
Switch	Mandatory if Tachyon is	Enter the connection details for the Tachyon Switch in the format: *<DNSnameFQDN>:<port>*

	enabled	Where **DNSnameFQDN** is normally a DNS alias, as used in the Tachyon Switch certificate, which is normally the same as the Tachyon Web Server certificate. **Port** is normally 4000. **Warning** Please ensure you use the same setting if you have previously deployed 1E Client with Tachyon platform client features enabled.
Background Channel URL	Mandatory if Tachyon is enabled	Enter the URL list containing one or more 1E Client Deployment Assistant Background Channel URL in the format: *https://<DNSnameFQDN1:443/Background/;https://<DNSnameFQDN2:443/Background/* Where **DNSnameFQDN** is normally a DNS alias, as used in the Tachyon Web Server certificate. **Warning** Please ensure you use the same setting if you have previously deployed 1E Client with Tachyon platform client features enabled.
Default Stagger Range Seconds	Mandatory if Tachyon is enabled	Enter the **Default Stagger Range Seconds**. The default is 300 (5 minutes).
Enable Inventory Insights	Optional	Uncheck this option to disable the Inventory module of 1E Client. Inventory supports the **Tachyon Activity Record** feature (also known as Inventory, and Historical Data Capture) which is required when using the Tachyon Connector for AppClarity or Application Migration. You can enable this separately from Tachyon, but the captured data cannot be used unless it is enabled.
Enable Interaction	Optional	Uncheck this option to disable the Interaction module of 1E Client. This feature was introduced in Tachyon 5.1.

		The Interaction module supports the **User Surveys and Notifications** feature (also known as 1E Client UI) which is required when using the Survey feature of Experience, and user-centric sampling features. You can enable this separately from Tachyon, but the captured data cannot be used unless the **Tachyon** is enabled.
Do not disturb	Optional	Uncheck this option to disable **Do not disturb** mode and allow the Client UI to show notifications from startup. Check this option to enable **Do not disturb** mode and stop the Client UI showing notifications, causing any surveys sent to this device to time out. If **Notification icon** is enabled, users will be able to enable or disable notifications by using the **Do not disturb** option. However, each time the user signs in, the **Do not disturb** mode will be reset.
Notification icon	Optional	Uncheck this option to disable the 1E Client UI notification icon. If enabled, the icon appears shortly after the user signs in.
Sample user interaction	Optional	Uncheck this option to disable Experience sampling the performance of user interactions with application windows in user sessions.
Local port	Mandatory if **Interaction** is enabled	The port number used for local communication between the 1E Client service and the 1E Client UI. Port is configurable between 100 and 65535. The default is 7766.

Enable Shopping	Optional	Check this option to enable the Shopping client module of 1E Client, which includes Windows Servicing Assistant (WSA).
Shopping Web URL	Mandatory if	Enter the **Shopping Web URL** in the format:

	Shopping is enabled	*http://<serverFQDN>/Shopping* where **serverFQDN** is normally a DNS alias. This option is available only if **Shopping** is enabled. **Warning** Please ensure you use the same setting if you have previously deployed 1E Client with Shopping client module enabled, unless you are sure you want to change it.
Enable Edge / Windows App browser support	Optional	Check this option to enable support for Microsoft Edge/Windows App browsers. This option is available only if **Shopping** is enabled.
Enable WakeUp	Optional	Check this option to enable the WakeUp client module of 1E Client.
Use FIPS Encryption	Optional	Check this option to enable the FIPS Encryption for WakeUp. This option is available only if **WakeUp** is enabled. **Warning** You must use the same Encryption setting on all WakeUp clients, all WakeUp Servers, and on the

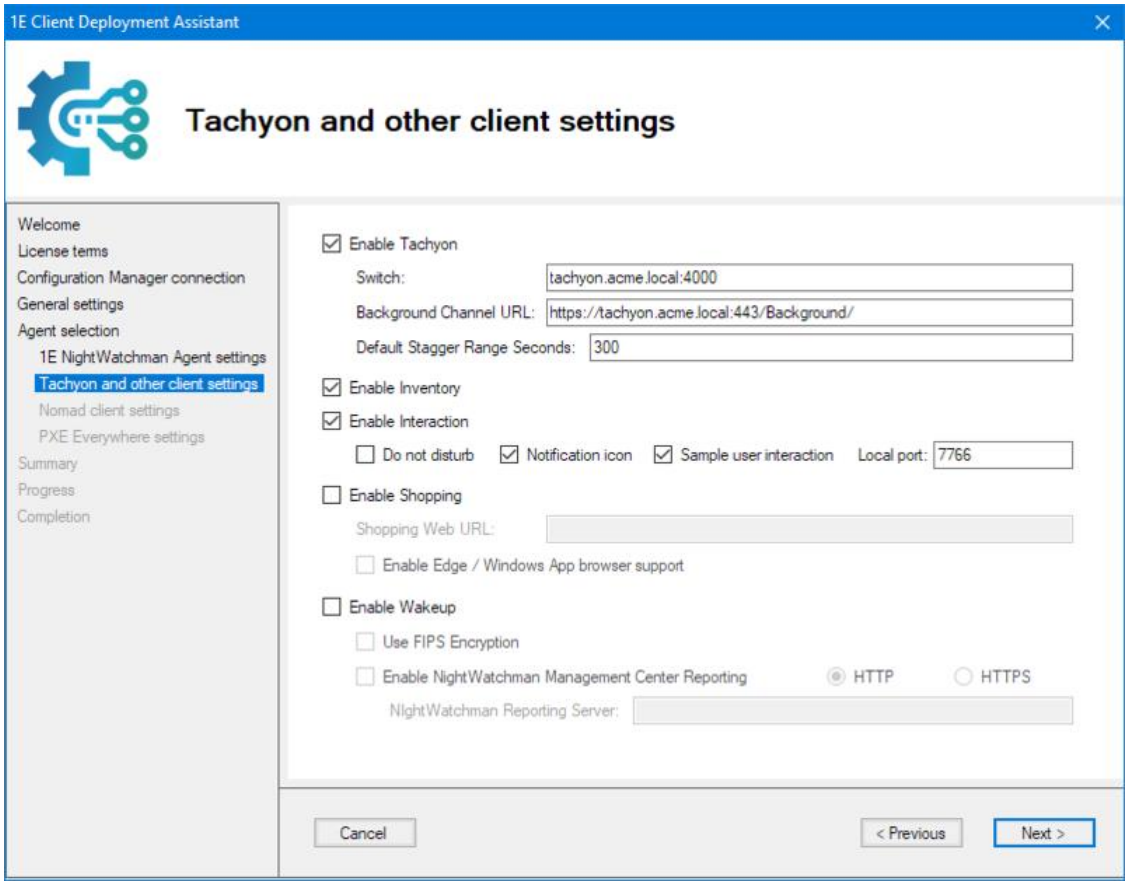
		NightWatchman Management Center server(s). Please ensure you use the same setting if you have previously deployed 1E Client or 1E Agent, unless you are sure you want to change it. **Note** Enabling FIPS Encryption will override the EncryptionLevel used by WakeUp, which is disabled by default. If you want to have FIPS Encryption disabled and WakeUp Encryption enabled then you must manually edit the EncryptionLevel setting in the MST. Please refer to Advanced configuration for how to edit an MST.
Enable NightWatchman Management Center Reporting	Optional	Check this option if you have a **NightWatchman Management Center** server installed, and want WakeUp to report subnet changes.

		Select either the **HTTP** or **HTTPS** protocol. These options are available only if **WakeUp** is enabled. This option is especially useful for computer which change location frequently. WakeUp reports subnet changes immediately, whereas NightWatchman reports changes according to its inventory reporting schedule. WakeUp only supports Wake-on-LAN for wired connections and not for wireless, therefore a laptop reporting a subnet change from wired (docked) to wireless helps the WakeUp Server avoid wakeup attempts on the wired connection, and a wakeup failure will be attributed to the wireless subnet.
NightWatchman Reporting Server	Mandatory if **NightWatchman Reporting** is enabled	Enter the name of the NightWatchman Management Center server in the format: *<serverFQDN>* Where **serverFQDN** is normally a DNS alias. This option is available only if **WakeUp** is enabled. The installer uses this name in the ServiceURL registry value for the WakeUp client,

and references the AFWebService.

Warning

Please ensure you use the same setting if you have previously deployed 1E Agent or 1E Client with WakeUp client module enabled, unless you are sure you want to change it.



3.2.2.1.11 Nomad client settings

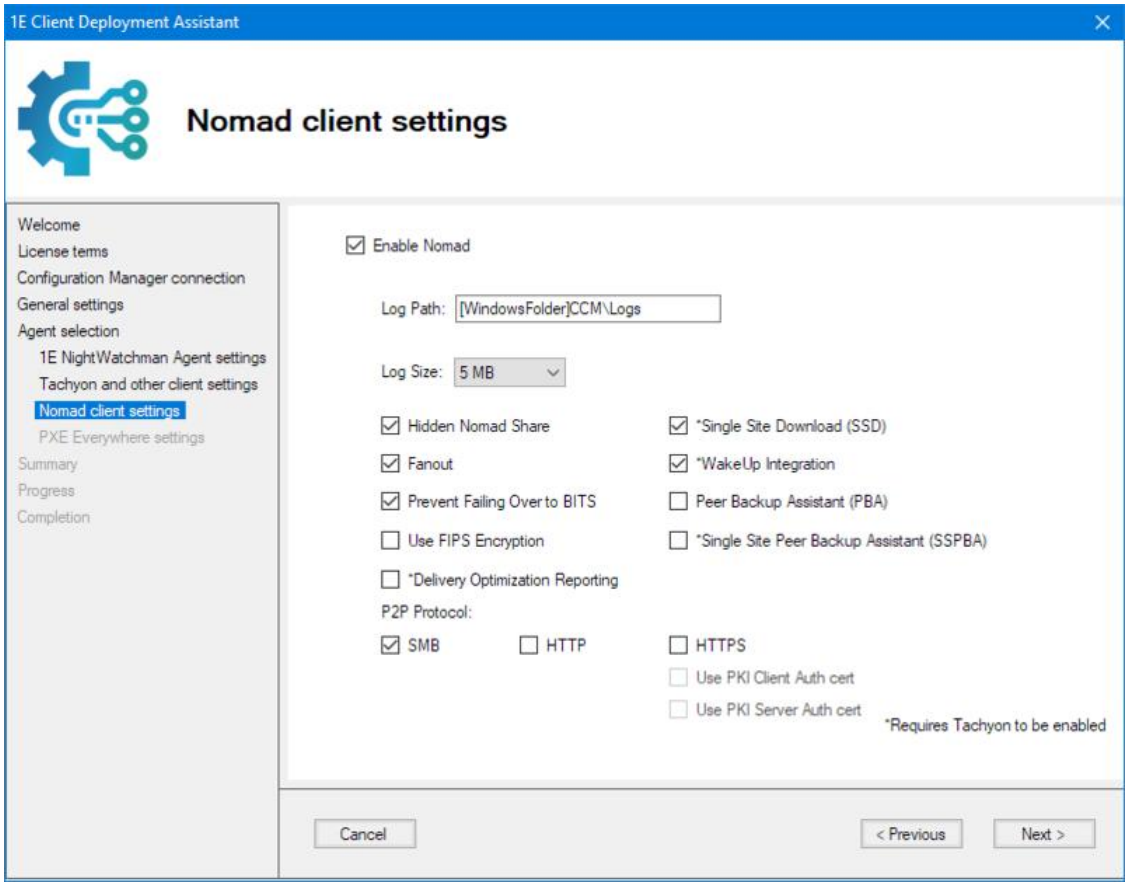
Review the following and click **Next** when completed.

Enable Nomad	Optional	Check this option to enable the Nomad client module of 1E Client.
Log Path	Mandatory if Nomad is enabled.	Enter the path to the logs. The default path keeps the log files together with the Configuration Manager client logs. It uses *[WindowsFolder]* which is a Windows installer property name that refers to the Windows OS folder. This default is useful for client OS. For location may be different for CM servers. For example CM logs on a Management Point server may be located in C:\Program Files\SMS_CCM\Logs if the MP roles was installed prior to the CM client.
Log Size	Mandatory if Nomad is enabled.	Select the size of for the log files. We recommend 5 MB.
Hidden Content Distribution Share	Optional	Check this to enable the hidden share feature and to prevents end-users from accidentally accessing the share. **Warning** If you tick this box, you must ensure that all Nomad installations are configured to use this feature. Please ensure you use the same setting if you have previously deployed Nomad Branch or 1E Client with Nomad client module enabled, unless you are sure you want to change it. **Note** Best practice is to use a **Hidden Nomad Share**. The default for this setting in the NomadMSI is disabled

		to be consistent with previous versions of installers and avoid issues for customers who deploy Nomad by other means.
Fanout	Optional	Check this to enable the **Fanout** feature. This feature is especially useful in large organizations with many networks.
Prevent Failing Over to BITS	Optional	Check this to prevent downloads from reverting to using BITS if an error occurs. It ensures that any download errors are reported back effectively with minimum impact on remote sites.
Use FIPS Encryption (v6 onwards)	Optional	Check this to ensure that Nomad is FIPS compliant in its communications. **Warning** You must use the same FIPS setting on all Nomad clients. Please ensure you use the same setting if you have previously deployed Nomad Branch or 1E Client with Nomad client module enabled, unless you are sure you want to change it.
Delivery Optimization Reporting	Optional	Check this to enable Nomad to monitor and report on Delivery Optimization (DO) downloads. Delivery Optimization monitoring and reporting is only supported in full versions (OS with UI) of Windows Server 2016 and Windows 10 Version 1909 onwards.

		You must have **Tachyon enabled** and **Tachyon Platform** installed for this feature to work.
Single Site Download (SSD)	Optional	Check this to enable Nomad single-site download feature where Nomad master caches can service an entire local site not just the local subnet. You must have **Tachyon enabled** and **Tachyon Platform** installed for this feature to work. See also **SSPBA** below.
WakeUp Integration	Optional	Check this to enable WakeUp integration so that machines where the Nomad cache contains a particular package can be used by the Nomad master even if the machine with the cache is currently switched off. You must have **Tachyon enabled** and **Tachyon Platform** installed for this feature to work. You will also need **NightWatchman and WakeUp** system.
Peer Backup Assistant (PBA)	Optional	Check this to enable Nomad PBA feature. See also **SSPBA** below, and **SDD** above. This OS deployment feature enables Nomad to be used as a data store for USMT data to migrate user settings from the old OS to the new one. It removes the necessity for specifically provisioning state migration points or servers to hold the backup data.

Single Site Peer Backup Assistant (SSPBA)	Optional	Check this to enable Nomad **SSPBA** feature (only enabled if **Peer Backup Assistant** is checked). You must have **Tachyon enabled** and **Tachyon Platform** installed for this feature to work. See also **SSD** above.
P2P Protocol	Optional	Check one or more of the following: SMB HTTP HTTPS When selecting HTTPS you can also check one or both of the following: Use PKI Client Auth cert Use PKI Server Auth cert



3.2.2.1.12 PXE Everywhere settings

Review the following and click **Next** when completed.

Enable PXE Everywhere	Optional	Check this option to enable the PXE Everywhere client module of 1E Client.
Log Path	Mandatory	The path to the PXE Everywhere logs. The default path keeps the PXE Everywhere log files together with the Configuration Manager client logs. It uses *[WindowsFolder]* which is a Windows installer property name that refers to the Windows folder.
Log Size	Mandatory	The size of for the PXE Everywhere log files. We recommend 5 MB.
Use FIPS Encryption	Optional	Check this to ensure that PXE Everywhere is FIPS compliant in its communications. This is only available from PXE Everywhere 3.0 and later.

Warning

		You must use the same FIPS setting on all PXE Everywhere Agents and PXE Everywhere Static Responders. Please ensure you use the same setting if you have previously deployed PXE Everywhere, unless you are sure you want to change it.
Windows ADK location	Mandatory	The location of the Windows ADK. If this has been installed on a Configuration Manager site server, the location should be: *C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit* PXE Everywhere requires that certain files are in its TftpRoot folder in order to be able to service PXE requests. These files mostly come from the winpe.wim file in the WinPE addon for the Assessment and Deployment Kit (ADK). 1E cannot bundle these files with PXE Everywhere because Microsoft does not allow their redistribution. The wizard automates this process by creating a CAB file and MST data so that the boot files are put in place as PXE Everywhere is installed. So you must locate the Windows ADK that will be used as the source.
PXE Everywhere Central web service	Mandatory	The full URL of the PXE Everywhere Central web service which the agent uses: *http://<serverFQDN>/PXELite/PXELiteConfiguration.asmx* You must have PXE Everywhere Central installed for this feature to work. **Warning** Please ensure you use the same setting if you have previously deployed PXE Everywhere, unless you are sure you want to change it.
Enable support for DHCP Snooping	Optional	Check this to enable support for DHCP Snooping. This feature requires you have at least one PXE Everywhere Responder installed, and configured

your network to forward PXE requests to the Responder(s) on the specified **DHCP port**, and authorize them to receive and respond to requests.

When you enable this option, you can also specify the **DHCP port** that the PXE Everywhere Agents listen for responses from the Responder. If you change this then you must configure Responders to use the same port. By default, this is port 2067.

If you do not check the DHCP Snooping option, then you do not need Responders and PXE Everywhere Agents listen for responses on port 67.

Note

In order to service PXE requests, certain files from the winpe.wim file in the ADK must be present in PXE Everywhere's TftpRoot folder on each client. Without using CDA, this process must be carried out after PXE Everywhere is installed, for example using a Task Sequence. However the CDA wizard automates this process during installation of PXE Everywhere. CDA uses DISM to extract files from the ADK's winpe.wim file and creates a **PXELiteLocal-xxxx.cab**, and adds custom actions to the MST transform file to do the following during installation of PXE Everywhere:

Place the boot file in the right location as PXE Everywhere is installed

Run *CreateBCD.exe* to copy an advertised PXE boot image to the PXE Everywhere cache thereby creating a boot configuration database that is useful when using task sequences.

The host computer used to run the CDA wizard can be the Configuration Manager site server or another computer that has the following installed:

Configuration Manager console

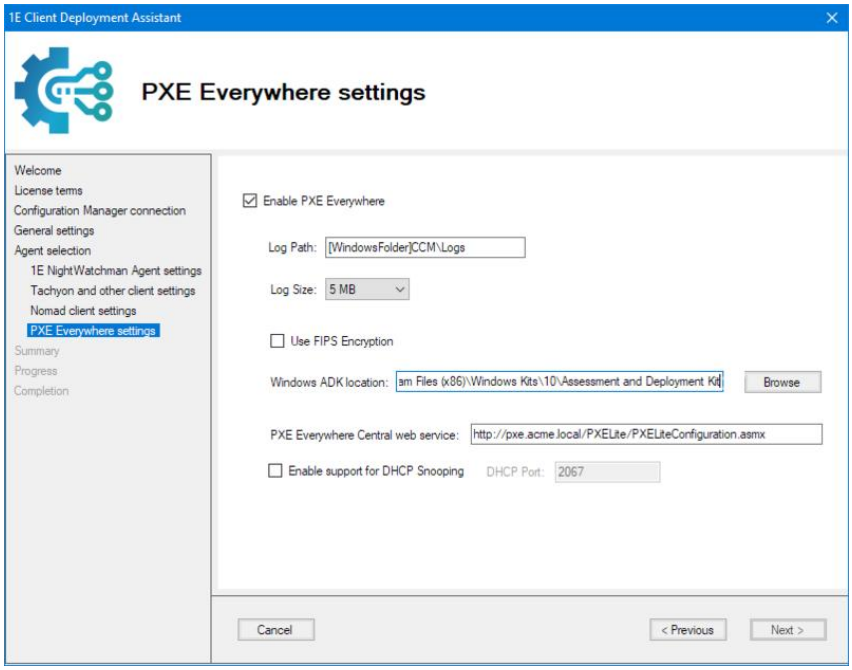
Microsoft ADK with WinPE addon - only if the CDA wizard is used to create PXE Everywhere applications

It will need to have .Net Framework v4.8 Runtime installed, a check when the wizard runs checks for this being installed, and will if not already installed, provide a link to https://dotnet.microsoft.com/en-us/download/dotnet-framework/net48?cid=getdotnetframework where you will need to download and run the .Net Framework v4.8 Runtime. The link is provided should you wish to install this prior to running the wizard. The install does require a reboot to complete.

If you are installing PXE Everywhere you must install the **Deployment Tools** feature from the Microsoft Assessment and Deployment Kit (ADK), and the **WinPE addon**. The user running the CDA wizard must have local administrator privileges because the CDA wizard uses *dism.exe* to mount a PXE *.wim* file in order to extract boot image files. Start the wizard using Run as Administrator.

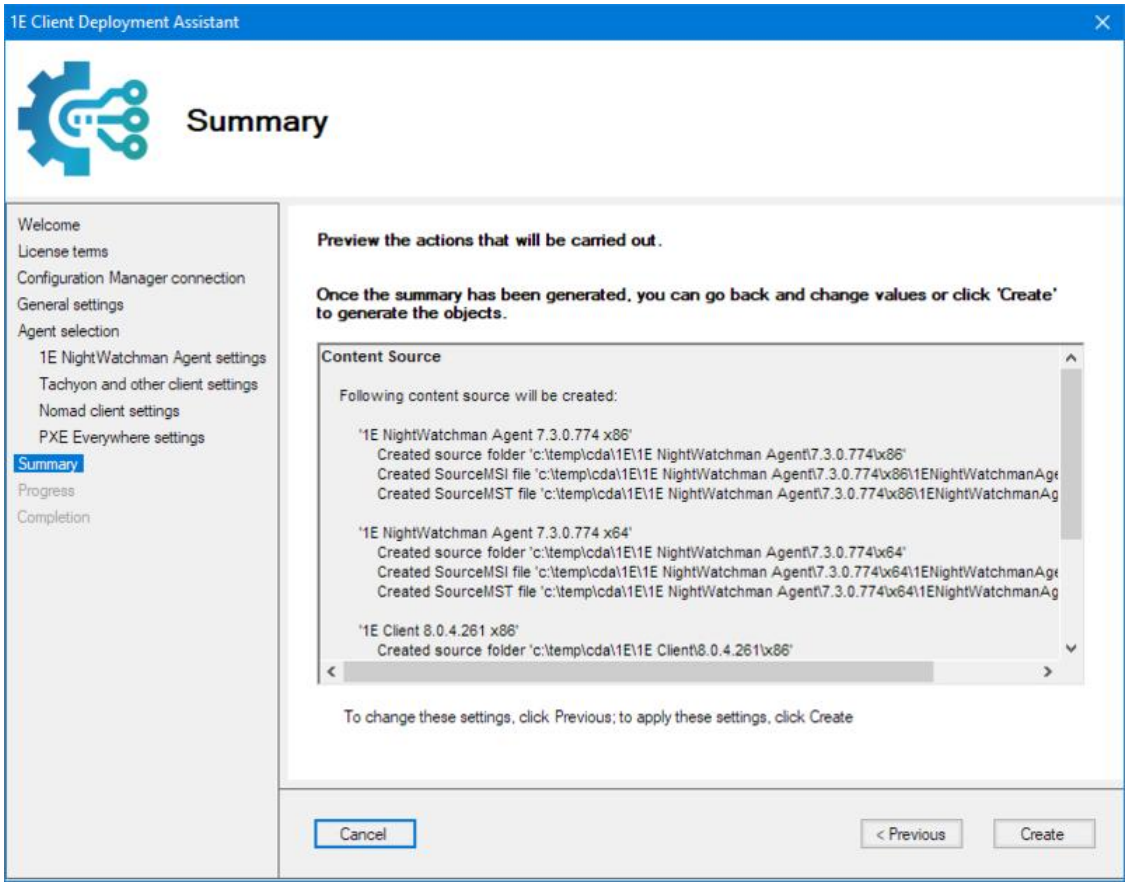
Note

To download and install the Windows ADK go to https://docs.microsoft.com/en-us/windows-hardware/get-started/adk-install. Starting with Windows 10, version 1809, WinPE is an add-on to the ADK, previously it was included in the ADK. First install the ADK, and then install the WinPE addon. Approximately 7GB disk space is required.



3.2.2.1.13 Summary

When you have defined the attributes for all the agents you intend to use, a summary screen is displayed. If you are happy with the settings for the agents, click **Create**, otherwise click **Previous** to return to review the issues and correct them.

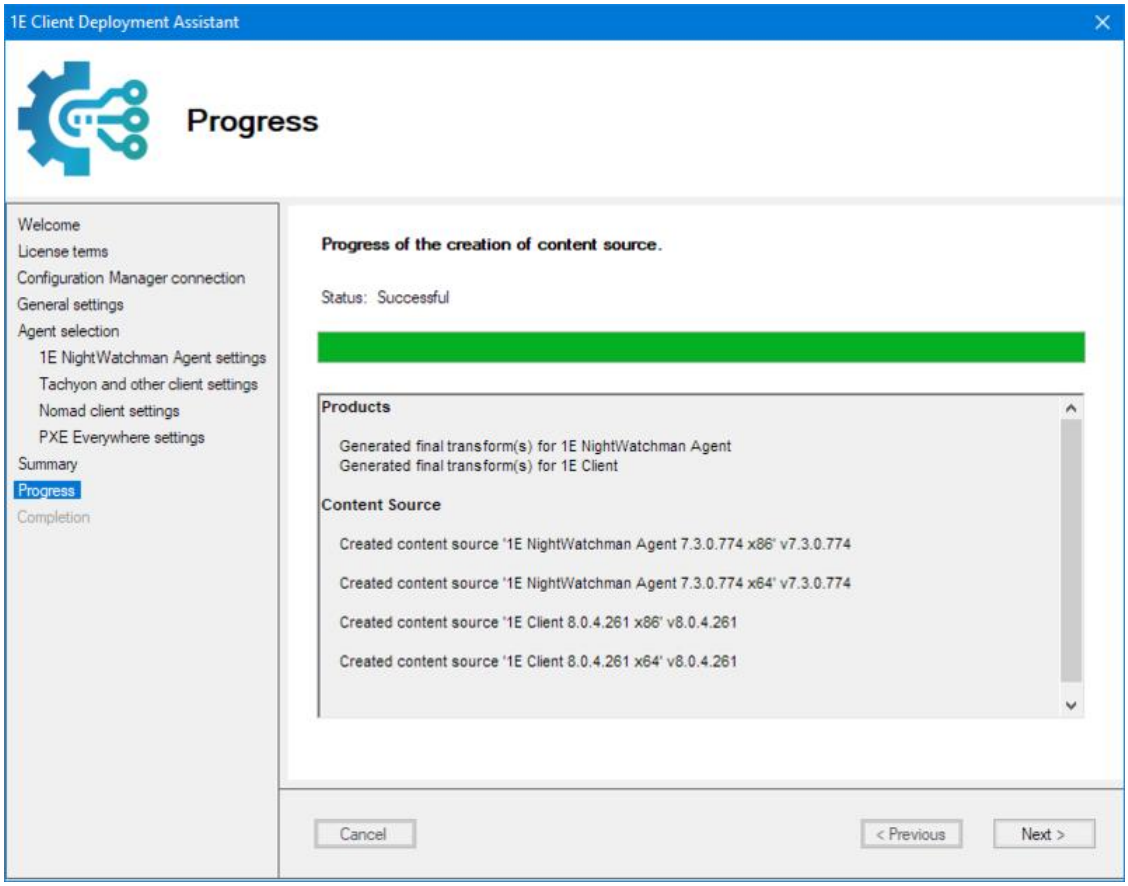


3.2.2.1.14 Progress

A screen is displayed to show the progress – there may be a slight delay before the progress bar starts as there's some background processing taking place.

Click **Next** when all the actions have been done.

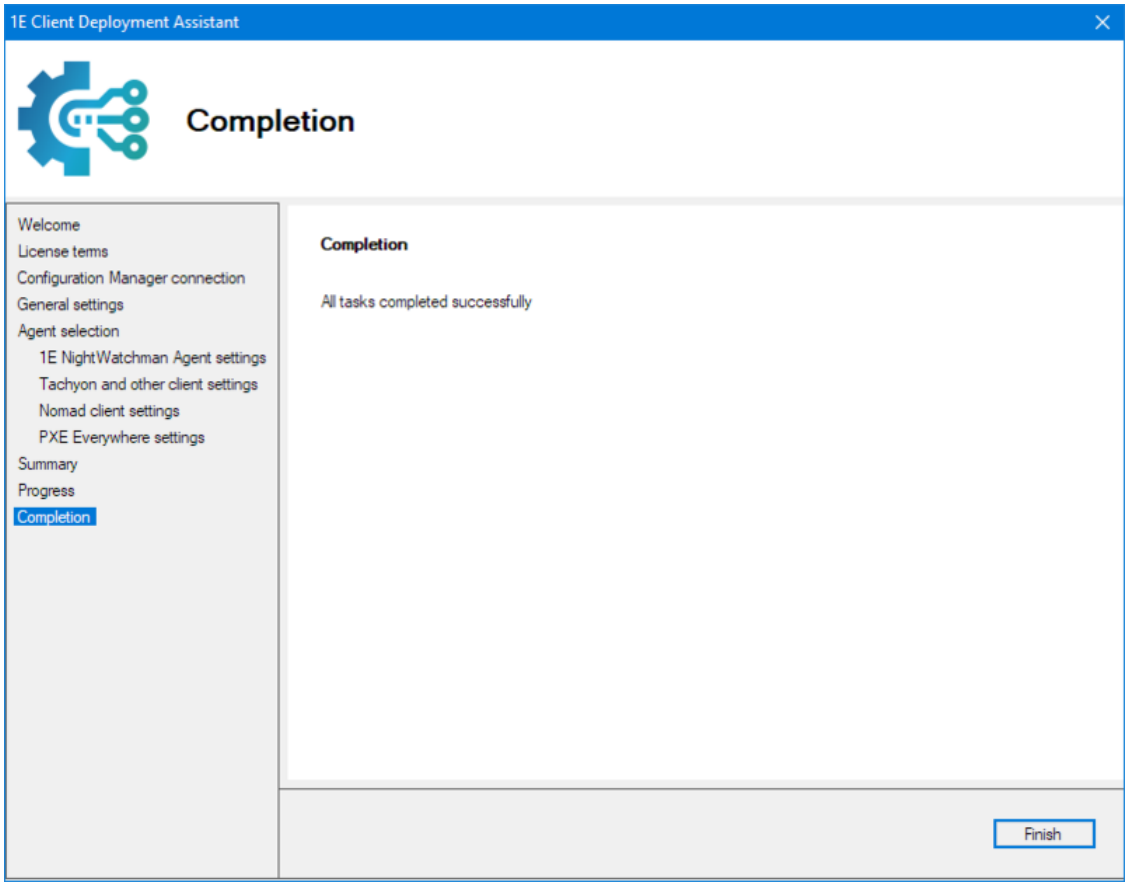
> **Note**
>
> If PXE Everywhere has been selected the CDA wizard can take a several minutes to load and extract files from the ADK winpe.wim file. You can use Task Manager to observe DISM in progress.



3.2.2.1.15 Completion

The screen will show details of any errors that were detected.

Click **Finish**.



3.2.3 Configuration Manager objects

Objects created in Configuration Manager when the CDA wizard is run using default settings.

The pictures on this page may not show the latest versions of 1E products. 1E Client Deployment Assistant 8.1 creates objects for the following 1E products:

1E Client 8.1.2.62 (includes clients for Nomad, PXE Everywhere, Shopping/WSA, WakeUp, and Tachyon) (new)

1E NightWatchman Agent 7.3.0.774

Note

The pictures on this page may not show the latest versions of 1E products.

3.2.3.1 Applications

A Configuration Manager application is created for each 1E Agent that was selected in the CDA wizard.

Applications are viewed in Configuration Manager console, Software Library as shown in the picture.

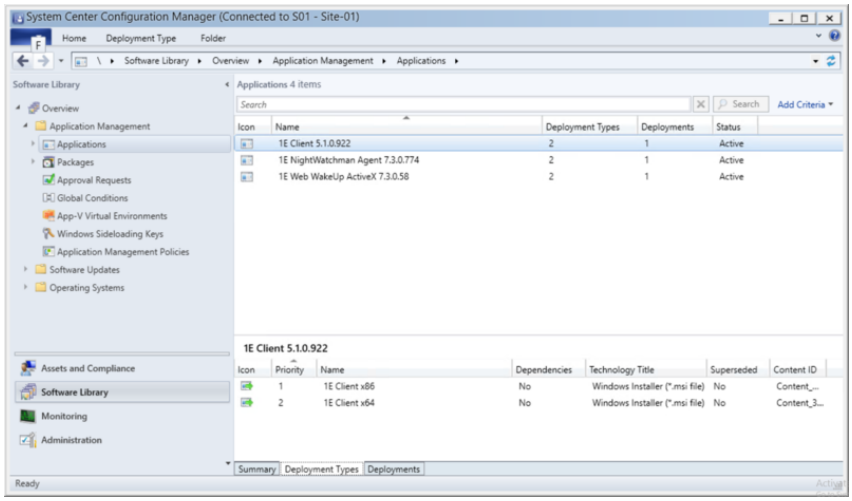
Click on an application to view its Summary, Deployment Types and Deployments tabs.

Tip

You can move the applications into folders in Configuration Manager, which will help you to organize and make it easier to find them later. For example, you can create a folder called **1E Applications** to store these applications and keep them separate from any other applications in your system.

3.2.3.2 Deployment Types

Each application has two deployments types – one for each architecture **x86** and **x64**.



3.2.3.3 Deployment Type properties

View the properties of a Deployment Type and view the settings in each tab. The Programs tab has an Installation program that installs an Agent using its MSI and the MST transform file that has been modified by the wizard, and creates a log file. You can modify the command-line as required.

Without patch:

```
msiexec /i 1E.Client-x64.msi REBOOT=ReallySuppress /l*v %TEMP%\1E.Client-x64-In
stall-5.1.0.922.log /qn TRANSFORMS="1E.Client-x64-5.1.0.922.mst"
```

With patch:

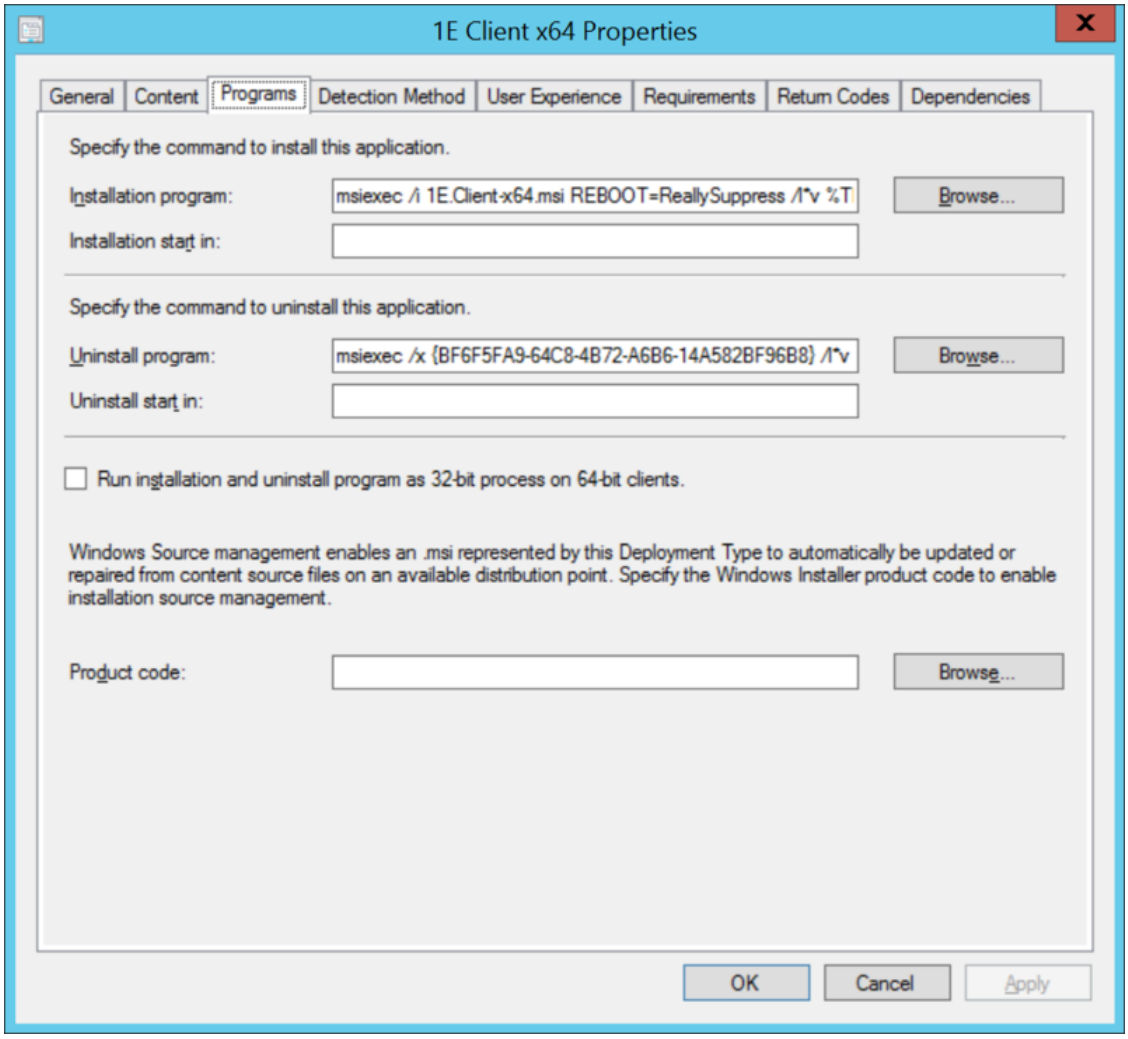
```
cmd /c "msiexec /i "%cd%\1E.Client-x64.msi" REBOOT=ReallySuppress /l*v %TEMP%\1
E.Client-x64-Install-5.1.0.922.log /qn TRANSFORMS="%cd%\1E.Client-x64-5.1.0.922
.mst" PATCH="%cd%\q21005-1e.client-x64.v5.1.0.922.msp"
```

Tip

You can make copies of Deployment Types for other purposes. For example the 1E Client x64 deployment can be copied to create one used to deploy the 1E Client (with Nomad module enabled) to Distribution Points, which would use an alternative MST transform file manually updated with relevent settings for DPs.

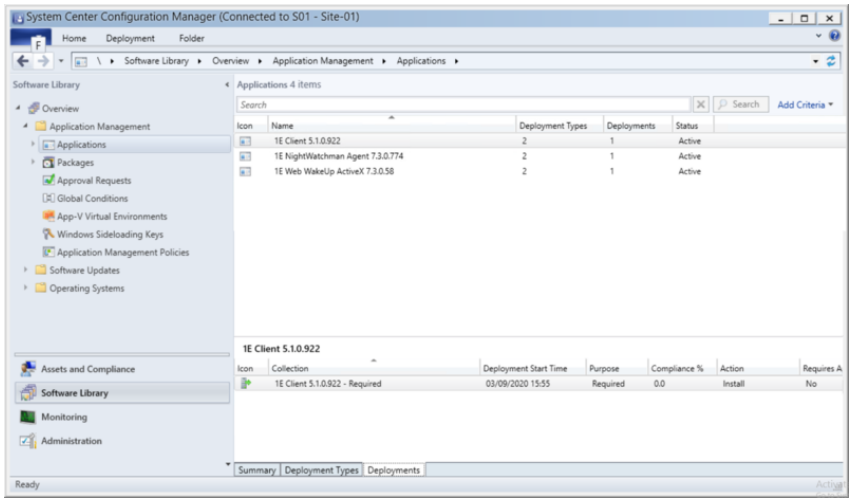
Note

The command-lines and picture shown here are an example for deploying the 1E Client with or without a patch.



3.2.3.4 Deployments

A deployment is created for each application for its corresponding device collection.



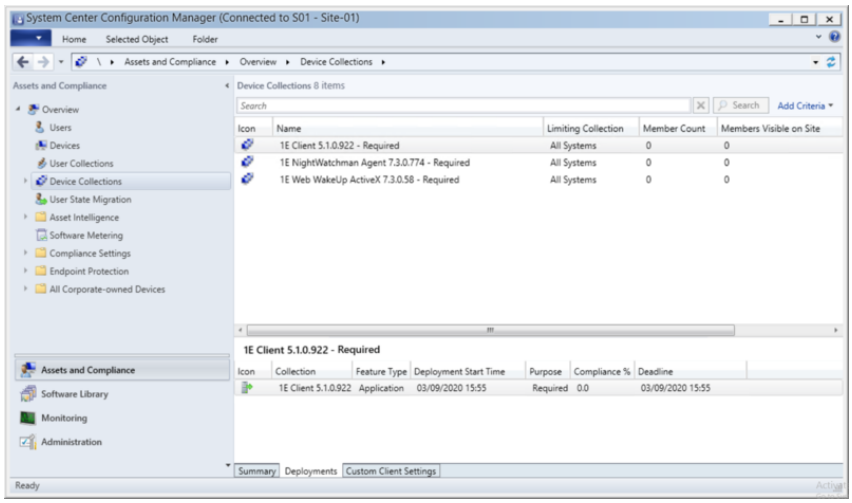
3.2.3.5 Device Collections

If you chose to create new device collections, they are found under **Device Collections** of **Assets and Compliance**.

Device collections are only associated with applications, via application deployments, and not with packages. If you have chosen to create legacy packages these require more manual work in order to deploy them.

You can move these collections into a folder.

> **Note**
>
> To deploy applications to intended targets, all you need to do is populate the appropriate device collections using membership rules according to your organization's practices.



3.2.3.6 Speeding up deployments

To speed up and monitor the progress of a deployment:

In the Configuration Manager console, select the **Assets and Compliance** workspace.

Select the **Device Collections** node, right-click on the relevant Collection created by CDA and choose **Client Notification** -> **Download Computer Policy**.

A dialog is displayed showing the number of resources in this collection. Click **OK**.

> **Note**
>
> This process causes each of the Configuration Manager clients to download the new deployment policy you just created rather than waiting for them to do it on their regular schedule, which should speed up the uptake of the new deployment.

Select the **Monitoring** workspace and choose the **Deployments** node.

Right-click the relevant client deployment and choose **View Status** from the context menu. You can view the next task when the current one finishes.

Repeat for other collections and deployments as required.

3.2.3.7 Packages

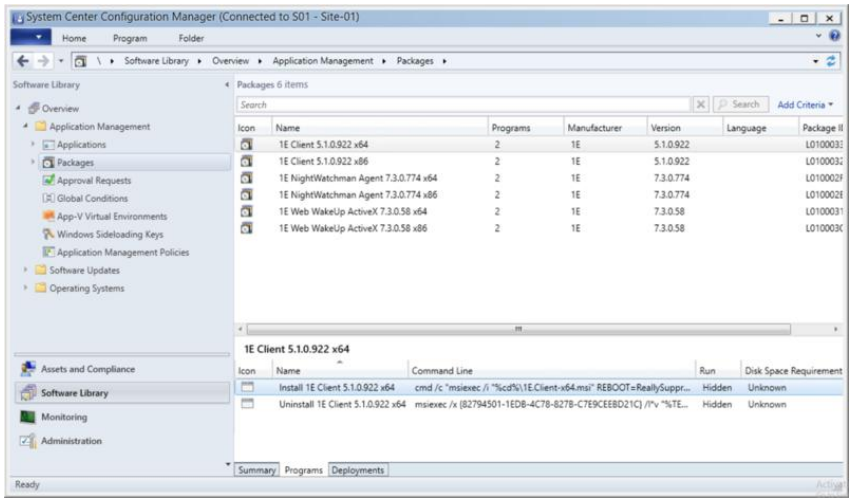
If you chose to create legacy packages one package is created for each combination of agent and architecture (**x86** and **x64)**.

Click on each package to view its **Summary**, **Programs** and **Deployments** tabs.

You can move these packages into a folder.

Packages are created primarily for use in Task Sequences, therefore the CDA wizard sets the **Allow this program to be installed from the Install Package task sequence without being deployed** property, and does not create collections or deployments.

You would not normally create packages for PXE Everywhere.



3.2.4 Advanced configuration

Advanced editing of a MST transform file to support configuration options not supported by the CDA wizard UI.

1E Client Deployment Assistant 8.1 supports the following 1E products, you should review documentation for their installer properties to know what options are possible.

1E Client 8.1 (includes clients for Nomad, PXE Everywhere, Shopping/WSA, WakeUp, and Tachyon) (new)

1E NightWatchman Agent 7.3.0.774

The guidance here is for adding an installer property by editing the base MST transform file provided out-of-box for 1E Client, but the process also works for other MST. Editing a base MST before running the CDA wizard helps you if know you will use the modified MST more than once, for example if you are working in a lab, and want to re-use it in a production environment. This approach only works if you are adding or editing installer properties that are not affected by running the CDA wizard.

An alternative approach is to edit the updated MST transform produced by CDA after running the wizard. This is only useful if the edited MST will be used in the same environment, although you can also edit the environment-specific settings you set when running the wizard. This approach is most frequently used if you

need fine-tune properties provided in the base MST and the CDA wizard is not able to configure them exactly the way you need.

In both cases, you will probably need to edit both x64 and x86 files.

Please review Installer properties page for a full list of installer properties included in each base MST.

> **Note**
>
> You must use UPPERCASE when specifying the *name* of any installer property in a **mst** transform file, and preferably when including them in a msiexec command-line.

> **Note**
>
> The pictures on this page may not show the latest versions of 1E products.

3.2.4.1 Adding installer properties to the base MST transform file

To extend installer properties or change default settings for Nomad clients, you can edit their associated MST transform files by using a tool such as Orca a database table editor for creating and editing Windows Installer packages.

> **Note**
>
> Orca is a Microsoft tool for creating and editing Windows Installer packages (MSI) and merge modules (MST transforms). It is available from the Windows Installer Development Tools - https://docs.microsoft.com/en-us/windows/desktop/msi/orca-exe.

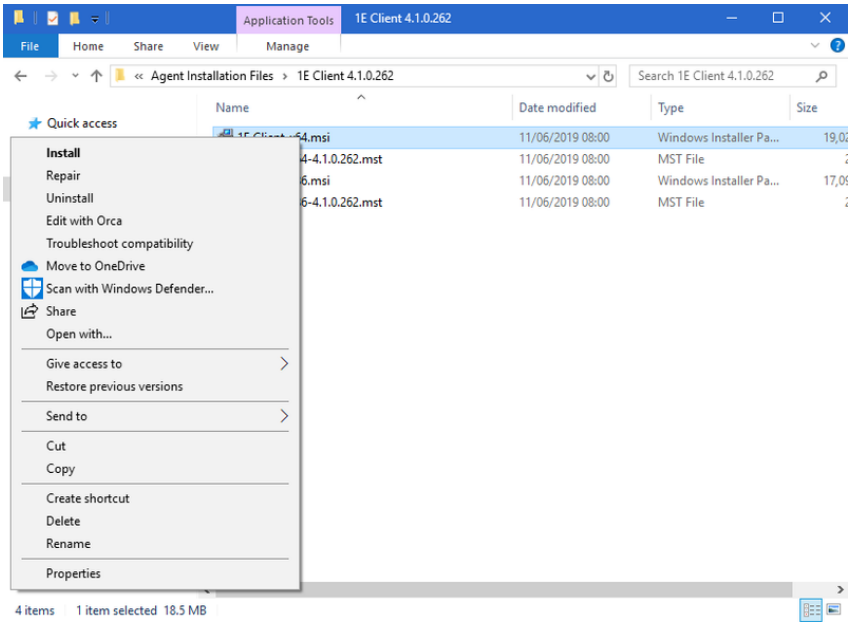
The following example configures StatusMsgEvents by modifying the x86 and x64 `.mst` files. When the wizard is run, the new transform is applied to the deployment and package, and the new value is set when Nomad is installed.

> **Warning**
>
> Status message events should be used with caution as they could impact your Configuration Manager environment when scaled up to tens of thousands of machines.

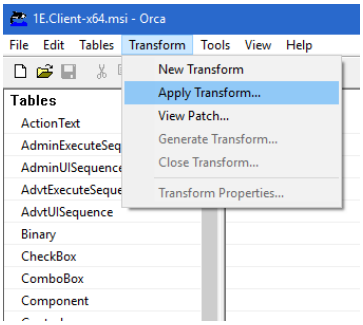
> **Note**
>
> The steps are recommended only for values unaffected by running the CDA wizard, because updated base settings may be changed when the wizard runs. Please review Installer properties page to see which installer properties are used by CDA.

To edit the installer with Orca:

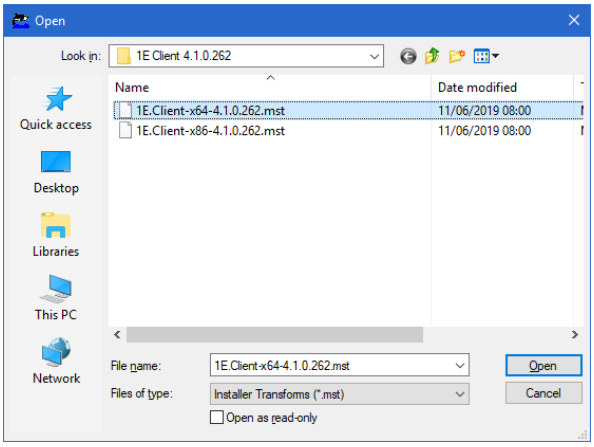
Right-click the 1E.Client-x64.msi choosing **Edit with Orca** from the context menu.



From the Transform menu in the Orca application, select **Apply Transform...**

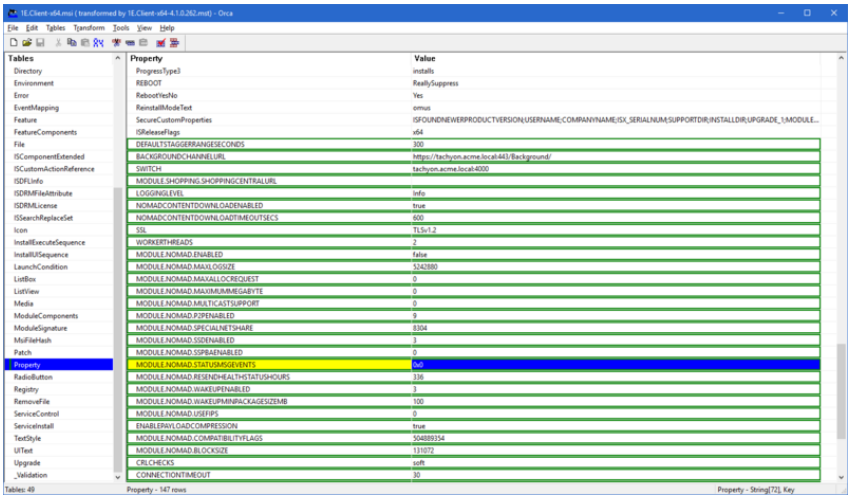


In the **Open** dialog, select the 1E.Client-x64-5.1.x.mst file.



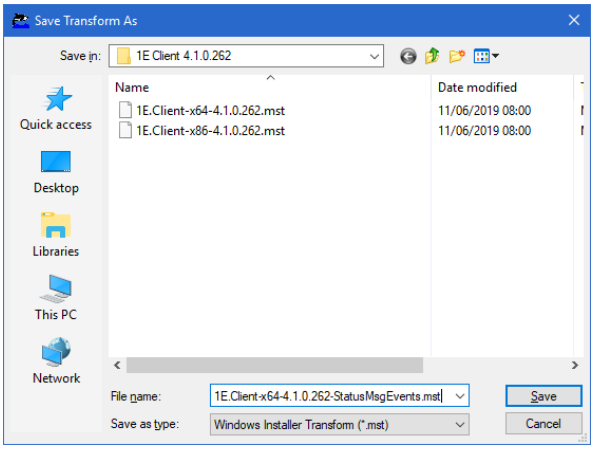
In the Table list on the left, scroll down and locate *Property*.

On the right pane, scroll down to StatusMsgEvents and update its value to 0x1000000064 (*0x0* by default).



From the Transform menu, choose Generate Transform and save the file with a new name.

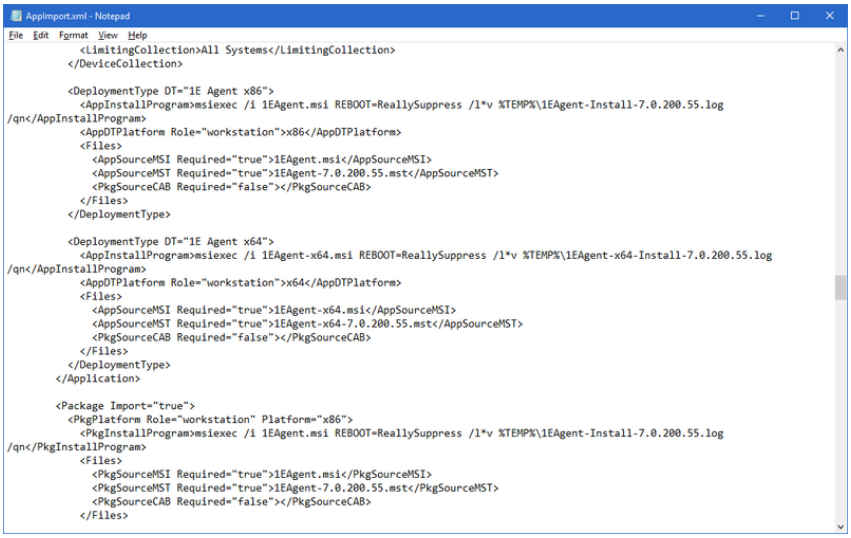
For example: 1E.Client-x64-x.x.x-StatusMsgEvents.mst



Repeat steps 1-6 for the x86 version of the installer and `.mst` file.

Edit the *`AppImport.xml`* file and update *`<AppSourceMST>`* and *`<PkgSourceMST>`* to point to the new transform files for both x86 and x64 versions.

The picture shows the original file.



3.2.5 Using client patch files with CDA

CDA supports the application of patch files during installation of the clients.

3.2.5.1 Using client patch files with CDA

The latest released patch for each client is now packaged along with the **.msi** in each new CDA release. Patches can only be installed alongside the **.msi**. That is the patching can't be done using CDA after the client has been installed.

CDA only supports single patch installation, that is you can only have one .msp file per client. In practice this shouldn't be an issue as cumulative patches are created across all the 1E products, so only one patch should be needed anyway.

Please check the 1E Support Portal https://support.1e.com/ to see if there is a later Accumulated Hotfix (Patch):

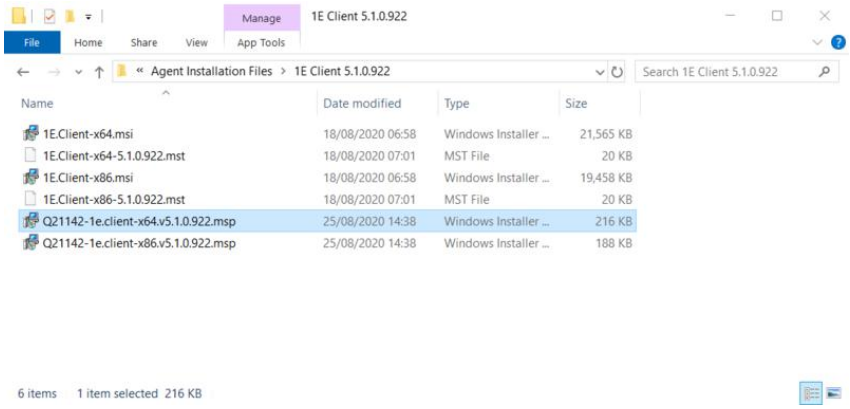
1E Client vx.x.x.x

1E NightWatchman Agent v7.3.0.774

If you want to apply patch to a client that is different to the packaged one, the existing **.msp** file must be replaced by your new one, this is located in the client's installation folder under the **Agent Installation Files** folder in the CDA artifact. This must be done prior to launching the CDA installer.

The picture opposite shows the CDA folder for the 1E Client. Here you can see the installer files for 1E Client, alongside the **.mst** files and **.msp** patches for 1E Client, which will be applied during the installation process.

Please refer to Configuration Manager objects for information about the command-lines created by CDA.



3.3 Troubleshooting

A general methodology for investigating issues with the 1E Client Deployment Assistant, as well as identifying key issues and their resolutions.

> **Note**
>
> If you are experiencing problems with client agents that have been deployed to devices already then please refer to documentation for the relevant product version.

For known issues relating to specific components, please refer to the respective troubleshooting pages:

Clients	Platform	Applications	Integration
1E Client	1E	Endpoint Automation	1E Core for ServiceNow
1E Client Deployment Assistant		Experience Analytics	1E ITSM Connect for ServiceNow
PXE Everywhere		Endpoint Troubleshooting	1E Service Catalog Connect for ServiceNow
		Writing 1E Instructions (1E SDK)	1E Virtual Assistant

3.3.1 1E Support contact details

3.3.1.1 Support Web portal

Maintenance support customers can log onto the 1E Support Web Portal at https://support.1e.com/ using the login details provided with their maintenance contract. This provides issue tracking, product hotfixes, and knowledge base articles related to each product.

3.3.1.2 Telephone support

Maintenance support customers can contact the technical support department at 1E through the following support numbers. Just phone the relevant number for your area, so your call can be routed quickly and efficiently to the correct support group:

US/Canada:	1-866-349-4032 (Toll-Free)
	1-917-339-2360 (Standard)
UK/Europe:	+44 (0)208 326 3499
India:	+91 120 402 4002
Australia:	+61 739 111 118

3.3.1.3 Email support

Maintenance customers can use the following email for additional support. Evaluation customers can also use this email with the temporary access code that is provided through customercare@1e.com as part of their evaluation.

support@1e.com

3.3.2 The technical support process

Read through the Troubleshooting pages to see if there are known issues, or quick resolutions to any problems you may have encountered.

Maintenance support customers can use the 1E Support Web Portal to review knowledge base articles and download hotfixes.

If still encountering problems, create a technical report (log files and details) and then contact the 1E technical support team.

3.3.2.1 Creating a technical report

If possible, please obtain the following details and log files before contacting 1E, to include in your technical report.

3.3.2.1.1 Version details

The OS, version number, and patch level for:

Tachyon Servers

1E Client

Configuration Manager - if used

Other 1E Server software, for example, Shopping, Nightwatchman, and WakeUp.

For Nomad and Shopping, please provide OS, version number, and patch level for:

Configuration Manager DPs

Nomad extensions used on Configuration Manager Consoles

ActiveEfficiency Server.

3.3.2.1.2 Environmental details

If there were any recent changes made to your configuration

The name of the machines, Configuration Manager Application and/or Package IDs for when the issue occurred

3.3.2.1.3 Problem details

When did the issue occur, ensure log files cover this period

The scope of the issue – did it affect a particular geographical location, group of users, or client machines

Details of any self-help troubleshooting steps you carried out

In the event of a service crash or if you are experiencing high CPU or memory usage, provide us with the dump file, event viewer logs, and traces. We will provide you with FTP details to upload these files.

3.3.2.2 Log files

1E needs details of the recorded time when the issue took place. To ensure logs contain relevant details, please try to rerun the steps to replicate the issue.

Copies of the **AppImport.xml** files found in the folder where you ran 1E Client Deployment Assistant 8.1.

Copies of log files from: C:\ProgramData\1E\Client Deployment Assistant\LogFiles

1E Client logs on Windows

%ALLUSERSPROFILE%\1E\Client\1E.Client.log (used by 1E Client and Tachyon features, and Shopping client)

%ALLUSERSPROFILE%\1E\Client\NomadBranchUninstall-YYYY_MM_HHTMM_HH_SS_000Z.log

1E Client logs on macOS

/Library/Logs/1E.Client.Daemon.log (shows any service start errors)

/Library/Logs/1E.Client.log (shows the current operation of the 1E Client)

1E Client logs on other non-Windows platforms

/var/log/1E/Client/1E.Client.log

Nomad client log

%ALLUSERSPROFILE%\1E\NomadBranch\LogFiles\NomadBranch.log

PXE Everywhere Agent log

%ALLUSERSPROFILE%\1E\PXEEverywhere\PXEEverywhere.log

Shopping WSA client log

%ALLUSERSPROFILE%\1E\Client\WSA.log

WakeUp client log

%ALLUSERSPROFILE%\1E\Agent\WakeUpAgt.log

> **Note**
>
> By default, Windows resolves %ALLUSERSPROFILE% as C:\ProgramData\

3.3.3 Known issues

Issue	Description	Workaround
When Creating a Device Collection on the Agent screens the Limiting Collection may be missing	On an Agent screen an existing collection may be selected using the Browse button, but if a name is then typed into the Create/Select Device Collection field, the Limiting Collection will initially be missing.	Clicking or tabbing to another field will resolve the issue.
The CDA wizard may terminate with a program exception under certain circumstances.	If the connection to Configuration Manager is dropped after the initial connection test in the wizard has succeeded a program exception may occur if the connection is re-established.	You will need to check the status of Configuration Manager and confirm that it is up and running before re-trying to run the CDA wizard.
1E Clients are not being installed on Windows 11 devices.	Applcations > Deployment Types and Packages > Programs do not have the Windows 11 Operating System	The Windows 11 (64-bit) needs to be manually enabled in order to allow 1E

Issue	Description	Workaround
	enabled by default in Configuration Manager.	Clients to be installed on these devices.

3.4 Reference

This section contains all the reference material for 1E Client Deployment Assistant.

3.4.1 Supported Platforms

A list of prerequisites and dependencies you need to meet in order to run the 1E Client Deployment Assistant, and eventually install each of the 1E Client/agents.

3.4.1.1 1E Client Deployment Assistant 8.1

The following are required in order to run the 1E Client Deployment Assistant.

Category	Product	Notes
OS	Windows Server 2022 Windows Server 2019 Windows Server 2016 Windows 10 CB 21H2 Windows 11 CB 21H2 Windows 10 CB 21H1 Windows 10 CB 20H2	CDA can be run on these OS.
Runtime libraries	.NET Framework 4.8	CDA requires one of these versions of .NET Framework.
Configuration Manager	SCCM CB 2203	CDA optionally supports these versions of Microsoft Systems Center Configuration Manager.

Category	Product	Notes
	SCCM CB 2111	
	SCCM CB 2107	
	SCCM CB 2103	
	SCCM CB 2010	
Other		Please see: Below for individual client/agent requirements on client computers Infrastructure requirements for each client/agent.

3.4.1.2 1E Client 8.1

The following are required in order to install 1E Client on client computers. Some are only required for particular client modules and features. Some real-time client features of 1E Client are also supported on non-Windows platforms, however, the **1E Client Deployment Assistant** does not support using Configuration Manager to deploy 1E Client to non-Windows computers. Instead, please refer to Installation account for Windows.

3.4.1.2.1 Windows client

Category	Product	Notes
Operating System	Windows Server 2022	The zip for 1E Client for Windows is available for download from the support.1e.com/.
	Windows Server 2019	Professional and Enterprise editions are supported for Windows 10 and Windows 11.
	Windows Server 2016	All versions are provided with 32-bit & 64-installers, and can be installed on physical and virtual computers.
	Windows 11 CB 22H2	**Note** This list shows only those OS versions in mainstream support by Microsoft, and therefore supported by Tachyon, and by 1E Client 8.1. Please refer to Constraints of Legacy OS regarding the end of mainstream support.
	Windows 11 CB 21H2	
	Windows 10 CB 22H2	

Category	Product	Notes
	Windows 10 CB 21H2	For Microsoft product lifecycle details, please refer to https://support.microsoft.com/en-us/lifecycle/search. Refer to Support for Microsoft Rapid-Release Cycle on https://support.1e.com/ for details of which Current Branch versions are supported by 1E products, and known issues regarding specific versions. For installation guidance on Windows, please refer to Deploying 1E Client on Windows. The following 1E Client features and modules are supported on Windows OS: Real-time features (for example instructions, experience, interaction) Nomad client PXE Everywhere Agent client Shopping client Windows Servicing Assistant (WSA) client (workstation OS only, not server OS) WakeUp client
Runtime libraries	.NET Framework 4.8	.NET Framework is required only for the following features of 1E Client:
	Visual C++ 2015-2019 Redistributable	The Real-Time Control Center feature of the 1E Client (also known as 1E Client UI and Interaction module) supports Experience Engagements (Announcements and Surveys), and ITSM Support Tickets Windows Servicing Assistant (WSA) is a feature of the Shopping/WSA client module, which supports OS deployment, upgrades and migrations. **Note** This list shows only those .NET Framework versions in mainstream support by Microsoft,

Category	Product	Notes
		and therefore supported by 1E, and by 1E Client 8.1. For Microsoft product lifecycle details, please refer to https://support.microsoft.com/en-us/lifecycle/search. 1E Client installer includes the Visual C++ 2015-2019 Redistributable package.
Other Windows Software	Nomad 8.0 (or later) PowerShell 3.0 (or later)	1E Client provides real-time client features. It also includes the Nomad client module. Real-time client features can optionally use Nomad to download content (feature enabled by default) if the Nomad client module in 1E Client is enabled (module disabled by default) or Nomad 7.0 or later is running. For more details please refer to Nomad client requirements. PowerShell is not a prerequisite for installation of the 1E Client. PowerShell is used by some Tachyon instructions (that have PowerShell commands embedded or scripts that are downloaded) and some of these require PowerShell 3.0 or later.
Microsoft Endpoint Configuration Manager Client	MECM CB 2211 MECM CB 2207 MECM CB 2203 MECM CB 2111 MECM CB 2107	The following client features work with these versions of Configuration Manager on Windows computers: Real-time client - instructions used by Tachyon Configuration Manager Console extensions Nomad client PXE Everywhere Agent Shopping/WSA client WakeUp client - including Policy Refresh and REFRESHONSUBNETCHANGE features Configuration Manager is not a prerequisite for installation of the 1E Client, and except for above features, the 1E Client, its features and modules, have no dependency on Configuration Manager.

Category	Product	Notes
		Tachyon, Nomad, WakeUp, and Application Migration have Configuration Manager Console extensions which are available separately. **Note** This list shows only those Configuration Manager versions in mainstream support by Microsoft, and therefore supported by 1E, and by 1E Client 8.1. For Microsoft product lifecycle details, please refer to https://support.microsoft.com/en-us/lifecycle/search. Please refer to the Support for the Microsoft Rapid-Release Cycle on https://support.1e.com/ for details of which Current Branch versions are supported by 1E products, and known issues regarding specific versions. (Microsoft Endpoint Configuration Manager - MECM - is also known as Configuration Manager, ConfigMgr, Config Man, CM, and SCCM among other names. Version names include 2012 and Current Branch or CB.)

3.4.1.3 1E NightWatchman Agent 7.3

The following are required in order to install 1E NightWatchman Agent on client computers. NightWatchman is also supported on macOS, however the **1E Client Deployment Assistant** does not support using Configuration Manager to deploy NightWatchman Agent to non-Windows computers.

Category	Product	Notes
OS	Windows 10 CB 21H2 Windows 11 CB 21H2 Windows 10 CB 21H1	Installs on these OS. 1E NightWatchman Agent does not install on server OS. CDA only creates deployment types for workstations which can be fine-tuned. Does not require .NET Framework.

Category	Product	Notes
	Windows 10 CB 20H2	
	Windows 10 CB 2004	
	Windows 10 CB 1909	
	Windows 10 CB 1903	
	Windows 10 CB 1809	
	Windows 10 CB 1803	
Configuration Manager	SCCM CB 2111	1E NightWatchman Agent feature MonitorJobs works with these versions of Configuration Manager.
	SCCM CB 2107	
	SCCM CB 2103	
	SCCM CB 2010	
	SCCM CB 2006	
	SCCM CB 2002	
	SCCM CB 1910	
	SCCM CB 1906	
	SCCM CB 1902	

Category	Product	Notes
	SCCM CB 1810	

3.4.1.4 Constraints of Legacy OS

1E does not provide support for 1E products on the following OS unless the OS is explicitly listed as being supported for a specific 1E product or product feature. This is because Microsoft has ended mainstream support for these OS or they are not significantly used by business organizations.

Windows XP *	**Windows Server 2003 ***
Windows Vista	**Windows Server 2008**
Windows 7	**Windows Server 2008 R2**
Windows 8.0	**Windows Server 2012**
Windows 8.1	**Windows Server 2012 R2**

Note

1E Client 8.1 and later will not install on Windows XP and Windows Server 2003. Please contact 1E if you intend to continue using any of the other legacy OS. If you experience an issue, then please try replicating the issue on a supported OS.

For Microsoft product lifecycle details, please refer to https://support.microsoft.com/en-us/lifecycle/search.

3.4.2 Installer properties

A list of installer properties included in the base MST files included with 1E Client Deployment Assistant – for the 1E Client (which includes clients for Tachyon, Shopping, WakeUp and Nomad), and NightWatchman Agent.

Where the list indicates an installer property is in the AppImport.xml file, it means the CDA wizard will include add it to the MST transform file if it is not already there.

For details of additional installer properties available for each client, please refer to their respective product documentation, however any additional properties are not supported by the CDA Wizard, but can be manually added to a MST transform file as described in Advanced configuration.

1E Client installer zips

/document/preview/712367#UUID-6a06ae62-a7cb-32ae-9448-414ef934fa33

3.4.2.1 1E Client installer properties - general

Note

These settings affect 1E Client and also affect Tachyon features of 1E Client.

Note

Settings shown in 1E Client mixed-case are stored in the configuration file. Settings in UPPERCASE are stored in the Windows registry.

Property	Default value	Notes
INSTALLDIR	%PROGRAMFILES%\1E\Client	Where to install the 1E Client. The registry name is InstallationDirectory which must not be changed after installation.
LogPath	%ALLUSERSPROFILE%\1E\Client\1E.Client.log	Log file path Can be updated in *AppImport.xml* This log is used by 1E Client, Tachyonfeatures, and Shopping client. Please refer to Log files
LoggingLevel	Info	Log level Can be updated in *AppImport.xml*
REBOOT	ReallySuppress	Suppress the host from rebooting after installation. Cannot be updated in *AppImport.xml* – Advanced configuration The REBOOT property is not in the base MST but is in the install command-line for Nomad in the answer file.

3.4.2.2 1E Client installer properties - platform client

Property	Default value	Notes
Switch	tachyon.acme.local:4000	Switch

Property	Default value	Notes
		Can be updated in *AppImport.xml* **Note** Must have a value in order to enable platform client features. Must be set to **none** if Tachyon feature are not required.
BackgroundChannelUrl	https://tachyon.acme.local:443/Background/	Background channel URL Can be updated in *AppImport.xml* **Note** Must have a value in order to enable platform client features. Must be set to **none** if Tachyon feature are not required.

Property	Default value	Notes
DefaultStaggerRangeSeconds	300	Default stagger range in seconds Can be updated in *AppImport.xml*
Module.Inventory.Enabled	true	Enable Inventory module Can be updated in *AppImport.xml*
Module.Interaction.Enabled	true	Enable Interaction module (Client UI used for Surveys feature) Can be updated in *AppImport.xml*
Module.Interaction.Port	7766	Port used by the Interaction module (Client UI) Can be updated in *AppImport.xml*
Module.Interaction.DoNotDisturb	false	Enable the Interaction Do Not Disturb feature Can be updated in *AppImport.xml*
Module.Interaction.NotificationIcon	true	Enable the Interaction Notification icon Can be updated in *AppImport.xml*

Property	Default value	Notes
Module.Interaction.SampleUserInteraction	true	Enable the Interaction sampling feature Can be updated in *AppImport.xml*
AuthenticationPolicy	optional	Authentication policy Can be updated in *AppImport.xml*
ConnectionKeepaliveTimeInSecondsMax	600	Maximum time for sending a keep-alive message to the Switch Can be updated in *AppImport.xml*
ConnectionKeepaliveTimeInSecondsMin	120	Minimum time for sending a keep-alive message to the Switch Can be updated in *AppImport.xml*
ConnectionRetryTimeInSecondsMax	900	Maximum time the Agent waits before trying to reconnect to a Switch after a connection failure Can be updated in *AppImport.xml*
ConnectionRetryTimeInSecondsMin	30	Minimum time the Agent waits before trying to reconnect to a Switch after a connection failure

Property	Default value	Notes
		Can be updated in *AppImport.xml*
ConnectionTimeout	30	The maximum time in seconds that can elapse between initialising the connection and having a fully established websocket Can be updated in *AppImport.xml*
CRLChecks	soft	Carry out CRL (certificate revolcation list) checks Can be updated in *AppImport.xml*
CrlTimeoutInSeconds	3	**Note** This setting is not supported as an installer property. It is in the AppImport .xml and in the base MST file for 1E Client, but is not used.
EnablePayloadCompression	true	Whether the Agent should attempt to

Property	Default value	Notes
		compress payloads when responding to instructions Can be updated in *AppImport.xml*
NomadContentDownloadEnabled	true	Whether to integrate with Nomad for content download Can be updated in *AppImport.xml*
NomadContentDownloadTimeoutSecs	600	Time limit to wait for Nomad to download content before switching to Tachyon own download mechanism Can be updated in *AppImport.xml*
SSL	TLSv1.2	Switch connection security Can be updated in *AppImport.xml*
WorkerThreads	2	Number of instructions that will execute concurrently Can be updated in *AppImport.xml*

3.4.2.3 1E Client installer properties - 1E Client client

Property	Default value	Notes
Module.Nomad.Enabled	false	Enable Nomad client module Can be updated in *AppImport.xml*
MODULE.NOMAD.BLOCKSIZE	131072	Minimum size of each block of data Nomad copies from the package source folder. Can be updated in *AppImport.xml* Registry value: *BlockSize*
MODULE.NOMAD.DOREPORTINGENABLED	false	Delivery Optimization (DO) Reporting (disabled by default). Can be updated in *AppImport.xml* Registry value: *DeliveryOptimizationReportingEnabled*
MODULE.NOMAD.LOGPATH	[WindowsFolder]\CCM\Logs	Folder containing Nomad log file. Can be updated in *AppImport.xml* Registry value: *LogFileName* (registry folder plus file name) Please refer to Log files.
MODULE.NOMAD.MAXLOGSIZE	5242880 (5 MB)	Maximum log size. Can be updated in *AppImport.xml* (1MB, 5MB,10MB) Registry value: *MaxLogFileSize*
MODULE.NOMAD.P2PENABLED	9	Peer-to-peer support (enabled with smb with net literal names by default). Cannot be updated in *AppImport.xml* – #UUID01a4b01f25464b0c7dcbc2ce1d6ce3a3_id_AdvancedconfigurationAdditionalinstallerconfiguration Registry value: *P2PEnabled*

<table>
<tr><th>Property</th><th>Default value</th><th>Notes</th></tr>
<tr><td>MODULE.NOMAD.P2PHTTPPORT</td><td>5080</td><td>Default HTTP port to use for peer copy.

Can be updated in AppImport.xml

Registry value: P2PHttpPort</td></tr>
<tr><td>MODULE.NOMAD.P2PHTTPSPORT</td><td>5443</td><td>Default HTTPS port to use for peer copy.

Can be updated in AppImport.xml

Registry value: P2PHttpsPort</td></tr>
<tr><td>MODULE.NOMAD.MAXALLOCREQUEST

MODULE.NOMAD.MAXIMUMMEGABYTE</td><td>Disabled</td><td>Peer backup assistant support.

Can be updated in AppImport.xml (when enabled, both MAXALLOCREQUEST and MAXIMUMMEGABYTE = 5120)

Registry value: NMDS\MaxAllocRequest * NMDS\MaximumMegabyte</td></tr>
<tr><td>MODULE.NOMAD.SPECIALNETSHARE</td><td>Default value in MSI is: 0x2060 (8286) - revised 8.1

Default value used by CDA is: 0x2070 (8304)</td><td>Can be partly updated in AppImport.xml (Nomad hidden share & FanOut)

Registry value: SpecialNetShare

<table>
<tr><th>Bit</th><th>Hex</th><th>Decimal</th><th>Notes</th></tr>
<tr><td>4</td><td>0x0010</td><td>16</td><td>Enable Nomad hidden share as NomadSHR$.</td></tr>
<tr><td>5</td><td>0x0020</td><td>32</td><td>Disable broadcast of download statistics. When enabled, Nomad broadcasts download statistics to all peers when a download is complete.</td></tr>
<tr><td>6</td><td>0x0040</td><td>64</td><td>Enable Nomad FanOut.</td></tr>
<tr><td>13</td><td>0x2000</td><td>8192</td><td>Use HTTP/S or SMB. HTTP/S is automatically used if CM client is detected. Must be set if using CM2007 or if</td></tr>
</table>
</td></tr>
</table>

Property	Default value	Notes
		Nomad integration is used by Tachyon.
		0x2070 8304
MODULE.NOMAD.SSDENABLED	3	Single-site download (enabled as both consumer and provider by default). Can be updated in *AppImport.xml* Registry value: *SSDEnabled*
MODULE.NOMAD.SSPBAENABLED	0	Single-site peer backup assistant (disabled by default). Can be updated in *AppImport.xml* Registry value: *SSPBAEnabled*
MODULE.NOMAD.STATUSMSGEVENTS	0x0	Status message events. Cannot be updated in *AppImport.xml* – #UUID01a4b01f25464b0c7dcbc2ce1d6ce3a3_id_AdvancedconfigurationAdditionalinstallerconfiguration Registry value: *StatusMsgEvents* Please refer to Advanced configuration for how to use Orca to edit the base MST file to change this setting.
MODULE.NOMAD.SUCCESSCODES	Enabled	Prevent failover to BITS (0x9999 added to default SuccessCodes). Can be updated in *AppImport.xml* Registry value: *SuccessCodes*
MODULE.NOMAD.USEFIPS	false	Use FIPS encryption. Can be updated in *AppImport.xml - FIPSEncryption* Registry value: *EncryptionType*
MODULE.NOMAD.COMPATIBILITYFLAGS	1572864	Enable compatibility checks.

Property	Default value	Notes
	Default value in MSI is: 0x2020 Default value used by CDA is: *0x2070*	Cannot be updated in *AppImport.xml* – #UUID01a4b01f25464b0c7dcbc2ce1d6ce3a3_id_AdvancedconfigurationAdditionalinstallerconfiguration Registry value: *CompatibilityFlags*
MODULE.NOMAD.PLATFORMURL MODULE.NOMAD.CONTENTREGISTRATION	User defined	ActiveEfficiency server. Can be updated in *AppImport.xml* Registry value: *ActiveEfficiency\PlatformUrl* *ActiveEfficiency\ContentRegistration*

3.4.2.4 1E Client installer properties - PXE Everywhere Agent

Property	Default value	Notes
Module.PXEEverywhere.Enabled	false	Enable PXE Everywhere Agent module Can be updated in *AppImport.xml*
MODULE.PXEEVERYWHERE.CONFIGSERVERURL	http://pxe.contoso.com/PXELite/PXELiteConfiguration.asmx	Enable PXE Everywhere Agent module Can be updated in *AppImport.xml*
MODULE.PXEEVERYWHERE.LOGPATH	[WindowsFolder]\CCM\Logs	Folder containing PXE Everywhere

Property	Default value	Notes
		Agent log file. Can be updated in *AppImport.xml*
MODULE.PXEEVERYWHERE.MAXLOGFILESIZE	10485760	Maximum size of the PXE Everywhere Agent log file. Can be updated in *AppImport.xml*
WindowsADKLocation	C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit	This is not an installer property Determines the location of the ADK files to allow CDA to build the PXE boot image
MODULE.PXEEVERYWHERE.USEFIPS	false	Enable FIPS encryption Can be updated in *AppImport.xml - FIPSEncryption*

3.4.2.5 1E Client installer properties - Shopping client

Property	Default value	Notes
Module.Shopping.Enabled	false	Enable Shopping client module Can be updated in *AppImport.xml*
Module.Shopping.ShoppingCentralUrl	(empty)	Shopping Web URL Can be updated in *AppImport.xml*
Module.Shopping.LoopbackExemptionEnabled	false	Enable Edge / Windows app browser support Can be updated in *AppImport.xml*
Module.Shopping.LocalhostUrl	(empty)	Cannot be updated in *AppImport.xml* – Advanced configuration

3.4.2.6 1E Client installer properties - WakeUp client

Property	Default value	Notes
Module.WakeUp.Enabled	false	Enable WakeUp client module Can be updated in *AppImport.xml*
MODULE.WAKEUP.LOGPATH	[WindowsFolder]CCM\Logs	Set the path for the WakeUp Agent logfile Can be updated in *AppImport.xml*
MODULE.WAKEUP.MAXLOGFILESIZE	5242880	Set the size of the WakeUp Agent logfile Can be updated in *AppImport.xml*
MODULE.WAKEUP.REPORTING	OFF	Enable WakeUp status message reporting to a NightWatchman server Can be updated in *AppImport.xml*

Property	Default value	Notes
		Can also be set in registry by setting HKLM\Software\1E\WakeUpAgt Reporting REG_SZ value to "ON"
MODULE.WAKEUP.REPORTINGSERVER	(empty)	Can be updated in *AppImport.xml* Can also be set in registry by setting HKLM\Software\1E\WakeUpAgt\Reporting\HTTP ServiceUrl REG_SZ value
MODULE.WAKEUP.SECUREREPORTINGSERVER	(empty)	Can be updated in *AppImport.xml* *Can also be set in registry by setting HKLM\Software\1E\WakeUpAgt\Reporting\HTTPS ServiceUrl REG_SZ value*
MODULE.WAKEUP.USEFIPS	0 (off)	Enable FIPS compliance in WakeUp module Can be updated in *AppImport.xml* Can also be set in registry by setting HKLM\Software\1E\WakeUpAgt\Reporting UseFipsComplianceEncryption REG_DWORD value to 1

3.4.2.7 1E NightWatchman Agent installer properties

Property	Default value	Notes
REBOOT	ReallySuppress	Suppress the host from rebooting after installation. Cannot be updated in *AppImport.xml* – Advanced configuration The REBOOT property is not in the base MST but is in the install command-line for PXE Everywhere in the answer file.

3.4.3 1E Client Deployment Assistant release information

3.4.3.1 1E Client Deployment Assistant 8.1 release notes – last updated 03-August-2022

These release notes contain late-breaking information about 1E Client Deployment Assistant 8.1. For the most up-to-date information, see the online release notes and Known issues.

3.4.3.2 New Features

The 1E Client Deployment Assistant 8.1 release introduces the following features:

CDA now uses .NET Framework 4.8

This release includes the following changes:

Updated products and Accumulated Hotfixes (Patches)

1E Client Deployment Assistant 8.1 includes the following product versions:

1E Client 8.1.2.62 (includes clients for Nomad, PXE Everywhere, Shopping/WSA, WakeUp, and Tachyon) (new)

1E NightWatchman Agent 7.3.0.774

Accumulated Hotfixes (Patches) included:

None

> **Note**
>
> CDA only supports single patch installation, that is you can only have one .msp file per client. In practice this shouldn't be an issue as cumulative patches are created across all the 1E products, so only one patch should be needed anyway.
>
> Please check the 1E Support Portal to see if there is a later Accumulated Hotfix (Patch):

1E Client v8.1.2.62 - https://1eportal.force.com/s/1eclienttopicdetail

1E NightWatchman Agent v7.3.0.774 - https://1eportal.force.com/s/nightwatchmantopicdetail

3.4.3.3 1E Client Deployment Assistant release history

3.4.3.3.1 8.1.2.19 - Web Release (19 Apr 2022)

Products included:

1E Client 8.1.2.62 (includes clients for Nomad, PXE Everywhere, Shopping/WSA, WakeUp, and Tachyon) **(new)**

1E NightWatchman Agent 7.3.0.774

Accumulated Hotfixes (Patches) included:

None

3.4.3.3.2 8.0.4.8 - Web Release (5 Nov 2021)

Products included:

1E Client 8.0.4.261(includes clients for Nomad, PXE Everywhere, Shopping/WSA, WakeUp, and Tachyon) **(new)**

1E NightWatchman Agent 7.3.0.774

Accumulated Hotfixes (Patches) included:

MSP-Q21807-1EClient.Accumulated.v8.0.4.261

3.4.3.3.3 1.6.0.21 - Web Release (5 May 2021)

Web WakeUp ActiveX removed

Products included:

1E Client 5.2.5.523 (includes clients for Nomad, PXE Everywhere, Shopping/WSA, WakeUp, and Tachyon) **(new)**

1E NightWatchman Agent 7.3.0.774

Accumulated Hotfixes (Patches) included:

MSP-Q21471-1EClient.Accumulated.v5.2.5.523 **(new)**

3.4.3.3.4 1.5.0.28 - Web Release (19 August 2020)

PXE Everywhere removed - PXE Everywhere is now a client module of 1E Client

Products included:

1E Client 5.1.0.922 (includes clients for Nomad, PXE Everywhere, Shopping/WSA, WakeUp, and Tachyon) **(new)**

1E NightWatchman Agent 7.3.0.774

Web WakeUp ActiveX 7.3.0.5

Accumulated Hotfixes (Patches) included:

MSP-Q21142-1EClient.Accumulated.v5.1.0.922 **(new)**

3.4.3.3.5 1.4.300.5 - Web Release (21 July 2020)

Updated products and Accumulated Hotfixes (Patches)

Products included:

1E Client 5.0.0.745 (includes clients for Nomad, Shopping/WSA, WakeUp, and Tachyon)

PXE Everywhere 3.2.0.56

1E NightWatchman Agent 7.3.0.774 **(new)**

Web WakeUp ActiveX 7.3.0.58 **(new)**

Accumulated Hotfixes (Patches) included:

MSP-Q21071-1EClient.Accumulated.v5.0.0.745 **(new)**

MSP-Q20742-PXELite.Server.Accumulated.v3.2.0.56

3.4.3.3.6 1.4.200.4 - Web Release (4 May 2020)

Support for Accumulated Hotfixes (Patches)

Minor improvements in CDA

Products included:

1E Client 5.0.0.745 (includes clients for Nomad, Shopping/WSA, WakeUp, and Tachyon)

PXE Everywhere 3.2.0.56

1E NightWatchman Agent 7.2.500.721

Web WakeUp ActiveX 7.2.500.34

Accumulated Hotfixes (Patches) included:

MSP-Q21005-1EClient.Accumulated.v5.0.0.745 **(new)**

MSP-Q20742-PXELite.Server.Accumulated.v3.2.0.56 **(new)**

MSP-Q20635-1ENightWatchmanAgent.Accumulated.v7.2.500.721 **(new)**

3.4.3.3.7 1.4.100.9 - Web Release (20 Mar 2020)

1E Client 4.1 replaced by 1E Client 5.0

Products included:

1E Client 5.0.0.745 (includes clients for Nomad, Shopping/WSA, WakeUp, and Tachyon) **(new)**

PXE Everywhere 3.2.0.56

1E NightWatchman Agent 7.2.500.721

Web WakeUp ActiveX 7.2.500.34

3.4.3.3.8 1.4.0.27 - Web Release (21 June 2019)

Renamed from Endpoint Agent Installation (EAI) Solution Accelerator to 1E Client Deployment Assistant (CDA)

1E Client added (includes clients for Nomad, Shopping/WSA, WakeUp, and Tachyon)

Tachyon Agent is replaced by 1E Client

Nomad removed - Nomad is now a client module of 1E Client

Products included:

1E Client 4.1.0.267 (includes clients for Nomad, Shopping/WSA, WakeUp, and Tachyon) **(new)**

PXE Everywhere 3.2.0.56

1E NightWatchman Agent 7.2.500.721

Web WakeUp ActiveX 7.2.500.34

3.4.3.4 Endpoint Agent Installation solution accelerator release history

3.4.3.4.1 1.3.0.13 - Support Release (11 Apr 2019)

Updated Tachyon Agent, Nomad and PXE Everywhere

Products included:

Tachyon Agent 4.0.0.580 (includes clients for Shopping/WSA, WakeUp, and Tachyon) **(new)**

Nomad 6.3.201.6 **(new)**

PXE Everywhere 3.2.0.56 **(new)**

1E NightWatchman Agent 7.2.500.72

Web WakeUp ActiveX 7.2.500.34

3.4.3.4.2 1.3.0.1 - Web Release (08 Oct 2018)

1E Agent removed

WakeUp client is now a client module of Tachyon Agent

NightWatchman client is replaced by 1E NightWatchman Agent

Products included:

Tachyon Agent 3.3.0.1033 (includes clients for Shopping/WSA, WakeUp and Tachyon) **(new)**

Nomad 6.3.201.6

PXE Everywhere 3.1.300.5

1E NightWatchman Agent 7.2.500.721 **(new)**

Web WakeUp ActiveX 7.2.500.34 **(new)**

3.4.3.4.3 1.2.1.8 - Web Release (01 Jun 2018)

Products included:

Tachyon Agent 3.2.0.638 (includes clients for Shopping/WSA and Tachyon) **(new)**

Nomad 6.3.201.6 **(new)**

PXE Everywhere 3.1.300.5

1E Agent 7.2.0.156 **(new)**

Web WakeUp ActiveX 7.2.0.33

3.4.3.4.3.1 1.2.1.6 - Support Release (27 Apr 2018)

Added Tachyon Agent

Removed Shopping Agent - Shopping Agent is now a client module of Tachyon Agent

Products included:

Tachyon Agent 3.2.0.618 (includes Shopping module to provide WSA and replace the Shopping Agent) **(new)**

Nomad 6.3.200.123 **(new)**

PXE Everywhere 3.1.300.5

1E Agent 7.2.0.156

Web WakeUp ActiveX 7.2.0.33

3.4.3.4.3.2 1.1.1.70 - Support Release (16 Jan 2018)

Updated Nomad 6.3.200.82

3.4.3.4.4 1.1.1.59 - Web Release (07 Nov 2017)

Updated Nomad 6.3.100.20

3.4.3.4.4.1 1.1.1.52 - Support Release (02 Oct 2017)

Updated Nomad 6.3.0.90

3.4.3.4.5 1.1.1.49 - Web Release (17 Aug 2017)

Updated 1E Agent 7.2.0.156

Updated Web WakeUp ActiveX 7.2.0.33

3.4.3.4.6 1.1.1.46 - Web Release (30 Mar 2017)

Updated Nomad 6.2.200.6

Updated 1E Shopping Agent 1.0.200.11

3.4.3.4.6.1 1.1.1.44 - Support Release (24 Mar 2017)

Updated Nomad 6.2.200.5

Updated PXE Everywhere 3.1.300.5

3.4.3.4.6.2 1.1.1.41 - Support Release (10 Mar 2017)

Updated Nomad 6.2.100.5

Updated PXE Everywhere 3.1.300.4

3.4.3.4.6.3 1.1.1.32 - Support Release (03 Feb 2017)

Updated Nomad 6.2.0.296

3.4.3.4.6.4 1.1.1.22 - Support Release (02 Feb 2017)

Updated Nomad 6.2.0.290

3.4.3.4.7 1.1.1.16 - Web Release (04 Nov 2016)

Updated Nomad 6.1.100.116

3.4.3.4.8 1.1.1.10 - Web Release (02 Sep 2016)

Updated Nomad 6.1.0.142

Updated PXE Everywhere 3.1.200.4

3.4.3.4.9 1.1.0.47140 - Web Release (30 May 2016)

Updated Nomad 6.0.200.25891

Updated PXE Everywhere 3.1.100.46309

Updated 1E Agent 7.1.0.263

Updated Web WakeUp ActiveX 7.1.0.12

Updated 1E Shopping Agent 1.0.100.2

3.4.3.5 CDA features by release

3.4.3.5.1 New in 1E Client Deployment Assistant 8.1

The 1E Client Deployment Assistant 8.1 release introduces the following features:

CDA now uses .NET Framework 4.8

This release includes the following changes:

Updated products and Accumulated Hotfixes (Patches)

1E Client Deployment Assistant 8.1 includes the following product versions:

1E Client 8.1.2.62 (includes clients for Nomad, PXE Everywhere, Shopping/WSA, WakeUp, and Tachyon) (new)

1E NightWatchman Agent 7.3.0.774

Accumulated Hotfixes (Patches) included:

None

> **Note**
>
> CDA only supports single patch installation, that is you can only have one .msp file per client. In practice this shouldn't be an issue as cumulative patches are created across all the 1E products, so only one patch should be needed anyway.
>
> Please check the 1E Support Portal to see if there is a later Accumulated Hotfix (Patch):

1E Client v8.1.2.62 - https://1eportal.force.com/s/1eclienttopicdetail

1E NightWatchman Agent v7.3.0.774 - https://1eportal.force.com/s/nightwatchmantopicdetail

3.4.3.5.2 Features released in version 8.1

CDA now uses .NET Framework 4.8

3.4.3.5.3 Features released in version 8.0

Version number of CDA is now inline with the version of 1E Client

CDA can run independently of Microsoft Endpoint Configuration Manager

3.4.3.5.4 Features released in version 1.6

Web WakeUp ActiveX removed

3.4.3.5.5 Features released in version 1.5

PXE Everywhere removed - PXE Everywhere Agent is now a client module of 1E Client

3.4.3.5.6 Features released in version 1.4.300

Updated products and Accumulated Hotfixes (Patches)

3.4.3.5.7 Features released in version 1.4.200

Patches are now supported for the products. This version supports the installation of patches (.msp) alongside their corresponding client installer files (.msi). The latest released patch for each client is now packaged along with the .msi in each new CDA release. Patches can only be installed alongside the .msi. That is the patching can't be done using CDA after the client has been installed. If you want to apply patch to a client that is different to the packaged one, the existing .msp file must be replaced by your new one, this is located in the client's installation folder under the **Agent Installation Files** folder in the CDA artifact. This must be done prior to launching the CDA installer. For more details, please refer to Using client patch files with CDA.

3.4.3.5.8 Features released in version 1.4.100

1E Client 4.1 replaced by 1E Client 5.0 (includes clients for Nomad, Shopping/WSA, WakeUp, and Tachyon)

3.4.3.5.9 Features released in version 1.4.0

The main 1.4.0 release included the following features:

Renamed from Endpoint Agent Installation (EAI) Solution Accelerator to 1E Client Deployment Assistant

1E Client added (includes clients for Nomad, Shopping/WSA, WakeUp, and Tachyon)

Tachyon Agent is replaced by 1E Client

Nomad removed - Nomad is now a client module of 1E Client

Other products updated

3.4.3.5.10 Features released in version 1.3.0

1E Agent removed

WakeUp is now a client module of Tachyon Agent

NightWatchman is replaced by 1E NightWatchman Agent

Other products updated

3.4.3.5.11 Features released in version 1.2.8

Tachyon Agent added

Shopping Agent removed - Shopping Agent and Windows Servicing Assistant are now client modules of Tachyon Agent

Shopping Client Identity removed

Other products updated

3.4.3.5.12 Features released in version 1.1.1

Endpoint Agent Installation (EAI) Solution Accelerator provides a single wizard interface covering the following agents:

Nomad – the wizard also adds a file to the Nomad cache to prevent it from being scanned for installed software during Configuration Manager inventory.

PXE Everywhere – the wizard also builds a PXE boot image and related files in order to service PXE requests and runs *CreateBCD.exe* to copy an advertised PXE boot image to the PXE Everywhere cache within a task sequence - thereby reducing the manual configuration required post-installation

1E Agent – NightWatchman and WakeUp

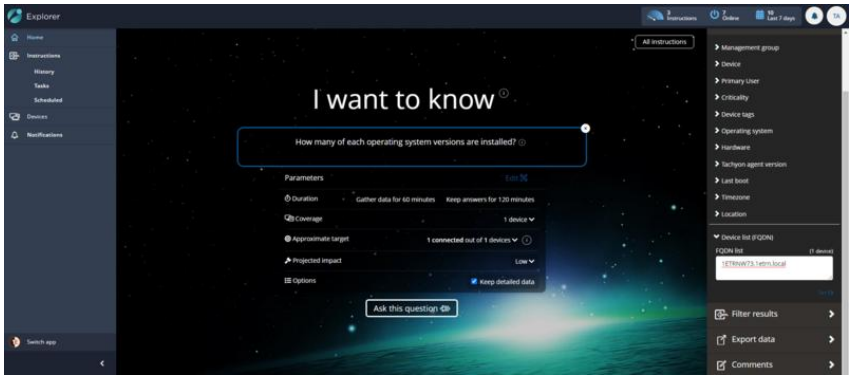
Shopping Client Identity

1E Shopping Agent

Web WakeUp ActiveX Control

4 Tachyon Explorer

Tachyon Explorer is the front-end to the real-time aspects of Tachyon. It lets you interactively ask questions, run actions and view responses. You can also use it to view the connected client devices.



4.1 Introducing Tachyon Explorer

An overview of Explorer is presented; what it does and how it can benefit your organization.

4.1.1 Tachyon Explorer features

Explorer gives you the ability to investigate, remediate issues and manage operations across all your endpoints in real time. For more information, please refer to Using Tachyon Explorer.

Here's an overview of the features available in the Explorer application.

4.1.1.1 Questions, actions and their responses

Explorer lets you directly question connected devices to retrieve responses, run actions, and get real-time information from them. The Explorer front-end capabilities ensure fast querying, investigation, and remediation.

The questions, responses and actions feature includes:

Graphical display of response information

Instruction impact assessment

Response history.

Note

For more information on Instructions and their responses, please refer to:

ExplorerHome page, questions and responses

Question parameters

Instructions

History.

4.1.1.2 Exporting data from Tachyon Explorer

Results visible in Explorer can be exported to files containing comma-separated values (CSV) or, in the case of the **Export all** option on the instruction response page, tab-separated values (TSV), and results can be marked for export at the point of asking a question to automate the process. Explorer lets you export the data on a number of pages to CSV files:

Instruction history

Responses - you can export a single page or all results once the Instruction has finished gathering responses - these can then be used for auditing purposes or to drive external programs

Drill-down responses

Device information.

Note

For more information on exporting data from Explorer, please refer to:

Exporting data from Explorer.

4.1.1.3 Coverage, question filters, view filters and follow-on instructions

Questions and responses can be tailored to focus on specific ranges of devices through the use of coverage and filters:

Coverage acts first to let you restrict the devices that will be asked a given question

Question filters act before devices have responded to narrow the responses that are sent

View filters act after the responses have been sent to focus the responses presented to the user and to determine the input into the follow-on instructions

The responses to initial questions can be further refined by asking follow-on questions or actions, allowing questioners and actioners to focus in on the results they want to see.

> **Note**
>
> For more information on coverage, question filters, view filters and follow-on instructions, please refer to:

Coverage, question filters and view filters

Limiting coverage using a Management group - tutorial

Refining responses with follow-up questions.

4.1.1.4 Approval workflow

To enhance the safety of running actions in the Tachyon system, there is an approval workflow that ensures that every Tachyon action requires the approval of designated approvers before it can be run. To make it even safer, someone with approval permissions cannot approve their own action.

When an attempt is made to run an action, the Tachyon approval workflow sends an email and a notification to all the approvers associated with the action. Any of the approvers may approve or reject the request to run the action.

> **Note**
>
> For more information on the Approval workflow, please refer to:

The action approval workflow

Performing an action - tutorial.

4.1.1.5 Authentication

Users must provide their user credentials when attempting to run an action, this prevents unauthorized access by a third party attempting to make use of an unattended computer.

Actions can also be configured to require two-factor authentication. This is where the user attempting to run an action is challenged to enter a unique, one-time authorization code that has been sent to them by an alternative method such as email or a registered mobile.

> **Note**

For more information on authentication, please refer to:

Two-factor authentication.

4.1.1.6 Task-based organization for accessing and scheduling instructions

Tachyon provides a way of accessing the questions and actions that is organized around the way that network administrators typically interact with their network. This interface also lets you run the Instruction using a schedule.

The **Explorer**→**Instructions**→**Tasks** page in Explorer provides a structured view of the instructions defined in the Product Pack. It also lets you schedule the tasks so they can be run in the future or according to a particular schedule.

4.1.1.7 Using task groups

The benefit of using **Tasks** lies in the task group structure that is defined in the Product Pack. It is this structure that enables you to focus in on specific task areas to find the particular instruction that you want.

For example you may be interested in instructions related to particular software vendor's products. Depending on the Instructions that you have uploaded to your Tachyon system you may see the following structure:

At the top-level there is a **Software Vendors** task group whose children are **1E** and **Microsoft**.

Underneath the **1E** task group there is a **Tachyon** group that contains **Configuration**, **Diagnostics** and **Verification** groups as well as a couple of Instructions.

Underneath the **Microsoft** task group is the **Configuration Manager** task group containing Instructions related to that product.

Note

For more information on using Task groups to access and schedule Instructions, please refer to:

Tasks

Scheduling instructions

Scheduling instructions - a tutorial.

4.1.1.8 Inventory and connectivity

The **Devices** page in the Explorer shows you all the devices that have connected with Tachyon and their current connection status. There are two views provided that let you research the devices: the devices table and the devices dashboard, please refer to The Devices Table and The Devices Dashboard for more details.

Note

For more information on inventory and connectivity, please refer to:

Investigating Devices

Using the Devices dashboard - Tutorial.

4.2 Planning for Tachyon platform

For information about planning your implementation, please refer to Planning for Tachyon.

4.3 Installing Tachyon Explorer

Tachyon Explorer is an application that is part of Explorer platform and is installed using Tachyon Setup. For more information on installing the platform, please refer to Installing Tachyon.

For more information on uploading Product Packs for use in Explorer, please refer to the following pages.

4.3.1 Tachyon Product Pack Deployment Tool

A description of the Tachyon Product Pack Deployment Tool (PPDT).

The PPDT can be used to upload multiple Classic and Integrated Product Packs into Tachyon.

The PPDT is found in the Product Packs folder of the Tachyon Platform zip, please refer to the Tachyon Platform zip for more details, and with appropriate permissions. Once the zip has been extracted, the tool can be used to upload any Classic and Integrated Product Packs found in its folder structure. Ensure you use the same version of the tool to match the version of Tachyon.

Classic Product Packs

Classic Product Packs contain instructions, for use in Explorer and other Tachyon applications.

Classic Product Packs can also be uploaded using the Settings app→ Instructions → Instruction Sets, described in Tachyon Platform - Instructions Menu, this method does not assign instructions to any instruction set. Settings can also be used to export instructions.

Hyphens

The tool creates an instruction set with the same name as its zip.

When creating or updating an instruction set, the tool converts hyphens to spaces. Hyphens can be included in names of Instruction sets, but they are converted by the tool. Older versions of the tool removed hyphens.

The Settings application keeps hyphens and spaces in the zip name when downloading (exporting) an instruction set. If the tool is then used to re-upload the same pack the hyphens are lost, creating a new instruction set with a different name to the original.

Individual Product Packs are not versioned, however each instruction has its version stored in the instruction definition.

Integrated Product Packs	Integrated Product Packs contain policies, rules and fragments for use by Guaranteed State, and may also include instructions. If the Product Pack contains instructions associated with the policies, the tool creates an instruction set using the name in its manifest file.

When the tool is used to upload new versions of instructions, then the updated instructions remain in their current instruction set, they are not moved to the new set created by the tool.

4.3.1.1 Getting started

To run the tool you need the following:

4.3.1.1.1 Account permissions

The account used to run the **Tachyon.ProductPackDeploymentTool.exe** must:

have local administrator rights on the computer it is running on

exist as a user with the following administrator rights:

Guaranteed State administrator

Instruction Set administrator.

4.3.1.1.2 Locating the Tachyon Product Pack Deployment Tool

This is now included in the Tachyon Platform zip file under the ProductPacks folder.

This folder holds the **Tachyon.ProductPackDeploymentTool.exe** (and its supporting files) used to upload the Classic and Integrated Product Packs into Tachyon.

It will create a log file called **Tachyon.ProductPackDeploymentTool.log** in the same folder.

4.3.1.1.3 What's in the ProductPacks folder?

The ProductPacks folder contains two directories, **Classic** and **Integrated**.

The **Classic** directory holds a number of Classic Product Packs that contain Tachyon Instructions.

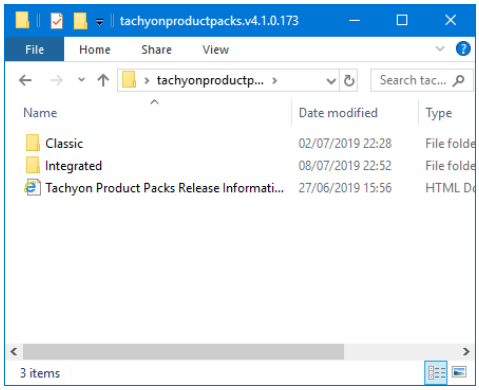
The **Integrated** directory holds a number of Integrated Product Packs that contain definitions for some Guaranteed State Policies, associated Fragments and Instructions. In addition a core utilities pack has been provided with common Fragments that you can use to build your own Policies.

4.3.1.2 Running the Tachyon Product Pack Deployment Tool

Here are the steps for running the tool:

Navigate to the directory where the **tachyonproductpacks.<version>.zip** file has been unzipped.

You will see two directories: **Classic** and **Integrated**.



Navigate to the **Integrated** directory**.**

In this directory you can see the Integrated Product Pack zip files along with the PPDT files:

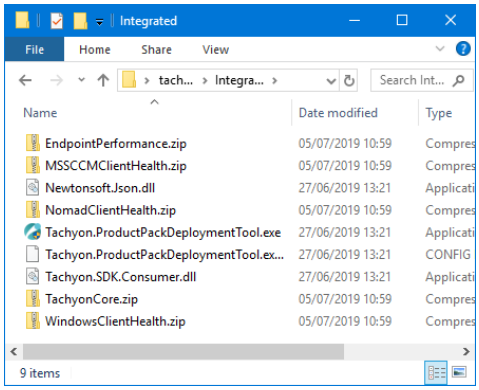
Newtonsoft.Json.dll

Tachyon.ProductPackDeploymentTool.exe

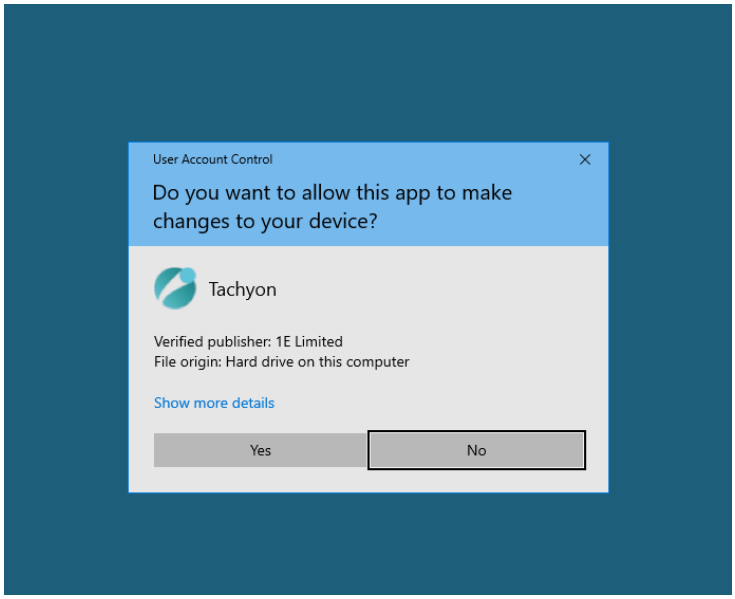
Tachyon.ProductPackDeploymentTool.exe.config

Tachyon.SDK.Consumer.dll

Double-click on **Tachyon.ProductPackDeploymentTool.exe**.



Click on **Yes** if any UAC dialog is displayed.



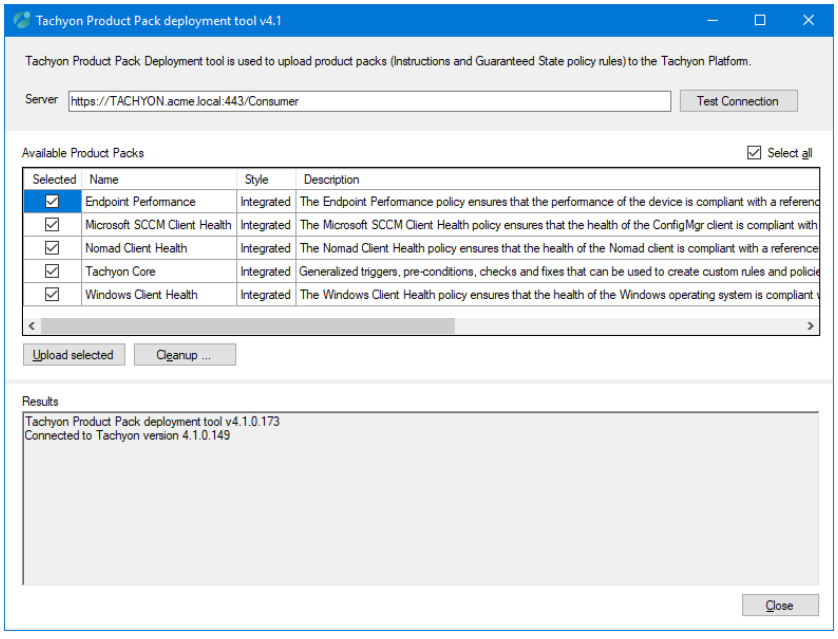
The **Tachyon Product Pack deployment tool** dialog will appear.

You must specify the URL of the Tachyon Consumer API in the **Server** field and then click on **Test Connection** to verify that you have entered the correct value.

Alternatively, you can specify the parameter *-url "<ConsumerAPI>"* on the command-line, for example: *-url "https://tachyon.acme.local/Consumer"*. If you run the tool on the Tachyon Server, the tool will automatically prefill the URL.

The **Style** column of the **Available Product Packs** table indicates whether each **Product Pack** is **Classic** or **Integrated**. The **Available Product Packs** table will be populated with all the zip files encountered in the directory the tool was launched from and all its sub-directories.

The **Select all** box can be used to select or deselect all the items in the **Available Product Packs** table.



4.3.1.2.1 Uploading Product Packs

When you have selected and checked the Tachyon Consumer API location you will then be able to upload the selected **Available Product Packs** by clicking on the **Upload selected** button. The content of the selected packs will then be uploaded to the Tachyon Server. The **Results** field displays the progress of the operation.

> **Warning**
>
> Updating Policies, Rules, Fragments, and Triggers that already exist in the Tachyon database is supported, but you need to be careful to ensure that the new artifacts uploaded are compatible with the existing ones. In particular, any new fragments and trigger templates uploaded need to have the same parameters that are used by the version of the same artifact that already exists in the database. Otherwise, any rules that are passing the previous set of parameters to the fragments will be broken when the new fragments start requiring a different set of parameters to be passed to them.

4.3.1.2.2 Cleanup option

The **Cleanup...** button on the main screen displays a **Cleanup** dialog that lets you remove items from the Tachyon server.

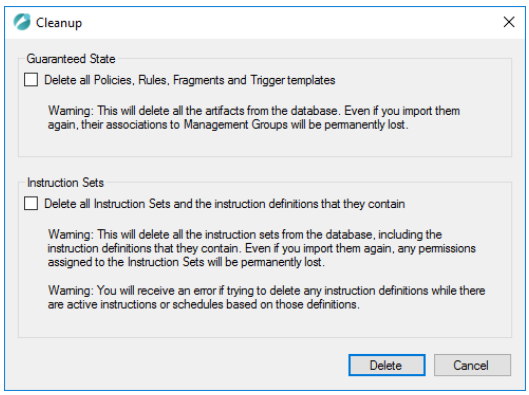
You would not normally perform a cleanup on a production server. This option is intended mainly for use in lab environments where you want to delete and re-upload the content in order to test different Product Packs.

There are two types of data that can be deleted using the Cleanup dialog and you will need to check the boxes for each type you want to delete:

Type of data	Description
Guaranteed State	Selecting this will delete **all** Policies, Rules, Fragments and Trigger templates from Tachyon and any previous associations those items had with any Management Groups will be permanently lost.
Instruction Sets	Selecting this will delete **all** the Instruction Sets and any Instruction definitions they contain. When you do this all the Instruction Sets and Instruction definitions currently loaded into Tachyon will be deleted and any permissions associated with them will be permanently lost. Errors will be generated if you try to delete any Instruction definitions that have active Instructions or schedules based on those definitions.

> **Warning**
>
> You need to read the warnings displayed on the dialog and be completely sure about wanting to delete the content before clicking on the **Delete** button. The program will display an additional confirmation dialog before proceeding to delete the selected content.

The deployment tool then calls the Consumer API and tells it to delete the selected items. If the Consumer API then decides that it cannot delete something because its current status doesn't allow it, then it returns an error to the deployment tool. The deployment tool displays the message. The tool doesn't care about whether a policy is enabled, or deployed or whatever. All validations are delegated to the Platform.



4.3.1.3 Log files

The log file is called **Tachyon.ProductPackDeploymentTool.log**. It is created in the same folder where the tool executable is located.

The logging level can be changed by adding the parameter **-log <level>** on the command line, for example, **-log DEBUG**. Supported values available:

TRACE

DEBUG

INFO (default)

WARN

ERROR

4.3.2 Verifying

The Verifying steps for Explorer can be found on the Verifying page.

4.4 Using Tachyon Explorer

How to use the Explorer application to investigate, remediate issues and manage operations across all your endpoints in real-time.

Note

Explorer can be reached directly using the following URL:

`https://<tachyon DNS Name FQDN>/Tachyon/App/#/explorer/`

where <tachyon DNS Name FQDN> is the one set up during the preparation phase, as described under the heading DNS Names.

4.4.1 Introducing Explorer

An overview of Explorer is presented; what it does and how it can benefit your organization. An introduction to the features is provided.

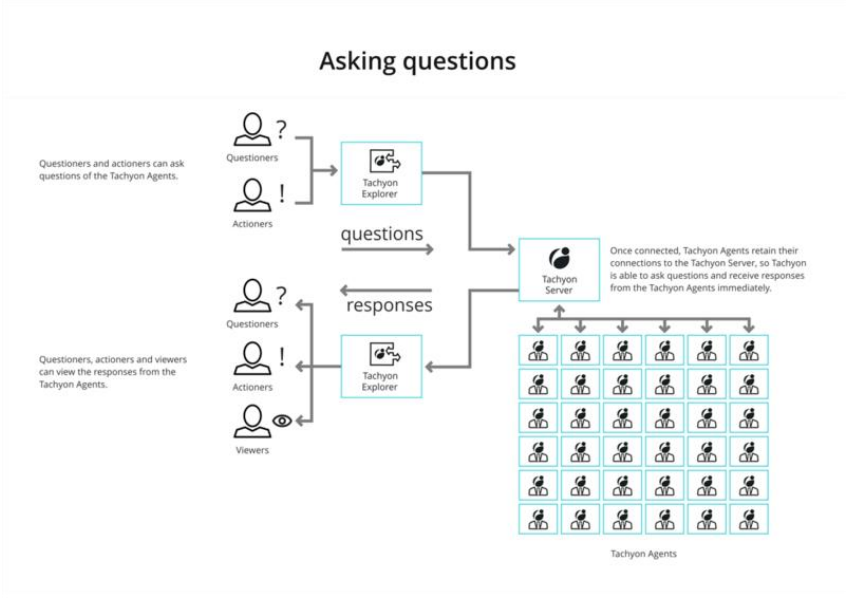
4.4.1.1 Introduction

Explorer is the front-end to the real-time aspects of Tachyon. It lets you interactively ask questions, run actions and view responses. You can also use it to view the connected client devices.

4.4.1.1.1 Asking questions

Using the Explorer, questions can be asked of the Tachyon client devices by users with the questioner or actioner roles . The responses can be viewed by viewers, questioners and actioners.

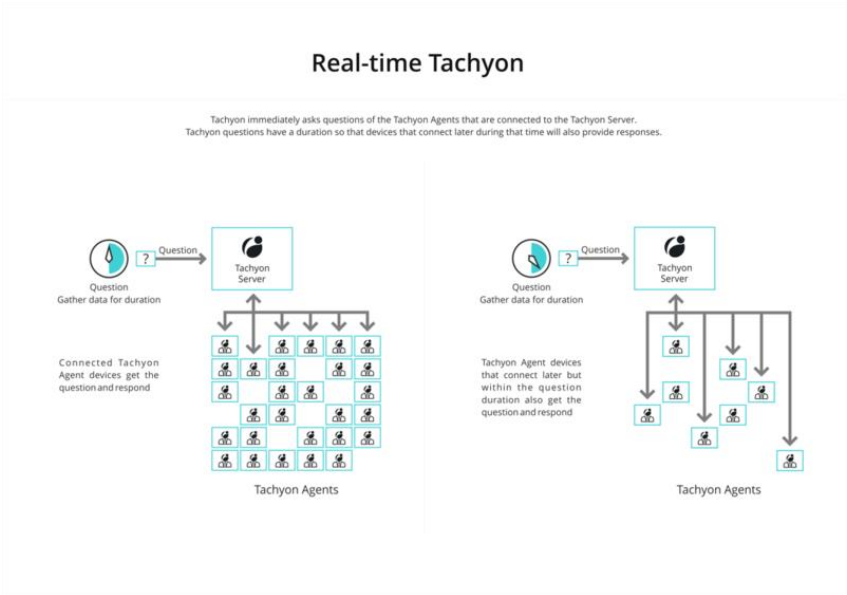
Details on asking questions can be found in ExplorerHome page, questions and responses.



4.4.1.1.2 Real-time Tachyon

Tachyon works in real-time, so not all of the devices may be connected at the time a question is asked. Questions have a configurable duration that they will gather data for - allowing devices that connect later, within the **gather data for** duration, to respond.

Questions also have a configurable **keep answers for** duration - given that the answers from a live network can potentially get stale quickly and questions are fast enough that you can simply ask the question again rather than relying on old answers.



4.4.1.1.3 Coverage and filters

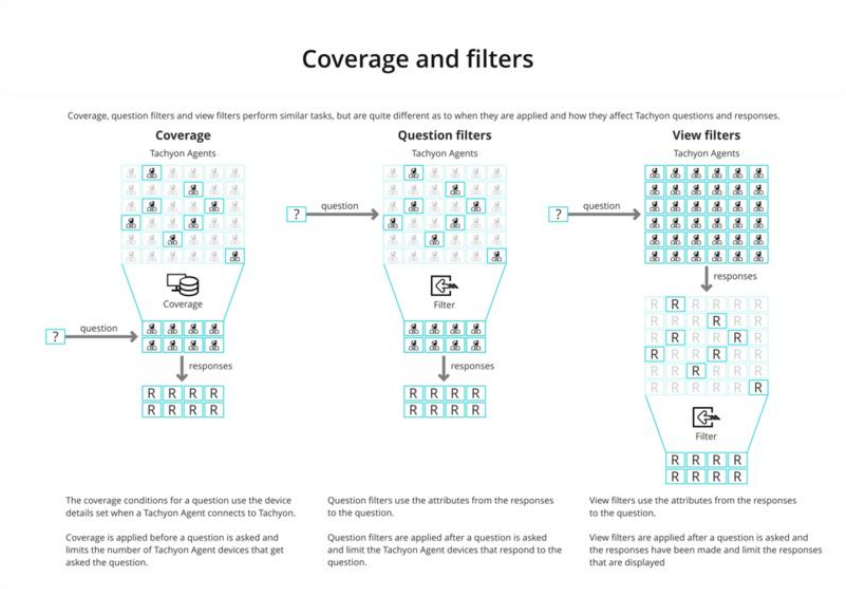
You can use coverage and filters to reduce the amount of network traffic caused by asking a question. They are also useful in reducing the amount of data that is presented to the Tachyon users. Tachyon provides coverage, question filters and view filters.

Coverage is applied before a question is asked and reduces how many Tachyon client devices get asked the question. Coverage uses the device properties that are sent by a Tachyon client when it connects to Tachyon.

Question filters are applied at the Tachyon client after the question has been asked and use the attributes from the question responses to determine whether the client should send the response.

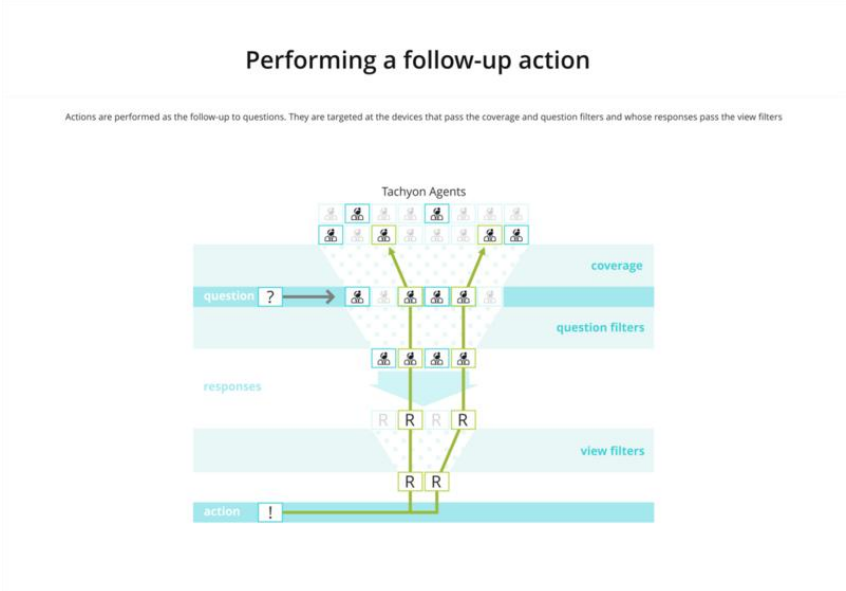
View filters are applied in the Explorer after the responses have been sent and reduce the responses that are displayed.

For more information see Coverage, question filters and view filters.



4.4.1.1.4 Performing actions

Normally, before an action is performed a question is asked. This identifies the set of devices the action will be performed on, after the coverage, question and view filters have been applied.



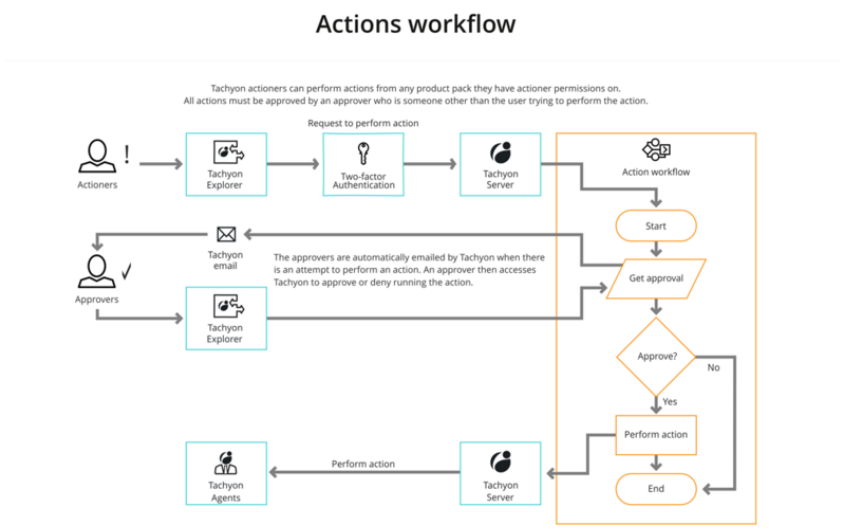
Using the Explorer, actions can be performed on the client devices by users with the actioner role on a product pack subject to the following:

they will need to enter their password

if the action has been configured to use two-factor authentication, they will need to enter the authentication code

they will need the approval of someone other than themselves with an approver role.

Details on performing actions and the approval workflow can be found in The action approval workflow.



4.4.2 Explorer Features

An overview of Explorer application features.

The Explorer application gives you the ability to investigate, remediate issues and manage operations across all your endpoints in real-time. For more information, please refer to Using Tachyon Explorer.

Here's an overview of the features available in the Explorer application.

4.4.2.1 Explorer features

4.4.2.1.1 Questions, actions and their responses

Explorer lets you directly question connected devices to retrieve responses, run actions, and get real-time information from them. The Explorer front-end capabilities ensure fast querying, investigation, and remediation.

The questions, responses and actions feature includes:

Graphical display of response information

Instruction impact assessment

Response history.

> **Note**
>
> For more information on Instructions and their responses, please refer to:

ExplorerHome page, questions and responses

Question parameters

Instructions

History.

4.4.2.1.2 Exporting data from Explorer

Results visible in Explorer can be exported to files containing comma-separated values (CSV) or, in the case of the **Export all** option on the instruction response page, tab-separated values (TSV), and results can be marked for export at the point of asking a question to automate the process. Explorer lets you export the data on a number of pages to CSV files:

Instruction history

Responses - you can export a single page or all results once the Instruction has finished gathering responses - these can then be used for auditing purposes or to drive external programs

Drill-down responses

Device information

> **Note**
>
> For more information on exporting data from Explorer, please refer to:

Exporting data from Explorer.

4.4.2.1.3 Coverage, question filters, view filters and follow-on instructions

Questions and responses can be tailored to focus on specific ranges of devices through the use of coverage and filters:

Coverage acts first to let you restrict the devices that will be asked a given question

Question filters act before devices have responded to narrow the responses that are sent

View filters act after the responses have been sent to focus the responses presented to the user and to determine the input into the follow-on instructions

The responses to initial questions can be further refined by asking follow-on questions or actions, allowing questioners and actioners to focus in on the results they want to see.

> **Note**
>
> For more information on coverage, question filters, view filters and follow-on instructions, please refer to:

Coverage, question filters and view filters

Limiting coverage using a Management group - tutorial

Refining responses with follow-up questions.

4.4.2.1.4 Approval workflow

To enhance the safety of running actions in the Tachyon system, there is an approval workflow that ensures that every action requires the approval of designated approvers before it can be run. To make it even safer, someone with approval permissions cannot approve their own action.

When an attempt is made to run an action, the approval workflow sends an email and a Tachyon notification to all the approvers associated with the action. Any of the approvers may approve or reject the request to run the action.

Note

For more information on the Approval workflow, please refer to:

The action approval workflow

Performing an action - tutorial.

4.4.2.1.5 Authentication

Users must provide their user credentials when attempting to run an action, this prevents unauthorized access by a third party attempting to make use of an unattended computer.

Actions can also be configured to require two-factor authentication, where the user attempting to run an action is challenged to enter a unique, one-time authorization code that has been sent to them via an alternative method - such as email or via a registered mobile.

Note

For more information on authentication, please refer to:

Two-factor authentication.

4.4.2.1.6 Task-based organization for accessing and scheduling instructions

Tachyon provides a way of accessing the questions and actions that is organized around the way that network administrators typically interact with their network. This interface also lets you run the Instruction using a schedule.

The **Explorer→Instructions→Tasks** page in Explorer provides a structured view of the instructions defined in the Product Pack. It also lets you schedule the tasks so they can be run in the future or according to a particular schedule.

4.4.2.1.7 Using task groups

The benefit of using **Tasks** lies in the task group structure that is defined in the product packs. It is this structure that enables you to focus in on specific task areas to find the particular instruction that you want.

For example you may be interested in instructions related to particular software vendor's products. Depending on the Instructions that you have uploaded to your Tachyon system you may see the following structure:

At the top-level there is a **Software Vendors** task group whose children are **1E** and **Microsoft**.

Underneath the **1E** task group there is a **Tachyon** group that contains **Configuration**, **Diagnostics** and **Verification** groups as well as a couple of Instructions.

Underneath the **Microsoft** task group is the **Configuration Manager** task group containing Instructions related to that product.

Note

For more information on using Task groups to access and schedule Instructions, please refer to:

Tasks

Scheduling instructions

Scheduling instructions - a tutorial.

4.4.2.1.8 Inventory and connectivity

The **Devices** page in the Explorer shows you all the devices that have connected with Tachyon and their current connection status. There are two views provided that let you research the devices: the devices table and the devices dashboard, please refer to The Devices Table and The Devices Dashboard for more details.

Note

For more information on inventory and connectivity, please refer to:

The Devices Table

Using the Devices dashboard - Tutorial.

4.4.3 ExplorerHome page, questions and responses

How to frame questions in Explorer and view the responses.

4.4.3.1 Asking a question

Explorer is where you frame the questions that let you immediately explore the information available on connected devices.

Note

Explorer can be reached directly using the following URL:

`https://<tachyon DNS Name FQDN>/Tachyon/App/#/explorer/`

where <tachyon DNS Name FQDN> is the one set up during the preparation phase, as described in DNS Names.

The animation shows the **TCNQuestioner01** user entering the URL used in our examples, **https://tachyon.acme.local/Tachyon/App/#/Explorer**

The animation shows the Explorer prompting for credentials only because the browser's security settings have been configured to prompt for username and password, which can be useful when testing.

4.4.3.1.1 Choosing your instruction

Clicking on the **All Instructions** button lets you browse through all the currently installed questions.

You can select to browse through the instructions using groups with the following options:

Group by	Description
Instruction set	This option groups instructions by the instruction set they belong to. You can click on an instruction set to expand and collapse a list of its instructions. An instruction can only belong to one instruction set.
None	This option lists all of the instructions without sets.

You can see the instruction type (question or action), name and description

The animation shows the following steps:

The user selects the **All Instructions** dialog for a Tachyon system which has had Product Packs already added.

In the **All instructions** popup the user then takes a quick look through the available **Instruction sets** as selected in the **Group by** options.

You can expand each of the Instruction sets and select the instruction that you want to run. In our example the user expands the **1E TachyonCore** set and then selects the **How many of each operating system versions are installed?** question.

Selecting the question loads it into Explorer You can see the text for the question loaded into the question box with its operational parameters laid out underneath.

The following table briefly describes the available parameters:

Parameter	Description
Duration	Determines how long the data will be gathered for and how long to keep the answers for. Instructions have defaults for the number of minutes to **gather data for** and **keep answers for**. You can override either of these defaults.
Approximate Target	An estimation of how many devices will receive the question.
Projected Impact	An estimation of how much impact the question will have on the target devices. The estimate depends on previous occasions the instruction has run.
Options	Lists any additional options that have been set for the question.

To ask a question you just click the **Ask this question** button below the parameters. When a question is asked, the view automatically switches to its **Responses** page and provides immediate feedback on how the question

responses are coming in. The **Responses from** value at the top-right of the page displays the number of devices that have responded. In our example all 12 devices respond.

The selected Instruction displays a response visualization chart and returns a list of responses. You can switch to the list by clicking the **List view** icon.

4.4.3.2 Interacting with a response visualization

Some questions provided in Product Packs are defined so that their responses can be viewed as graphs.

In our example we want to know which processes have made the most connections to the Domain Controller for our example environment in the past 10 days. The question we will ask is:
Which processes have made connection to <ipAddresss> in the last <numDays> days?. This question will return the information so that it can be reviewed as a graph. It also makes use of Tachyon Activity Record, where potentially useful information about network and device performance is gathered and held by the Tachyon client.

The animation opposite shows the following steps of the example:

On the Explorer home page the **TCNQuestioner01** user types the text **which processes** into the text box and then selects the **Which processes have made connection to <ipAddress> in the last <numDays> days?** question from the matching list.

They then set **<ipAddress>** to **100.100.100.100** (the IP address for the ACME Domain Controller) and **<numDays>** to **10**.

Once the parameters are set they then click on the **Ask this question** button and the clients respond with the list of **Process Names** that have connected to that IP address.

You can interact with the charts, toggling the display for each individual process between on and off, by clicking on the name of the process displayed beneath the chart. In our example **TCNQuestioner01** toggles the display of each process with the highest number of connections off to reveal the processes with less connections.

You can also investigate the individual data nodes of the graphs by hovering the mouse over the points. Here the user looks at each node in turn for **ccmexec.exe**.

4.4.3.3 Checking the status of responses using the summary tab

In the animation opposite we show how the **Summary** tab on the **Responses** page can be used to check the status for the responses to a question.

To check the Response page **Summary** tab we will run a Configuration Manager client health check question.

From the Tasks view navigate to **Software Vendors→Microsoft→Configuration Manager**

Select the
What is the health of my SCCM clients? Check that inventory has run and that policy has been evaluated in the last <numdays> days. question.

Set **<numdays>** to **7** and click the **Ask this Question** button.

When the responses start coming in for the question, select the **Summary** tab to see how they are progressing.

On this page you will see some statistics related to the question responses and some charts that display the information graphically.

The **Sent Count** chart shows the total number of questions that have been sent and the balance between the responses that have been received and the awaiting responses. As each response comes in the percentage of **Responses** goes up and the **Awaiting** goes down. This is also seen in the actual values for the **Responses count** and **Awaiting responses count**.

The **Responses Status** chart shows the status for each response as it comes in. For each response the status may be one of the following:

Reponses	Description
Success	Devices that have responded with a success status
Success - no content	Devices that have responded with a success status but did not provide a response to the instruction content request
Error	Devices that have responded with an error encountered when attempting to run the instruction
Not implemented	Devices that have responded where the feature contained in the instruction is not implemented on the device
Response too large	Devices that have not been able to respond to the instruction content request because their response was too large

In our example, eventually the **Responses** count in the **Percent Sent Count** chart rises to 100% indicating that all the responses have been received now (for the devices currently connected).

We can now check on the **Status** tab to investigate the reasons for the response statuses we've seen.

Expanding the **Not implemented** row, we can see that our Linux device cannot run this instruction because it uses a PowerShell script that is not supported on this platform.

Expanding the **Error** row, we can see that one of our Windows 7 devices generated a PowerShell error.

4.4.3.4 Question parameters

How to configure Question Parameters.

4.4.3.4.1 Duration

The section in the list of instruction parameters is **Duration**. When Explorer asks a question it does so immediately to all the connected devices, which can be seen in the **Approximate Target** parameter, in the picture there are 12 out of 12 devices connected so the question will get sent immediately to all of the devices.

In a large dynamic network having all the devices connected at one time is unlikely, due to the nature of laptops or mobile devices for example connectivity is liable to be a very fluid thing with devices connecting and disconnecting constantly.

For this reason questions are asked over a duration, this allows devices that connect inside of that duration to answer the question. The default time varies according to the instruction definition in the Product Pack but you can change this parameter to the time that you think will give the highest number of responses.

The other aspect of a dynamic network is that the information returned in the responses to a question may change afterwards at the source. For this reason the responses to a question are only kept for a configurable period of time. Like the **Gather data for** parameter, the default **Keep answers for** time varies according to the instruction definition in the Product Pack but you can change this parameter to a time appropriate to how volatile the information in the question response is.

Setting the duration for gathering data and keeping answers can be done by:

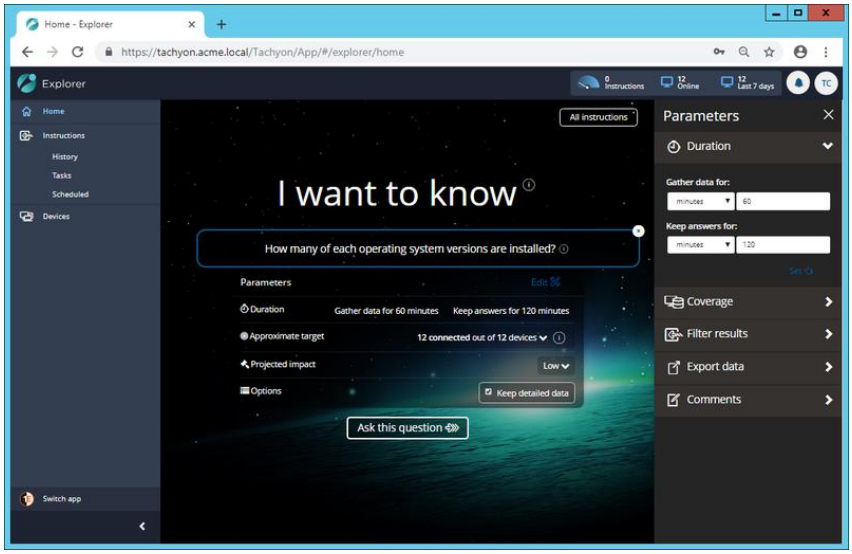
Editing the question **Parameters**

Expanding the **Duration** heading in the **Parameters** rollout

Selecting a value and unit (minutes or hours) for each of the **Gather data for:** and **Keep answers for:** fields.

Clicking the **Set** link at the bottom-right of the expanded **Duration** heading.

The picture shows a question **Duration** with the default values.



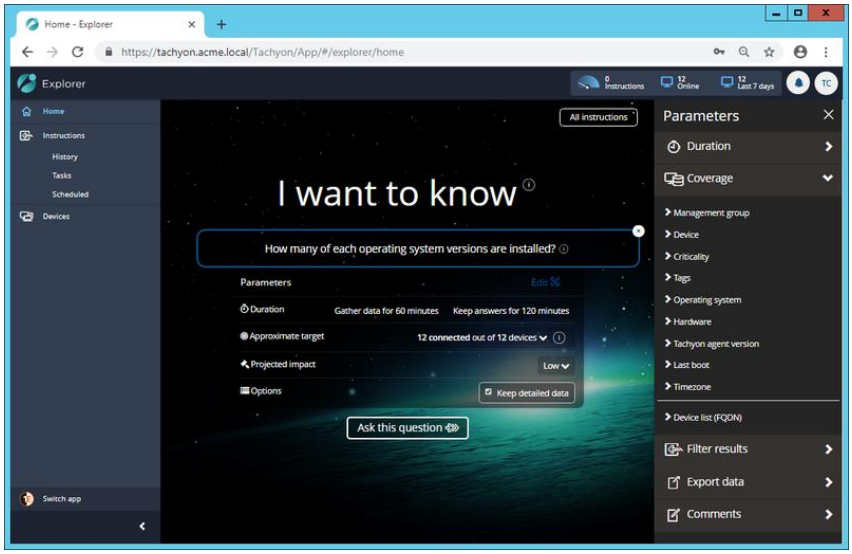
4.4.3.4.2 Coverage

The Coverage section lets you control which devices get sent the instruction you are defining. This helps to minimize network bandwidth usage as all the processing of which devices get targeted is all done within Tachyonbefore the instruction is sent. Coverage uses the data sent to Tachyon by devices when they register.

The picture shows the Coverage section for a question.

4.4.3.4.2.1 More information on Coverage

Coverage, question filters and view filters describes the similarities and differences between the three main types of filter that can be applied to an instruction, and a tutorial on Management groups and coverage can be found on Limiting coverage using a Management group - tutorial. Tables of information on the coverage parameters can be found in Coverage parameters.



4.4.3.4.3 Filter results

The **Filter results** section lets you define a question filter that determines which devices respond to an instruction. In this case the instruction is sent to the device and the filter is applied there to determine whether the device sends a response or not. Like Coverage this reduces unnecessary network bandwidth usage but unlike Coverage the data that can be used for the filter comes from the instruction and is not limited to the data sent to Explorer when devices connect.

The picture shows the **Filter results** parameter section expanded.

4.4.3.4.3.1 Selecting the attributes to filter

The **Filter results where:** field lets you build filter conditions from the attributes of the question, a comparison operator and a value. You can build multiple filter conditions, but each of them must be built and set before you can build the next.

The workflow steps for creating each condition are as follows:

Choose the attribute to filter

Choose the comparison operator

Set the value

Each step uses the **Filter results where:** field in a slightly different way. To choose the attribute you click in the field. A list of the attributes that are available to filter on from the selected question will be displayed. Each attribute has a type that changes the options that are available for the operator and value selectors, as shown in the following table.

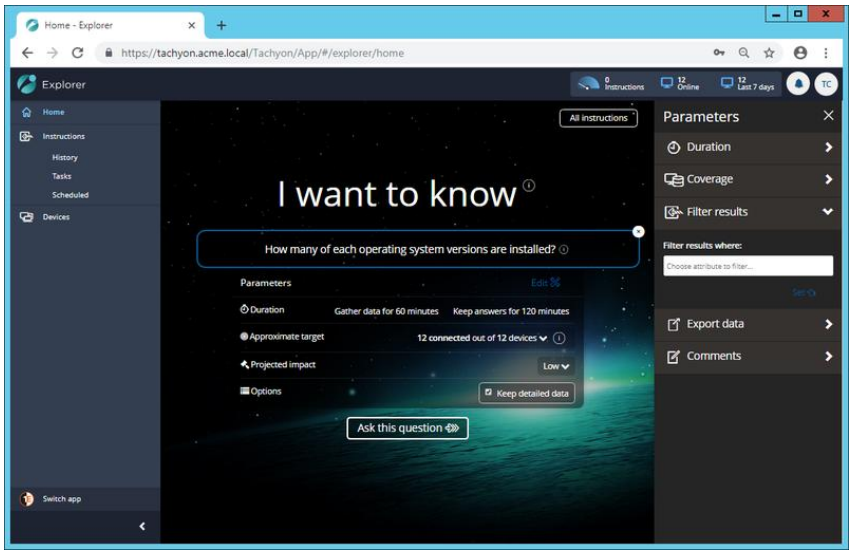
Attribute type	Operators	Value field
string	begins with	Edit field

Attribute type	Operators	Value field
	contains	
	is	
	ends with	
integer	>=	Edit field constrained to integer values
	=	
	<=	
datetime	before	date/time picker
	after	
bool	is	menu containing true/false

Once the operator has been set the value can be set. For string and integer type attributes there is an edit field. For boolean type attributes there is a menu that allows you to select true or false. For datetime type attributes there is a date picker that lets you select the date and time interactively.

4.4.3.4.3.2 More information on Filter results

Coverage, question filters and view filters describes the similarities and differences between the three main types of filter that can be applied to an instruction.



4.4.3.4.4 Export data

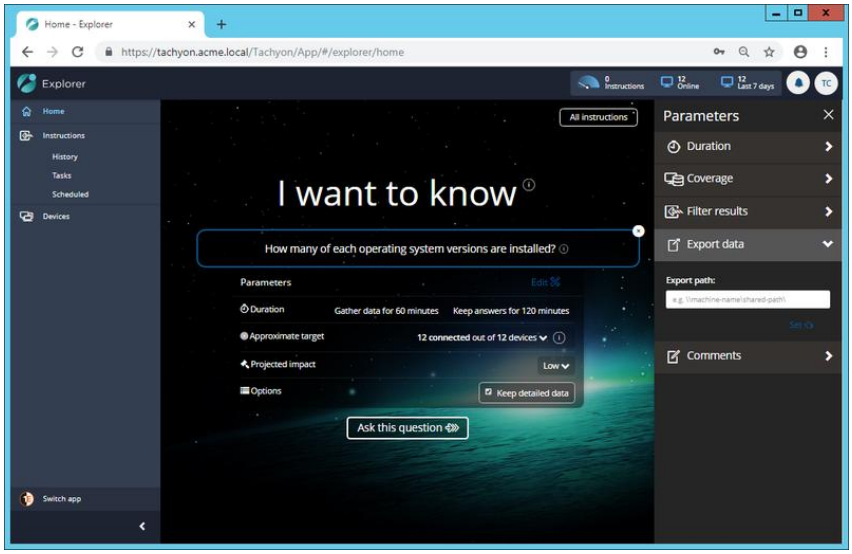
The Export data section lets you define from the outset that the responses to the instruction will be exported when all the results have been gathered.

The picture shows the Export data section expanded. There is a single edit field where you must supply the path to a Windows share with the appropriate permissions set, please refer to Configure Tachyon to support the Export all responses feature for more details.

4.4.3.4.4.1 More information on Export data

An example of running an instruction with **Export data** enabled can be found in Tasks.

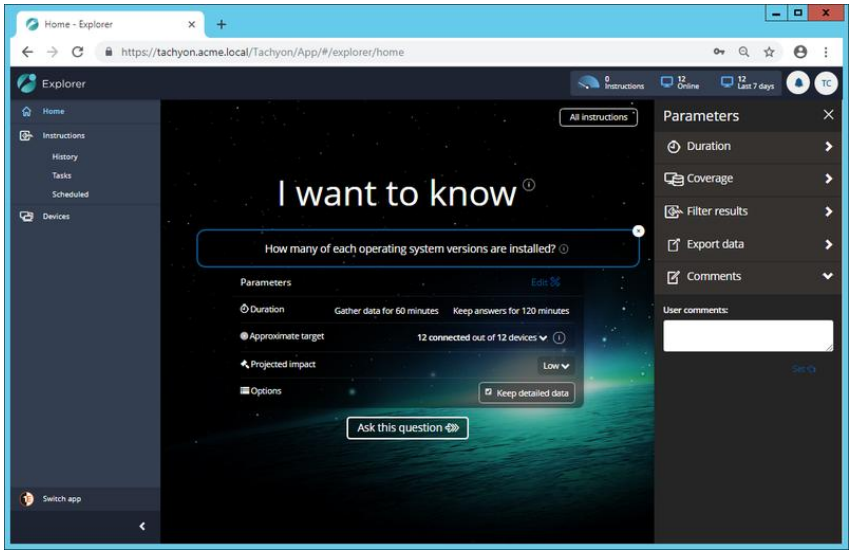
Exporting data from the outset is also similar to exporting all results from the responses page, as described in Exporting data from Explorer.



4.4.3.4.5 Comments

The **Comments** section lets you add a comment to the instruction that will appear in the emails sent to approvers.

The picture shows the **Comments** section expanded.



4.4.3.5 Coverage, question filters and view filters

How to define the coverage for a question, how to filter the responses to a question at source and how to filter them in the responses view.

4.4.3.5.1 Coverage and filters

In ExplorerHome page, questions and responses we've seen an example of asking a question and returning some responses. The question was asked of all 6 devices and the responses from all 6 devices could be seen. However, our example environment is not representative of a real network where there may be many thousands of devices and a corresponding number of responses. In the real world it would be expected that questioners would want to perform some limiting of the number of devices questioned, the number of responses returned and the number of responses displayed.

Explorer provides options for each of these:

Coverage - limits the number of devices that are questioned

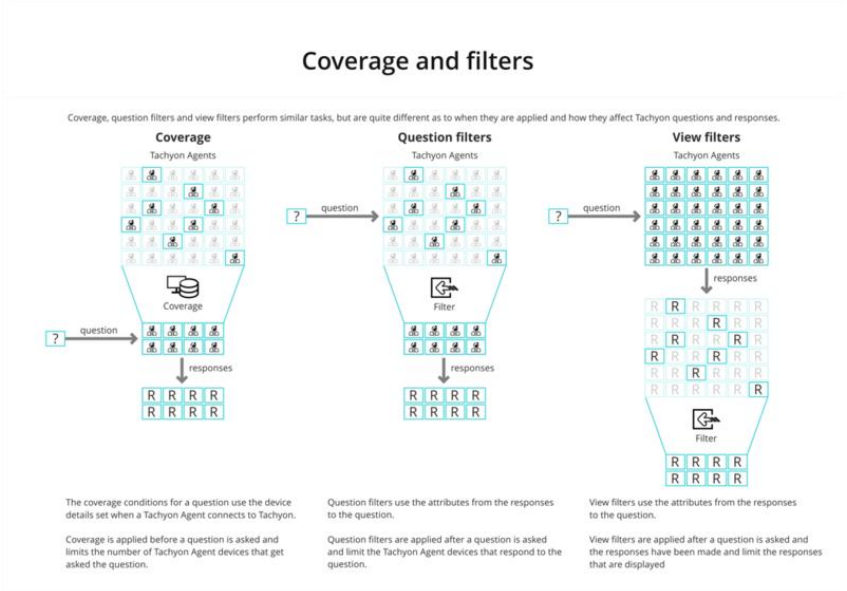
Question filters - limits the responses at the client

View filters - limits the number of responses shown in a view

All of these limit the amount of data that is displayed to the user, but it's worth while making a quick comparison of the similarities and the differences to help determine when it is best to use each.

The picture shows the basic similarities and differences between the three options. We'll look at each option in more detail in the following headings.

In the following examples **TCNQuestioner01** is logged in to Explorer, they have access to the **How many of each operating system version are installed?** question that we will use to illustrate the similarities and differences between Coverage, Question filters and View filters.



4.4.3.5.2 Coverage

Let's take a look at coverage first. To demonstrate the difference between filters and coverage we will set the coverage of the question to only target devices that have Windows 10 or later installed.

In the example we're logged on as **TCNQuestioner01**, here are the instructions for it:

After typing the text **How m** in the edit field, select the
How many of each operating system version are installed? question from the list of matching questions.

Note that the **Approximate target** field shows that there are **12 connected out of 12 devices**. This is because in our example environment there are only 12 client devices in total and all of them are connected. In a real network you are liable to have intermittently connecting devices and the connected number shown will vary accordingly.

After the question is loaded click on the **Edit** link in the parameters section beneath the question text. Doing this expands the **Parameters** rollout.

On the **Parameters** rollout click the **Coverage** heading to see the coverage parameters.

Click the **Operating system** heading to expand the controls for setting a coverage using the operating system details

The **Type** parameter lets you select the device's operating system from a list of supported OS. Select **Windows**.

The **Version** parameter lets you define a numeric comparison for the number you type in the edit field. Select the **>=** operator and then type **10** in the edit field. This will check for all Operating Systems of version 10 or later.

Click the **Set** link in the bottom-left of the expanded **Operating system** heading, which adds the **OsVer >= 10** and **OSType = Windows** coverage parameters to the question details.

Now click the **Ask this question** button. The question will only be asked of the devices whose device parameters match the coverage just set.

The **Responses** page for the question displays the selected **Coverage** parameters in the question header.

Once all the responses have been received you can see in the video that there are two rows where the **Os Version Text** is **Windows 10 Enterprise** and **Windows 10 Pro** respectively and the **Count** totals **2**.

4.4.3.5.2.1 Real-time coverage

Explorer does not just work on the basis of the client devices that are currently, or have previously, connected to Tachyon. It is also open to existing information changing and to new, previously unconnected, client devices that come online while a question is active. This means that the coverage information in the question header, where it shows the percentage of answers received out of the total number of devices included in the coverage, could change as client devices change their device properties registered with Tachyon or new client devices come on line.

In our coverage example the responses could change if a client device finishes a migration to a Windows 10 operating system or a new client device with the Windows 10 operating system connects while the question is still active. In this case the number of devices in the coverage would change but the percentage could stay at 100% if all of the new devices covered have also sent responses.

4.4.3.5.3 Question filters

The second option is to apply a filter at the point the question is being framed. This does not affect which clients get asked the question. The question filter, which is constructed from the attributes of the question response, controls which of the clients actually send their responses.

Question filters are set by editing the question parameters, once a question has been selected, you expand the **Filter results** heading in the **Parameters** rollout.

In the example we're logged on as **TCNQuestioner01**, here are the instructions for it:

After typing the text **How m** in the edit field, select the
How many of each operating system version are installed? question from the list of matching questions.

After the question is loaded, click on the **Edit** link in the parameters section beneath the question text. Doing this expands the **Parameters** rollout.

On the Parameters rollout, click the **Coverage** heading to see the coverage parameters.

Click on the **Filter results** heading to expand that section.

Clicking on the **Filter results where:** field displays the question attribute list, that is the list of attributes that are defined as part of the question.

Select **OsType** from the list and it gets added to the field and a second list is displayed containing the operators that are relevant to the attribute type, in this case a string.

Select the **contains** operator and that gets added to the field. Now the rest of the field becomes an edit field.

Type in **Windows** to complete the filter and then click the **Set** link in the bottom-right of the expanded **Filter results** heading to add the filter to the **Filter results** for the question.

Now start the process of building the second part of the filter. This time, click in the field and select **OSVersionText**.

Select the **contains** operator.

Type **10** into the edit field and finally click the **Set** link to add the second filter to the **Filter results** for the question.

Once the filters have been added, click on **Ask this question**.

The **Responses** page for the question displays the selected **Filter results** parameters in the question header.

The responses come back from the devices and the results look similar to the coverage example.

4.4.3.5.4 View filters

The last option is to apply a filter at the point of viewing the responses to the question. This does not affect which client devices get asked the question, nor does it affect which client devices return responses.

View filters are set on the **Responses** page for the individual instruction, once a question has been selected and asked, you then expand the **Filter results** panel just above the responses table.

In the example we're logged on as **TCNQuestioner01**, here are the instructions to follow it:

After typing the text **How m** in the edit field, select the
How many of each operating system version are installed? question from the list of matching questions.

This time go straight to clicking on **Ask this question**.

In moments, the **Responses** page for the question shows that all the devices have responded.

Click on the **Filter results** button to expand the filter results panel.

Type **Windows** into the **OS Type** field and **10** into the **OS Version Text** field then click the **Search** button.

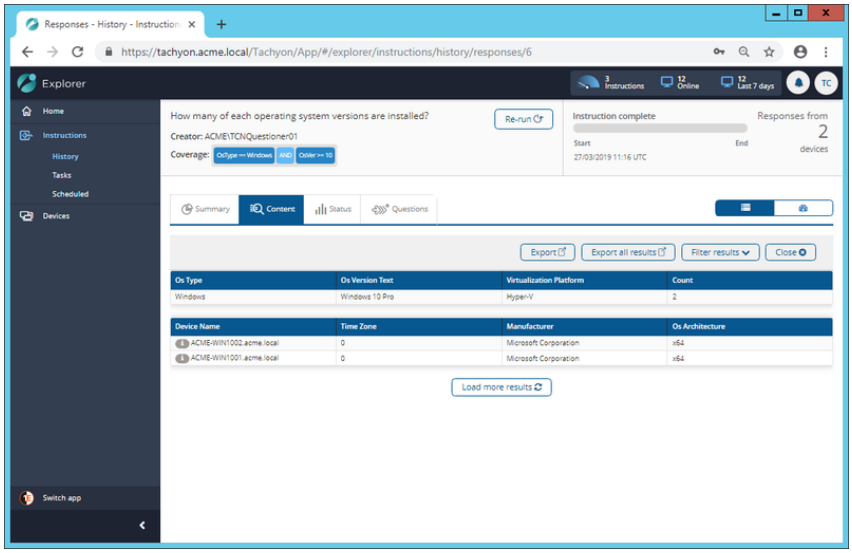
Now the responses from all the connected devices are filtered to just the Windows 10 devices.

4.4.3.5.5 Comparing coverage, question filters and view filters

Here we compare the three sets of responses to the same question, but set with different coverage, question filters and view filters.

4.4.3.5.5.1 Coverage

Here are the results of running a question with coverage set.



The following points summarize coverage:

Lets you constrain a question so that it only gets asked of particular client devices

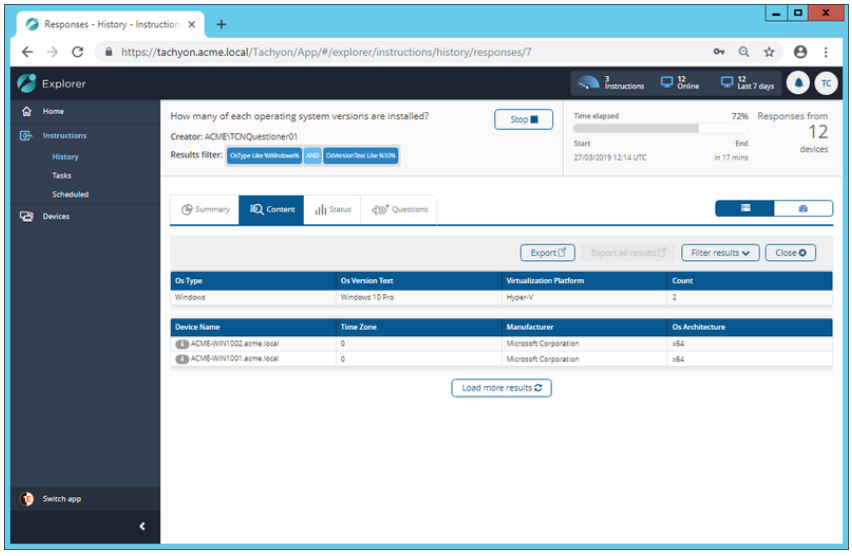
Uses the device details registered with Tachyon by each client device

Is applied at the Tachyon Server before the question is asked

Remains active for the duration of the question, so client devices that change their device details registered with Tachyon may subsequently be included in the question's coverage - that may include new client devices that haven't previously connected.

4.4.3.5.5.2 Question filter

Here are the results of running a question with a question filter set.



The following points summarize a question filter:

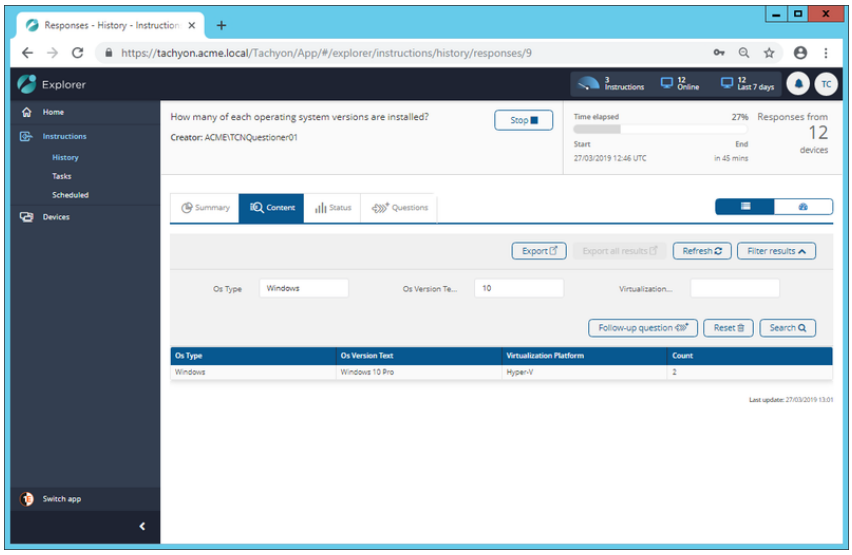
Lets you constrain a question so that responses are only made by particular client devices

Uses the question attributes. The question is run on the client and if the response satisfies the question filter it is sent to Explorer

Is applied at the client after the question is asked but before the response is sent.

4.4.3.5.5.3 View filter

Here are the results of running a question with a view filter set.



The following points summarize a view filter:

Lets you constrain the responses for a question so that only the ones that pass the filter are displayed

Uses the data in the columns for the responses to a particular question

Is applied in the Explorer in the **Responses** view after the responses have been sent to Tachyon Server and are being viewed.

4.4.3.5.6 Limiting coverage using a Management group - tutorial

How to use Management groups to set the coverage for a question to target a specific set of devices.

In this tutorial

In this tutorial, we set the coverage for a question using a Management group. The examples assume that the Management groups have already been configured by a userwho has the group administrator role, please refer to Management Groups - tutorial for more details.

As an example, we will show how to specifically target the devices in the **Executive** Management group. In our example this Management group, defined according to the OU the devices belong to, contains two devices used by members of the executive team:

ACME-WIN1001.acme.local

ACME-WIN1002.acme.local

In this tutorial, we will demonstrate:

Opening the Parameters Coverage Management group panel

Searching for the Management group and setting the coverage

Asking the question, viewing the results and drilling down to see the devices.

4.4.3.5.6.1 Setting Management group coverage

This tutorial starts at the point the **TCNQuestioner01** user has already selected the question: **How many of each operating system versions are installed?**

To set the coverage for the question they need to open the **Parameters** rollout to locate the **Coverage** section and open the **Management group** panel.

4.4.3.5.6.1.1 Opening the Parameters Coverage Management group panel

To do this:

Click the **Edit** link displayed below the question field in the **Parameters** section. Doing this opens the **Parameters** rollout on the right-hand side of the screen.

Click on the **Coverage** heading in the rollout to expand that section and display all the alternative types of coverage that can be set.

Click on the **Management group** heading to expand that panel and reveal a search combobox.

4.4.3.5.6.1.2 Searching for the Management group and setting the coverage

When the Management group field is open:

Click in the edit field, a drop-down list with all the currently defined Management groups is displayed.

Type the first few letters of the Management group you want to use. In our example **TCNQuestioner01** types **Ex** to find the **Executive** Management group.

Click on the Management group in the list of matches displayed.

When the Management group has been selected click **Set** to add it to the question parameters.

> **Note**
>
> You can only set one Management group for a given question. If you try to set another it will replace the one already set.

In our example you can see in the question parameters that the coverage has been set to the **Executive** Management group and the **Approximate target** has changed from **12** to **2**. Hovering over the information icon by the **Approximate target** field displays a notification that the target has been reduced.

4.4.3.5.6.1.3 Asking the question, viewing the results and drilling down to see the devices

We're now ready to ask the question.

Click the **Ask this question** button.

Having set the coverage, the question will only be asked of the devices contained in the selected Management group.

In our example, when the responses come back a single bar is displayed indicating that the 2 devices both have the **Windows 10 Pro** operating system installed.

When **TCNQuestioner01** clicks on the **Responses list** icon, it displays a single entry for the **Windows 10 Pro** operating system.

Clicking on that entry expands the devices that have that operating system installed.

Here the two target devices in the Executive Management group can be seen:

ACME-WIN1001.acme.local

ACME-WIN1002.acme.local

In this tutorial we've shown how to:

Open the Parameters Coverage Management group panel

Search for a Management group and apply the coverage to the question

Ask the question, view the results and verify the devices the question was targeted at.

4.4.3.6 Refining responses with follow-up questions

How to refine responses by asking follow-up questions.

4.4.3.6.1 Follow-up questions

Explorer lets you build on top of initial questions by asking follow-up questions. Those questions may themselves have follow-up questions and so on. The purpose of the follow-up questions is either to constrain the responses further, acting as a kind of super filter, or to get additional information from the devices in the initial responses.

4.4.3.6.2 The example

To illustrate the use of follow-up questions we will use a scenarios where an administrator wants to find out which users are currently logged on to just the Windows devices that have previously been tagged with an **ACMEDEPLOY Phase 3** value coverage tag.

A user with permissions to ask questions, in our example **TCNActioner01**, is logged on to Explorer.

The example contains the following steps:

On the Explorer home page, type in **coverage** to find and then select the **What are the coverage tags?** question.

Click the **Ask this question** button.

Responses are sent back from the client devices showing the coverage tags applied to each of the devices

Filter the responses to show just those with the **Phase 3** value set. This is done by clicking on the **Filter results** button, which expands the **Filter results** panel.

Enter the text **Phase 3** into the **Values** edit field and then click **Search** to apply the filter. The responses change to display just the **Phase 3** tagged devices.

Now click the **Follow-up question** button to ask a question of just these devices. Doing this displays the **Questions** tab with the original question and filter displayed above the usual question edit field.

Type **How many** to find and then select the **How many of each operating system version are installed?** question.

Click **Ask this question**, at the bottom of the page

Responses to the new question are sent back from the client devices that pass the original question and filter. In this case it provides responses from just the **Phase 3** tagged devices

From these follow-up responses the **Os Type** of the devices can be used to filter and just display the **Windows** devices. To do this Expand the **Filter results** panel, type **Windows** in the **Os Type** field and then click the **Search** button. Notice how the **Linux** device has been filtered out.

Click the **Follow-up question** button to create a second follow-up question. Again the follow-up **Questions** tab is displayed, this time with the follow-up question and filter displayed.

Type the word **logged** into the edit field to find and then select the **Who is currently logged in?** question.

Click the **Ask this question** button.

Now the responses to the second follow-up question display the logged on users for just the Windows devices that have been tagged with the **Phase 3** value for the **ACMEDEPLOY** coverage tag. Job done.

If the user wants to monitor how they got to this point they can look at the **Trail**, over on the left of the responses table

Going from top to bottom they can see they asked **What are the coverage tags?**, then **How many of each operating system version are installed?** and finally **Who is currently logged in?**

4.4.4 Instructions

Viewing the instruction history, navigating instructions using the tasks page and scheduling instructions. This page describes how the Instructions section of the Explorer interface works and how it relates to the running of instructions.

4.4.4.1 Instructions

Instructions must be loaded into Tachyon before it can be used to question or perform actions on your network. For more details please refer to Instruction sets page.

4.4.4.1.1 Questions and actions

There are two types of instruction: questions and actions. When an instruction is run it returns a table of responses, for questions the responses are the answers to the question - for actions the responses are the results of running the action. Questions do not require approval. Actions must be approved before they can be run.

4.4.4.2 The History page

When an instruction is run an entry appears in a table on the **History** page. The responses for an individual question or an action can be viewed by clicking on its entry in the **History** page table. This page also supports search and filtering of the instruction history and interacting with the instruction entries, for example to re-run a question.

For more details please refer to History.

4.4.4.3 The Tasks page

Questions may be asked from the **Home** page using the edit field which presents a list of matching questions as you type text into the field, please refer to ExplorerHome page, questions and responses for more details. This is useful if you know the name of the question you want to ask. From the **Home** page you can also view the available questions using the **All questions** button, which displays a list of the questions that have been loaded into Tachyon and can also be organized by Instruction Set.

The **Tasks** page also lets you browse instructions, this time organized into a hierarchy of Task groups, where each Task group denotes a particular functional area and may be broken down into more specific functional areas. For example the **Systems Management** Task group could contain a **Software Distribution** Task group and then any instructions related to software distribution would appear there. A single instruction can also appear in more than one Task group. The last difference is that instructions may be scheduled from the **Tasks** page but not from the **Home** page.

For more details please refer to Tasks.

4.4.4.4 The Scheduling page

Tachyon allows instructions to be scheduled from the **Tasks** page. This enables particular instructions to be run at some point in the future, or on a regular basis depending on your requirements. The Scheduling page lets you interact with the schedules that have been defined for instructions. For more details please refer to Scheduling instructions.

4.4.4.5 History

How the History and individual Instruction **Responses** pages work.

4.4.4.5.1 The History page

On this page you can see a table that shows all the instructions that have replies, are in progress, have expired, have been canceled and have been rejected.

4.4.4.5.1.1 The Instruction History header

Located just above the Instruction History table this section lets you sort, search and filter the instructions displayed in the table. From here you can also export the instruction data for the current page and change the view from a table to a grid.

The options available in the Instruction History header are shown in the following table:

Option	Description
Created	Here you can set a filter on the date and time an instruction was created. The **From** date picker lets you select a time and date that filters the view to show responses that occurred after that time and date. The **Until** date picker lets you select a time and date that filters the view to show responses that occurred before that time and date. You can combine the two to display the responses that occurred between the **From** and **Until** filters.
Filter by	Here you can select to show all or just the instruction responses that are in the following states, corresponding to the **Status** column:

State	Description
Created	A transitory state showing that the instruction has just been created but not yet processed
In approval	The action is awaiting approval

Option	Description	
	Rejected	The action has been rejected
	Approved	The action has been approved
	Sent	The instruction has been sent to the switches via the cores
	Expired	The instruction responses have expired
	Canceled	The instruction has been canceled and any existing responses have been deleted
	Failed	The instruction failed to run

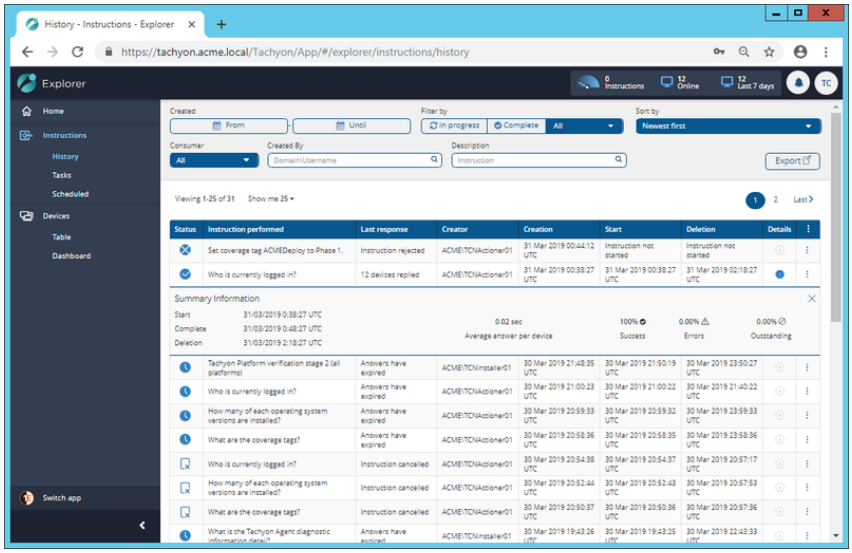
Sort by This control lets you sort the responses by the time they were created or alphabetically by their name in ascending or descending order.

Consumer This control lets you filter the Instruction history according to the consumer that created the instruction. This can be one of the consumers listed in the following table:

Consumer	Description
All	Displays the Instruction history for all the consumers.
Explorer	Investigate, remediate issues and manage operations across all you endpoints in real-time.
Platform	Formerly the SLA Platform, this consumer provides a semi-permanent storage mechanism for different types of information that can be used by other consumers.
Inventory	This is a placeholder for the Inventory consumer, which will be provided in future releases of Tachyon.
GuaranteedState	Ensure endpoint compliance to enterprise IT policiies.
PatchSuccess	Maximise enterprise-wide patch deployment success.

Created By This field filters the Instruction history according to the value in the **Creator** column.

Option	Description
Description	This field filters the Instruction history according to the value in the **Instruction performed** column.
Export	Exports the instructions listed on the current page to a .csv file. This will be saved to your browser's download directory.



4.4.4.5.1.2 The Instruction History table

The Instruction History table displays and lets you interact with the instructions that have been created. The columns are described in the following table:

Column	Description
Status	The icons displayed at the start of each row show the status of the instruction.

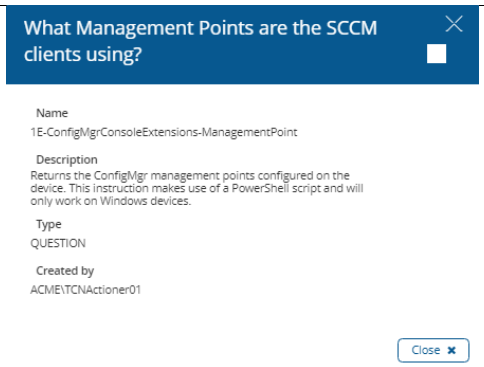
Icon	Description
	This instruction is in progress and still gathering responses
	This instruction has responses that can be viewed
	This instruction's responses have expired
	This instruction has been canceled in Explorer
	This action has been rejected by an approver

Column	Description
Instruction performed	The name of the question or action. Clicking on the **Instruction performed** name in the instruction row takes you to that instruction's Responses page where you can view all its responses.
Last response	The last response received from the instruction. Equivalent to its last known status.
Creator	The user who ran the instruction.
Creation	The time and date the instruction was requested by the creator.
Start	The time and date the instruction was started.
Deletion	The time and date the responses to the instruction will be or were deleted.
Details	Clicking on the information icon in this column expands a **Summary Information** panel below the selected row. The information displayed is described in the following table:

Information	Description
APPROVED BY	This information is only displayed for actions that have been approved and gives the user name for the approver
INSTRUCTION REJECTED BY APPROVER	This information is only displayed for actions that have been rejected and gives the user name for the user who rejected the action. When an action has been rejected this is the only information that is displayed in the **Summary Information** panel.
Start	The time and date the instruction was started
Complete	The date and time the instruction completed
Deletion	The date and time the responses for the instruction will be deleted

Column	Description	
	Average answer per device	Provides an average for the amount of time it took to process the action
	Success	Gives a percentage for the successful responses returned by the devices targeted by the instruction
	Errors	Gives a percentage for the errors returned by the devices targeted by the instruction
	Outstanding	Gives a percentage for the devices targeted by the instruction that have yet to respond.
⋮	Selecting this icon when it is present at the end of a row displays a menu that lets you interact with the instruction. It is only displayed on questions not on actions. The items on the menu are: Item / Description Stop — Displayed if the question is currently running. It stops the currently running question. Re-run — Displayed if the question has completed or the answers have expired. It runs the question again with the same parameters as before. Show advanced information — Displays a popup containing additional information about the instruction. For example the following shows the advanced information for a **What Management Points are the SCCM clients using?** Instruction.	

Column	Description



4.4.4.5.2 The instruction Responses page

On this page you can see the device responses for an individual instruction, summary information about the way the instruction is running and the status of the responses. You can also select to run follow-up questions and actions.

4.4.4.5.2.1 The instruction header

Just below the status bar at the top of the **Responses** page is the instruction header. Here you can see what instruction was run, who ran it and what parameters were set (coverage, question filter etc...). On the right-hand side you can see the percentage of elapsed time for the question's duration and the answers that have been received from the Tachyon client devices currently covered by the question.

You also have an option to stop the instruction. When you click **Stop** you will see a confirmation dialog that gives you the option to keep the responses or not. If you continue Tachyon immediately stops the instruction from running and retrieving any further responses. Any subsequent responses that may come in will be disregarded.

4.4.4.5.2.2 The instruction response tabs

The tabs just below the instruction header provide various information and ways of interacting with the responses. They are described in the following table:

Tab	Description
Summary	This tab provides summary information about the instruction. More information on this tab can be found in #UUIDde48b76b58e22788044acbfe820f803d_id_ExplorerHomepage,questionsandresponsesCheckingthestatusofresponsesusingthesummarytab.
Content	This tab displays the actual response data. Here you can define filters that can be used as the basis for follow-up actions and questions. These follow-up actions and questions will be targeted at the devices whose responses pass the filter. This should be contrasted with the follow-up actions and

Tab	Description
	questions that can be defined on the Questions and Actions tabs, which are targeted at all the same devices as the original instruction.
Status	This tab displays the status information for the responses. Here you can track down the reasons for any errors generated by devices when attempting to respond to the instruction.
Questions	This tab lets you define questions that follow-up the original instruction. Any questions defined here will be targeted at the same devices as the original instruction.
Actions	This tab lets you define actions that follow-up the original instruction. Any actions defined here will be targeted at the same devices as the original instruction.

4.4.4.6 Tasks

How to use Tachyon's Task-based user interface to select and configure instructions.

4.4.4.6.1 Tasks

The **Explorer→Instructions→Tasks** page in Explorer provides a structured view of the instructions defined in the product packs. It also lets you schedule the tasks so they can be run in the future or according to a particular schedule.

4.4.4.6.1.1 Using task groups

The benefit of using **Tasks** lies in the task group structure that is defined in the Product Packs. It is this structure that enables you to focus in on specific task areas to find the particular instruction that you want.

For example you may be interested in instructions related to particular software vendor's products. Depending on the Instructions that you have uploaded to your Tachyon system you may see the following structure:

At the top-level there is a **Software Vendors** task group whose children are **1E** and **Microsoft**.

Underneath the **1E** task group there is a **Tachyon** group that contains **Configuration**, **Diagnostics** and **Verification** groups as well as a couple of Instructions.

Underneath the **Microsoft** task group is the **Configuration Manager** task group containing Instructions related to that product.

4.4.4.6.1.2 Navigating Tasks

Navigating around and using **Tasks** is simple:

The top-level is called **Tasks**. At this level are all the top-level task groups

Clicking on a task group displays all its children in the column to the right, which also shows the name of the selected task group. A child may be a task or another task group

Clicking on a child task group in the next column displays all its children in a column to its right and so on

Clicking on a task displays a page that lets you set the parameters for the task before sending it to some Tachyon client devices

A task is a question or action that has been made part of a task group. Tasks have a grey background and are marked with a question icon

or an action icon

To illustrate the use of the Tasks page we provide two examples: in the first example a user asks a question to retrieve the currently running processes; in the second an actioner has to respond to an emergency situation by asking to perform an action to stop the Configuration Manager client service.

4.4.4.6.1.3 Asking a question from Tasks

In this example we'll track down and ask the **What are the Tachyon Agent settings?** question, as illustrated in the animation shown.

Navigate to the **Explorer**→**Instructions**→**Tasks** page.

The top-level **Tasks** is displayed, here there are three task groups: **Security**, **Software** and **Software Vendors**.

The one we want is the **Software Vendors** task group. Select this to display the child task groups **1E** and **Microsoft**in the next column.

Select the **1E** child task group to display its child task group **Tachyon** in the next column.

Select **Tachyon** and a combination of groups and Instructions are shown at the next level: the **Configuration**, **Diagnostics** and **Verification** task groups and two Instructions. To get to the question we want select the **Configuration** task group.

Scrolling to the bottom of the list of Instructions in the **Configuration** Task group we see the question that we want to run. Click on the **What are the Tachyon Agent settings?** question to display the task page for that Instruction, which provides parameters and information for running the task and two buttons: **Schedule question** and **Ask this question**.

We click the **Ask this question**button and in our example the question is then asked of all the Tachyonclient devices.

After a moment Explorer then displays the responses from all the target devices - task done.

4.4.4.6.2 The Task page

Each question and action has its own Task page which provides information related to the task or action and lets you control how the task is run.

Section	Description
Name and Description	The title of the task and a description that tells you what the task does.
Task parameters	This section displays the **Duration**, **Coverage**, **Filter results**, **Export data on expiry** and **Comments** parameter settings for the current task. To set these you can use the **Parameters** section of the page.
Approximate target	This provides information about the target devices the task will be applied to.
Ask this question Perform this action	This button, named according to whether the task is a question or an action, tells Tachyon to start processing the task.
History	This section provides information from the previous times the task was processed.

Information	Description
Last executions	Provides information on the last time the task was processed.
Projected impact	This describes the projected impact of the task on the Tachyon client devices, based on the last time the task was processed.

Beneath these are a set of statistics related to the selected task based on this instruction's previous runs:

Statistics	Description
Number of times this instruction was run	The total number of times this instruction has been run previously
Average network transfer per device	The average amount of data transferred over the network per Tachyon client device as a result of running the instruction

Section	Description	
	Database rows inserted per device	The total number of database rows inserted per Tachyon client device as a result of running the instruction
	Average execution time on device	The average time it took to run the instruction on a Tachyon client device
Parameters	This section provides controls for setting the duration and coverage for the task. It also lets you set a filter on the results, specify that you want to export the data and add comments.	

4.4.4.6.2.1 A Task page example

As an example of setting parameters on the Task page we'll use the **What processes are running?** question to filter for occurrences of running the winlogon.exe process and restrict this to a coverage of Tachyon client devices running Windows 10. To speed things up we'll set this to gather responses for 10 minutes and keep those responses for 20 minutes. We'll also select to export the data to a previously defined share with the appropriate permissions and add a suitable comment to the question.

The animation opposite shows the following steps

On the **Parameters** pane we set:

Duration to **Gather answers for** 10 minutes and **Duration** 20 minutes

Coverage to check **Operating system Type** Windows and **Version** is greater than or equal to 10

Filter results using the **Executable** attribute where the value contains **winlogon.exe**

Export data to export the responses to the previously configured share **\\ACME-CM01\Tachyon**

Comments to **Need to find currently running winlogon.exe on devices running the Windows 10 os**

We then click the **Ask this question** button to fire the question off to the devices in the coverage.

Here we can see two responses from the two Windows 10 devices in our environment.

We then speed things up in the animation to get to the end of the 10 minutes of data gathering. Complete responses can only be exported once the question has finished data gathering.

We then pick up the results from the **\\ACME-TCN01\TachyonResponses** share and see the complete output for the two responses we saw earlier.

4.4.4.7 Scheduling instructions

Scheduling instructions.

4.4.4.7.1 Creating a scheduled instruction

The following headings show how to create, configure, authenticate and approve a scheduled instruction. A tutorial showing the steps in greater detail is provided on the Scheduling instructions - a tutorial.

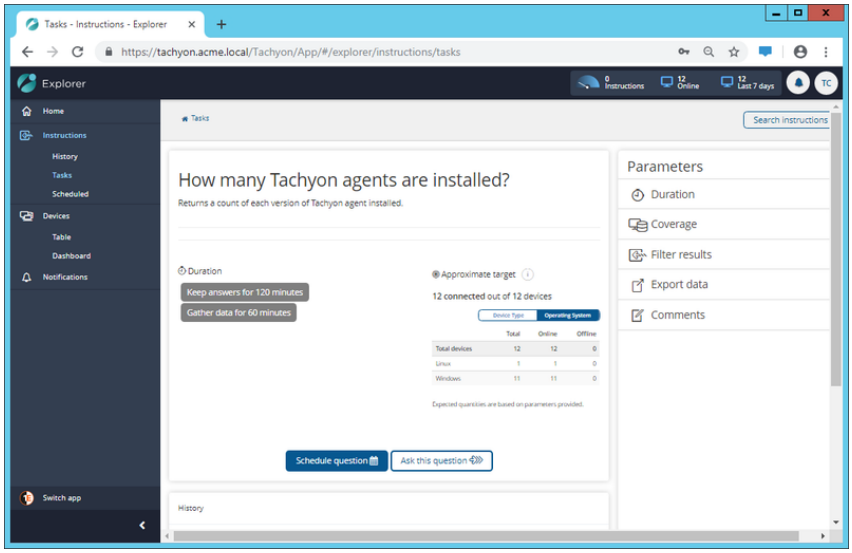
4.4.4.7.1.1 Scheduling an instruction from the Tasks page

Select the Instruction from any of the Task Groups it belongs to or search for it using the **Search instructions** button.

Complete the parameters for the instruction.

Click the **Schedule question** button, as shown in the image.

Fill out the **Instruction scheduler** popup.



The **Instruction scheduler** popup lets you:

Add **Comments** to the schedule that will help later to identify the reasons for the schedule.

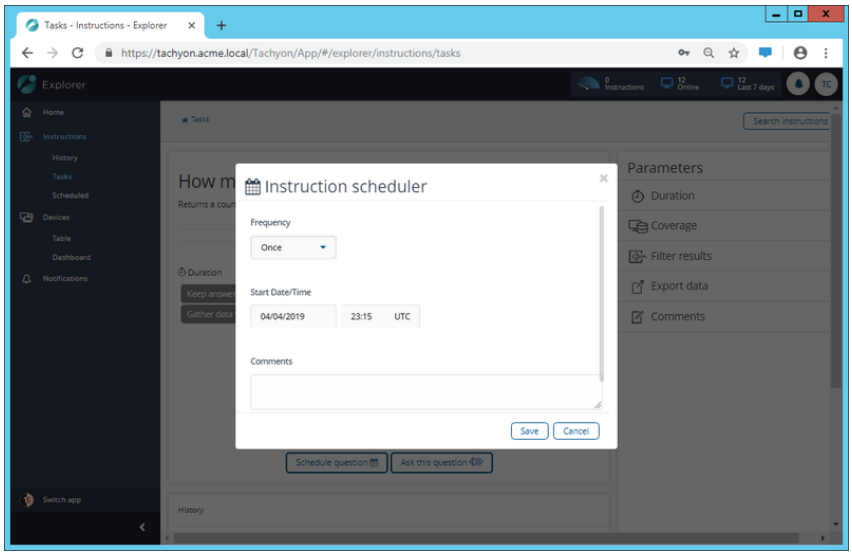
Set the**Frequency**of the schedule:

Type	Description
Once	Specifies a one-off schedule for the selected instruction. The **Once** frequency type uses the following controls: Control — Description **Start** — Set the **Start** dateandtimefor when you want the instruction to run.
Daily	Specifies a daily schedule for the selected instruction between a start and end time.

Type	Description
	The **Daily** frequency type uses the following controls: Control — Description **Start** — Set the **Start** dateandtimefor when you want the schedule to run from. **End** — Set an **End** date and time for when you want the schedule to end. **Every** — Set how many days are left between each run of the scheduled instruction **Repeat Every** — Optionally set how many hours the scheduled instruction is set to repeat on each day it is set to run
Weekly	Specifies a weekly schedule for the selected instruction between a start and end time. The **Weekly** frequency type uses the following controls: Control — Description **Start** — Set the **Start** date and time for when you want the schedule to run from. **End** — Set an **End** date and time for when you want the schedule to end. **Every** — Set how many weeks are left between each run of the scheduled instruction **On** — Check which days of the week you want the scheduled instruction on during the weeks it is set to run
Monthly	Specifies a monthly schedule for the selected instruction between a start and end time. The **Monthly** frequency type uses the following controls: Control — Description **Start** — Set the **Start** date and time for when you want the schedule to run from.

Type	Description	
	End	Set an **End** date and time for when you want the schedule to end.
	Every	Set how many months are left between each run of the scheduled instruction
	Repeat Every	Select the day of the month when you want the scheduled instruction to run on the months it is set to run

After the **Instruction scheduler** dialog has been filled out, you click **Save** to set the schedule. The new schedule will then appear in the **Scheduled instruction** page.



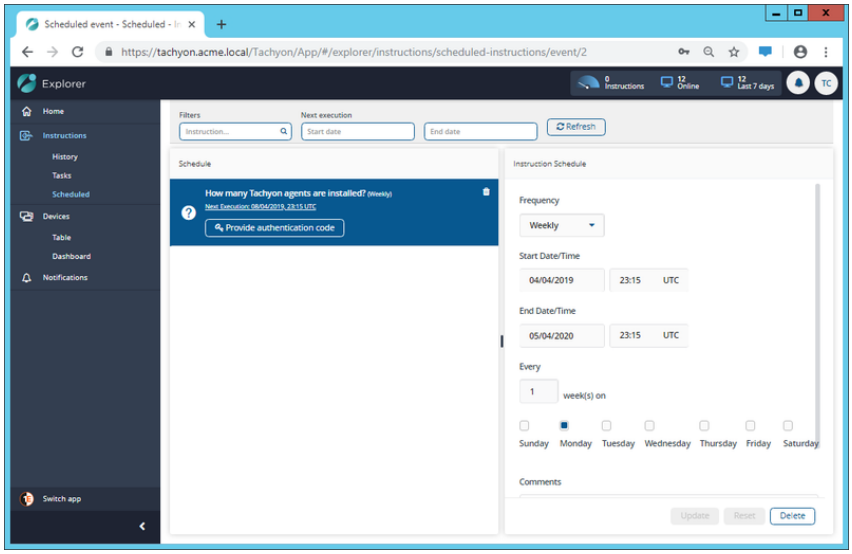
4.4.4.7.1.2 Authentication and approval

The first time the scheduled instruction appears in the **Scheduled instruction** page you will be notified of its authentication and approval state, as shown in the picture opposite.

Before the schedule starts, regardless as to whether the instruction is a question or an action, there are two further steps:

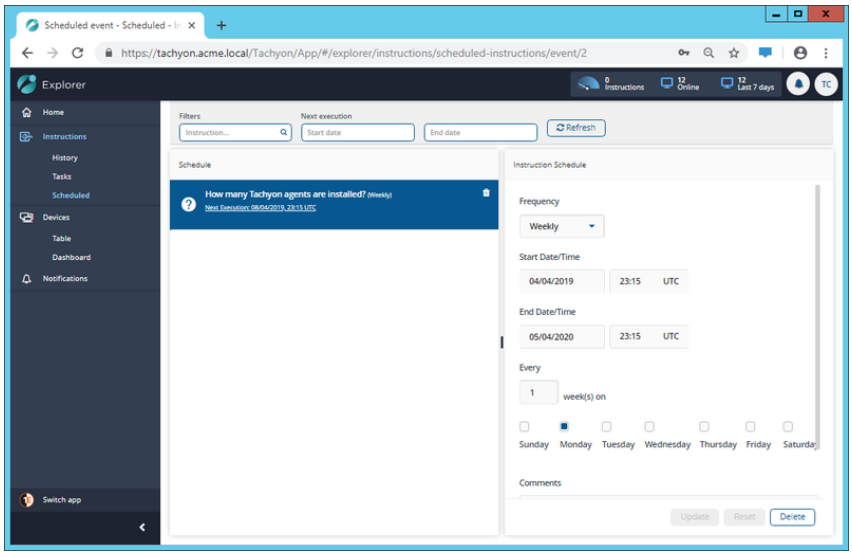
The scheduled instruction must be authenticated, only required if two-factor authentication is enabled.

The scheduled instruction must be approved.



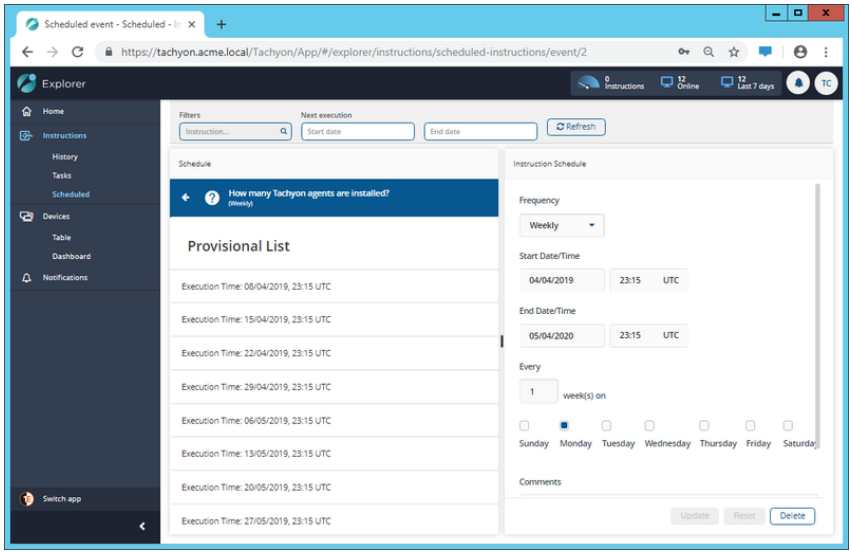
4.4.4.7.1.3 The next execution

After the scheduled instruction has been authenticated and approved its entry in the Scheduled instruction page will show its next scheduled execution date and time, as shown in the picture opposite.



4.4.4.7.1.4 Expanding the execution schedule

Clicking on the **Next Execution** link on the scheduled instruction entry expands the execution schedule, so you can see the future dates and times for the instruction execution, as shown in the picture.



4.4.4.7.2 Updating a scheduled instruction

You can update the configuration for a created scheduled instruction by:

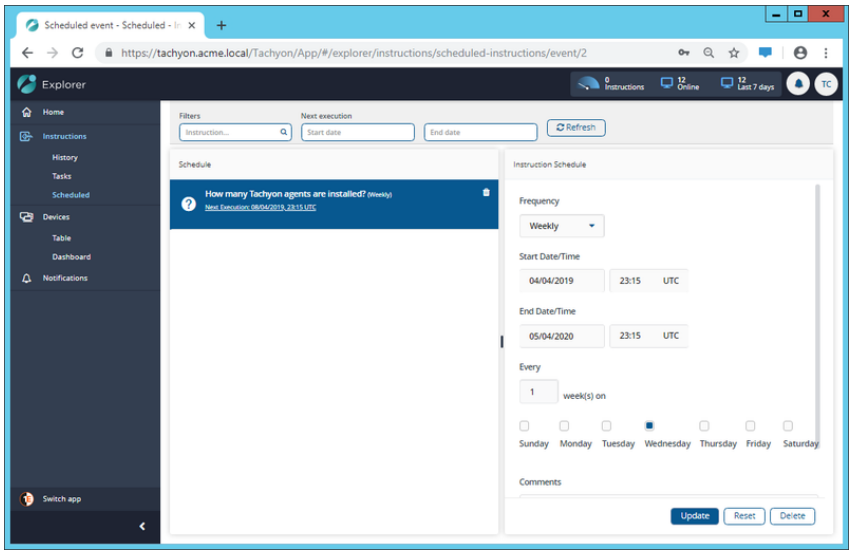
Click on the scheduled instruction entry you want to change in the **Schedule** list.

Modify the parameters on the **Instruction Schedule** panel to its right.

Click the **Update** button to commit the changes.

The picture shows a scheduled instruction where the day for a weekly schedule has been changed from **Monday** to **Wednesday**. The **Update** button is shown highlighted.

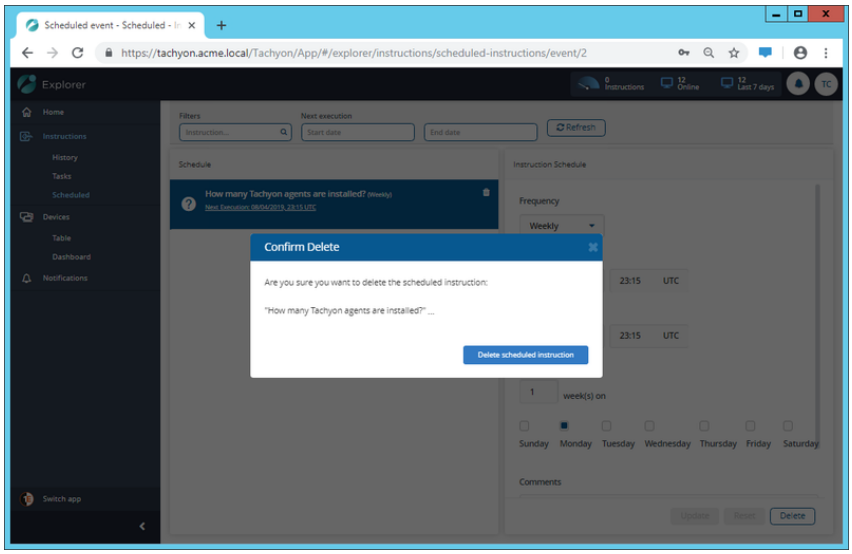
You can also click **Reset** to discard any changes you have made.



4.4.4.7.3 Deleting a scheduled instruction

You can delete a scheduled instruction by clicking on the bin icon to the right of its entry in the **Schedule** list.

Doing this will display the **Confirm Delete** popup that will ask if you want to proceed. Click the **Delete scheduled instruction** button to continue. The schedule for the instruction will then be deleted and no further attempts will be made to run the instruction. Instructions currently in-flight will not be affected by this and will continue to completion.



4.4.4.7.4 Scheduling instructions - a tutorial

A tutorial on creating a daily scheduled instruction that will check for any machines that have Windows update pending reboots.

4.4.4.7.4.1 Creating a weekly instruction schedule

To illustrate this we will use a simple example where Tachyon will check every week to see if any Windows updates are pending a reboot.

4.4.4.7.4.1.1 Selecting the question for scheduling

Use the Tasks page to locate and select the instruction you want to schedule.

Set any desired **Duration** and **Scope** parameters for the instruction.

Click the **Schedule question** button.

The animation starts with the **Which Windows updates are pending a reboot?** question already selected from the Tasks page.

4.4.4.7.4.1.2 Filling out the Instruction scheduler dialog

Set the **Frequency** to **Weekly**.

For any schedule you have to set the **Start Date/Time**. We want ours to run each **Sunday** at **23:53** AM, so we leave the **Start** date at the default current time plus one hour.

Set the **End Date/Time**. We want to review the schedule on April the 14th 2020 so we set this as the **End** date.

For a weekly schedule you must select how many weeks between running the instruction. In our case we want the schedule to run on a weekly basis, so we leave the **Every** field at the default of **1**.

For a weekly schedule you also select which day of the week you want the schedule to run. In our example we click the **Sunday** box to highlight it.

Add a suitable comment to the schedule. This will be stored with the schedule and can be used as a reminder for why the schedule was configured.

This completes the configuration of the **Instruction scheduler** dialog so we click **Save** to create the schedule.

4.4.4.7.4.1.3 Authenticating and approving the schedule

Normally questions do not require authentication and approval, however for scheduled questions this is required.

The scheduled instruction entry appears in the **Scheduled instruction** page showing that it needs an authentication code.

The user requesting the schedule is sent an email with the authentication code.

They click on the **Provide authentication code** button and enter the code in the dialog then click **Submit.**

The scheduled instruction entry now shows that it is Awaiting Approval.

The approver receives an email requesting approval for the requested scheduled instruction.

They log on to Explorer and fill out the approval request notification, by entering a suitable approval comment, checking the **I understand the impact of this scheduled instruction and approve this request** checkbox and clicking the **Approve** button.

The scheduled instruction has now been authenticated and approved.

4.4.4.7.4.1.4 The scheduled instruction

Once authenticated and approved, the scheduled instruction entry now displays a link which indicates the scheduled times that the selected instruction will be run. In our example the instruction will now run every **Sunday** at **23:53** AM until the **14th April 2020**.

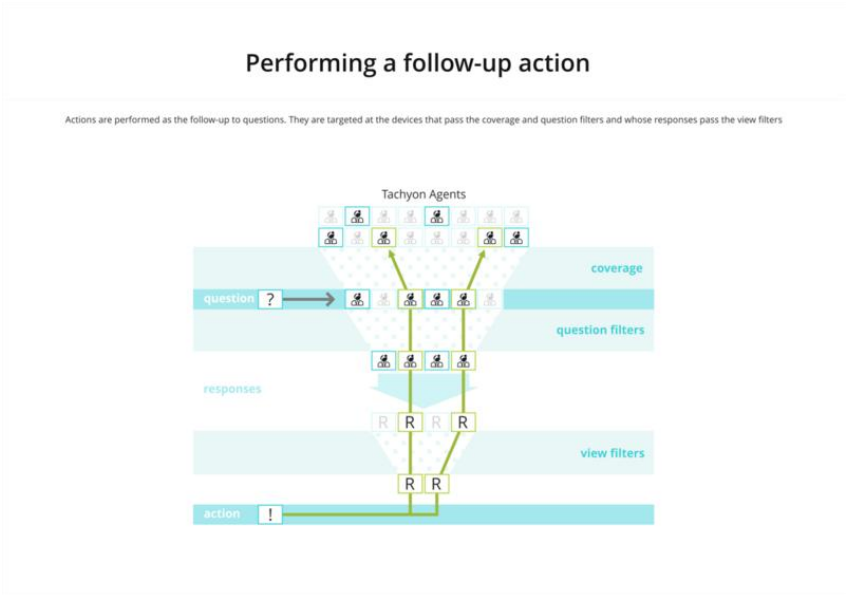
4.4.5 The action approval workflow

How to run actions with approval.

4.4.5.1 Running an action that restricts the number of devices sending

To run any action in Tachyon, you first need to ask a question. Questions may have coverage and question filters applied that restrict the number of devices that send responses.

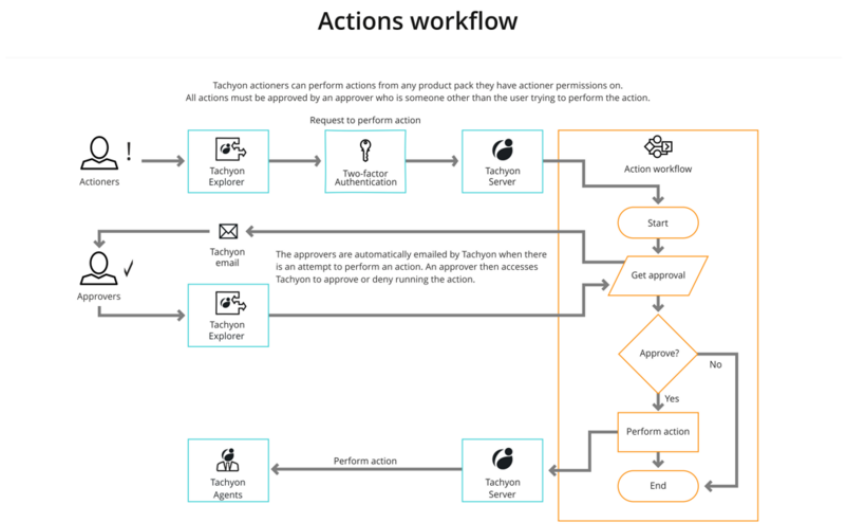
When the responses come back you can apply a view filter to reduce the responses even further. When you select a follow-up action, this will be only be performed on the final set of filtered responses.



4.4.5.2 Approving an action

Configuration of approvers is explained on the Roles page.

Enabling Tachyon users to run actions on devices in a network is always a powerful proposition. The potential for mistakes or deliberately malicious actions is always there. For this reason Tachyon has role-based access control to the features it presents and it implements an approval workflow that implements a process to prevent unauthorized changes from taking place.



4.4.5.3 Two-factor authentication

Two-factor authentication is now the default mode for running actions. When an actioner creates an action they are first required to enter their password. They are then required to enter an authentication code which is sent to them by email. Because this is now the default mode for

performing actions there are numerous examples of two-factor authentication throughout this documentation wherever an action is described. A good example of the two-factor authentication process can be found in Performing an action - tutorial. You can also find some additional details in Two-factor authentication.

4.4.5.4 Performing an action - tutorial

A quick tutorial on asking a question and then performing an action, getting approval and confirming the action has been performed successfully.

4.4.5.4.1 The example

To illustrate the process of performing an action we use an example of setting registry entry for the **ACMEFinance** application. We do not want to create the registry entry, we only want to change an existing entry.

The **ACMEFinance** application has a registry entry that determines whether the automatic backup feature is enabled. We want to run a question which will find devices where the registry entry has the feature turned off and then perform a follow-up action that will turn it on for those devices.

The registry entry for ACMEFinance is under the following key:
HKLM\SOFTWARE\ACME\ACMEFinance\AutoBackupEnabled

The value is a string and may be set to either **TRUE**, where the feature is turned on, or **FALSE**.

4.4.5.4.2 Asking a question

In this example, to perform a follow-up action we first ask a question. The responses to the question then gives Tachyon a list of devices to perform the action on.

In our example we want to check a specific value in the registry and change it if necessary. To find the registry related questions we enter the text **registry** into the Explorer and then select
What is the value of registry entry <hive> <subkey> <name>?

For our example the user is **TCNActioner01**, with the All Instructions Actioner role, who is going to set the registry entry for the **ACMEFinance** application. The animation illustrates the following steps:

Type **registry** into the I want to field and select the
What is the value of the registry entry <hive> <subkey> <name>? question.

Fill out the question variables, leaving **<hive>** as the default **HKLM**, setting **<subkey>** to **SOFTWARE\ACME\ACMEFinance** and **<name>** to **AutoBackupEnabled**

Click **Ask the question** and a number of responses are returned from devices where the **ACMEFinance** application is installed.

We are only interested in the responses where the value is **FALSE**. Double-clicking on the **FALSE** value in the responses opens up the **Filter results** panel with the **Value** set to **FALSE**. Cllck the **Search** button to filter the responses.

Now the responses show only the responses where the value for the registry key is **FALSE**. This filtered list represents the devices where we want to follow-up with an action to change the registry entry.

4.4.5.4.3 Follow-up with an action

Click the **Follow-up action** button.

Type **registry** into the edit field and then select the **Set registry entry <hive> <subkey> <name> to <valuetype> <value>** action from the list of matching actions.

Fill out the action variables, leaving **<hive>** as the default **HKLM**, setting **<subkey>** to **SOFTWARE\ACME\ACMEFinance** and **<name>** to **AutoBackupEnabled**. The **<valuetype>** variable must be set to **REG_SZ** to indicate a string type and lastly the **<value>** gets set to **TRUE**.

Having set and reviewed the parameters, scroll to the bottom of the page and click the **Perform this action** button

The action is subject to confirmation, authentication and approval. First confirm your credentials by entering the password of **TCNActioner01**.

When challenged to provide an authentication code, emails for **TCNActioner01** are checked, and the code is copy and pasted it into the challenge dialog.

Approvers for this action are sent an email. **TCNApprover01** is a global approver, receives the email, and uses the link at the bottom of the email to navigate to Explorer and approves the action.

The action runs and the responses appear to **TCNActioner01**. In our example **TCNActioner01** sees that 1 device has had a value set.

Clicking on a response shows the device that made the response. In our example it is the **ACME-WIN1001.acme.local** device that has responded. This was the device that responded to the original question with the value for the registry entry as set to **FALSE**.

4.4.5.4.4 Confirm the action was successful

To confirm that the action was successful you can re-run the original question to retrieve that registry entry value.

> **Note**
>
> Before a follow-up action is run, all devices within the coverage will be re-asked the same question, and the Tachyon client will apply the filter to the latest result on each device. In this example, if someone changed the registry entry on their device from TRUE to FALSE *after* the first question was asked, then the filter will detect this and the follow-up action will also apply to this device.
>
> This is why you see the Approximate target remain the same as when you asked the first question. The number of devices connected will change only if devices within the coverage come online or go offline.
>
> **Note**
>
> Using the Follow-up action button ensures the action is carried out on the filtered devices. If the Action tab is used instead then the Follow-up action applies to all the devices that were asked the question without using the filter, as if the filter has been reset.

4.4.5.5 Two-factor authentication

How Tachyon implements two-factor authentication for users running actions.

4.4.5.5.1 Two-factor authentication

Tachyon is a powerful tool that enables changes to be made across an organization's entire estate. It employs RBAC to ensure that only users with the required permissions can run particular actions. In addition, at the point of running an action, Tachyon uses two-factor authentication to ensure that the logged-on user is actually the user with the correct permissions.

Two-factor authentication is implemented through a unique authentication code (one-time password) that is generated at the point of running an action. This authentication code is then sent to the user by email. The authentication code is then used to proceed with the action.

4.4.6 Tagging client devices

Tachyon client devices can have a number of custom tags assigned using Tachyon and the Tachyon clients. There are two types of tag: Device tags, which can be used in the scopes for questions and actions to help target specific collections of devices; and freeform tags that can be queried and set using specific questions and actions.

4.4.6.1 Device versus freeform tags

Tachyon supports two kinds of tag that can be used to set properties on Tachyon client devices. The Tachyon client stores both types of tag in persistent storage. Values are set or deleted using actions and queried using questions. The differences are described below.

Tag type	Description
Device	Can also be used when defining the coverage for questions and actions. A Full Administrator must define the names and values for Device tags before they can be applied to devices using Device tag actions. Once set by an action, the Tachyon client reports device tags back to the System where they are stored in the TachyonMaster database for each device, which is how they can be used to define coverage for questions and actions. The Tachyon client regularly reports back its list of tags. The list consists of a separator and name=value for each tag plus a final separator at the end of the list. The entire list of name=value pairs and their separators must not exceed 511 bytes. Any tags that exceed this limit are not reported back. Only the tags reported back by each client can be used for coverage. Therefore, the length of tag names and values should be kept short if many different tags are to be used. The maximum length of a tag name is 16 characters, and the maximum length of a tag value is 32.

Tag type	Description
	More details on the Coverage tag workflow are given below, including links to associated tutorials.
Freeform	Cannot be used when defining the coverage for a question. Freeform tags can be set with arbitrary names and values that are defined only when running a Freeform tag action. There is no limit to the number of freeform tags or the length of the list, and no limit to the length of tag name or tag value.

Tag names are case-insensitive. Tag values are not case-sensitive, and case is preserved.

Note

Please refer to /document/preview/737044#UUID-c70396b5-6ef9-af19-7b28-3665ddcb7687 for how to use tagging methods when writing your own instructions.

4.4.6.2 The Device tag workflow

You create and manage Device tags using the **Custom properties** page in **Settings→Configuration**.

Tachyon enables Device tag properties to be created and set on Tachyon client devices, which can then be used when setting the coverage for a question. The basic workflow is:

A Full Administrator defines the name of a Device tag and one or more associated values. See Adding properties - tutorial for more details on this step.

Actioners with permissions to the Tachyon client tags Product Pack run actions that use the defined properties and values and assign them to particular client devices. See Actions to set tags - tutorial for more details on this step.

Questioners can then use the **Tags** parameter, when defining the coverage for a question, to constrain the coverage to particular properties and values thereby targeting particular client devices. See Using tags to set the coverage for a question - tutorial for more details on this step.

4.4.6.3 Adding properties - tutorial

A quick tutorial on adding properties and values for use when setting the coverage for questions.

Tachyon enables Device tag properties to be created and set on client devices, which can then be used when setting the coverage for a question. The basic workflow is:

A Full Administrator defines the name of a Device tag and one or more associated values. See Adding properties - tutorial for more details on this step.

Actioners with permissions to the Tachyon client tags Product Pack run actions that use the defined properties and values and assign them to particular client devices. See Actions to set tags - tutorial for more details on this step.

Questioners can then use the **Tags** parameter, when defining the coverage for a question, to constrain the coverage to particular properties and values thereby targeting particular client devices. See Using tags to set the coverage for a question - tutorial for more details on this step.

This page provides a quick tutorial on how to perform step 1.

To illustrate the configuration of device tags, we use an example where the property relates to the business function of a device. We'll create a single **Department** property with a number of values that enables us to differentiate between the departments we want Tachyon to support.

4.4.6.3.1 Adding a property and values

The first step to creating a property with values is to create the property name. Generally to do this you click on the **Add** button on the **Settings→Custom Properties→Device Tags** page.

The following steps walk through how to add a Device tag:

4.4.6.3.1.1 Add a property and values

The following steps can be used to create a property name:

Navigate to **Settings→Configuration→Custom properties→Device Tags**.

Click the **Add** button.

Type in a name for the new device Tag.

You now need to add values to the property:

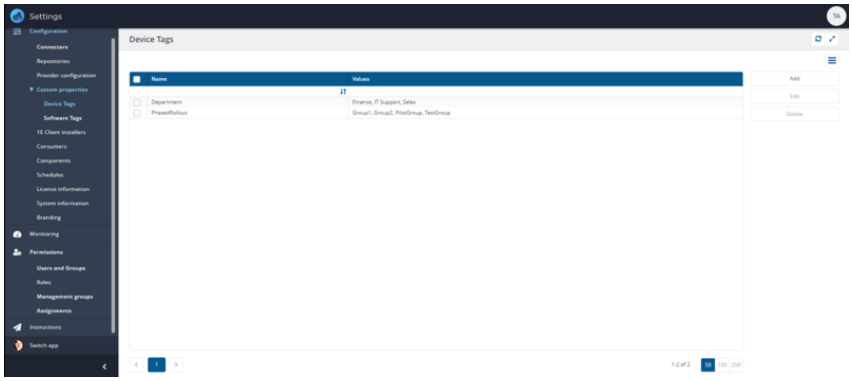
In the edit field below the **Values** heading, type in a value for the property.

If you want to add more values, click the **+** button beneath the **Values** heading.

Repeat step 4 to add as many values as you require for the selected property name.

When all the values have been added, click **Add**. (An error message is displayed if you exceed a maximum of 16 characters).

We use these steps to create Device Tags for Finance, IT Support and Sales departments.



In this brief tutorial, we've shown how to create a Device tag. The next step is to apply a tag to the appropriate devices, as described in Actions to set tags - tutorial.

4.4.6.4 Actions to set tags - tutorial

A quick tutorial on adding properties and values for use when setting the coverage for questions.

Tachyon enables Device tag properties to be created and set on client devices, which can then be used when setting the coverage for a question. The basic workflow is:

A Full Administrator defines the name of a Device tag and one or more associated values. See Adding properties - tutorial for more details on this step.

Actioners with permissions to the Tachyon client tags Product Pack run actions that use the defined properties and values and assign them to particular client devices. See Actions to set tags - tutorial for more details on this step.

Questioners can then use the **Tags** parameter, when defining the coverage for a question, to constrain the coverage to particular properties and values thereby targeting particular client devices. See Using tags to set the coverage for a question - tutorial for more details on this step.

This page provides a quick tutorial on how to perform step 2.

4.4.6.4.1 Setting tags

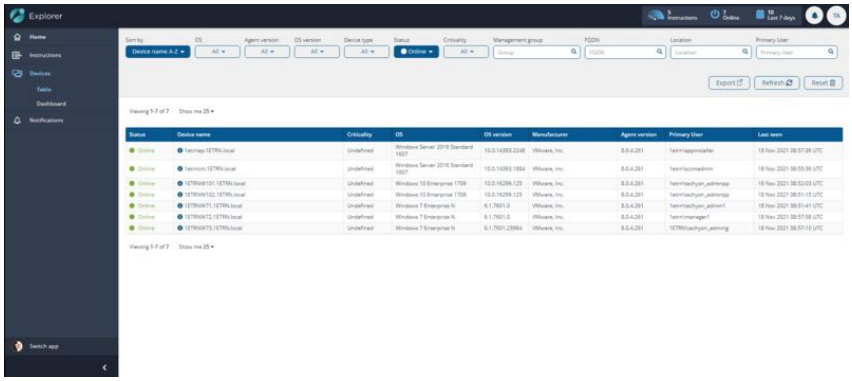
4.4.6.4.1.1 The example

On the Adding properties - tutorial page we set up a scenario with three departments whose devices we want to manage using Tachyon. The three departments are **Finance**, **IT Support** and **Sales**. We want to map these departments onto the devices in our example by setting tags. The only thing that links the devices is the departments they belong to, and this is known according to the FQDN of the devices. The best way to handle the setting of the tags is to use a question where the coverage is set to a list of FQDN for a particular department, and follow that with an action that sets the tags for that department.

The following table shows the department mapping we want to model using tags:

Department	Device FQDN
Finance	1ETRNW73.1etrn.local
IT Support	1ETRNW102.1etrn.local
Sales	1ETRNW71.1etrn.local
	1ETRNW72.1etrn.local

Our example environment, as shown in the picture, is obviously very small, but the advantages will be seen for much larger examples, where each department's set of devices may run into the hundreds or even thousands.



4.4.6.4.1.2 Choosing the right Instruction

Which Instruction should you run? You may already know what devices to target, and so can create a management group, or provide a list of FQDN to run an action against, if now then running a question to obtain the list would be a good way to begin.

Fundamentally, questions return a list of device names, with associated information. This list of device names can then be used to target the devices on which to run actions.

There are many different circumstances, questions and actions that may be used, but generally the question selected should try to meet the following guidelines:

The question should identify a superset or the set of devices that you want to run an action on. Question responses can always be refined by setting coverage, response filters or view filters.

Avoid questions that retrieve information that isn't relevant to the action. This is mainly to avoid unnecessary network traffic.

In our example, we will select the question of
How many of each operating system version are installed?.

We choose this question because:

We want a question that would get a response from every device, and we'll apply a coverage that selects the devices we want using their FQDN

The question does not return much unnecessary information.

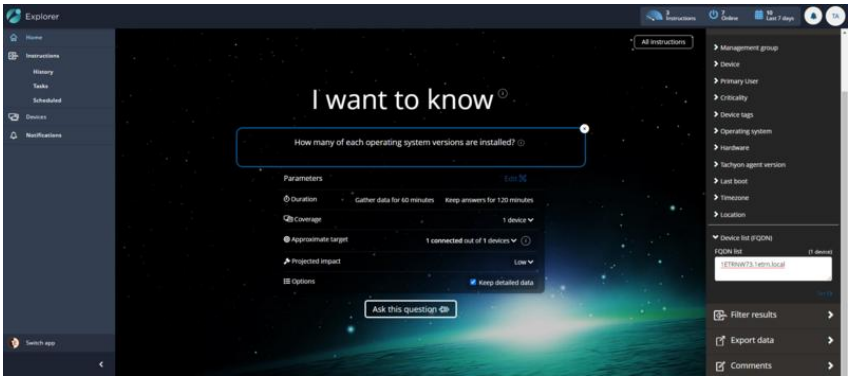
4.4.6.4.1.3 Setting coverage tags

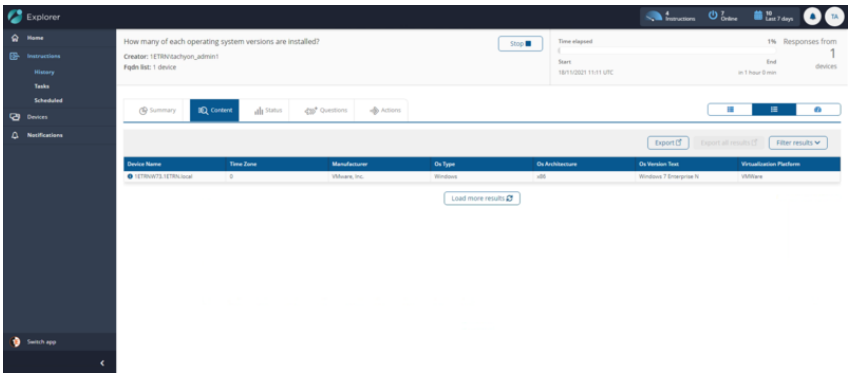
For our example, the user **Tachyon_Admin1**, with the Full Administrator role, is going to set the tags for the finance department. The following steps illustrate how to achieve this:

Tachyon_Admin1 selects the **How many of each operating system version are installed?** question.

After the question has been selected, they then edit the question parameters, expand the **Coverage** heading and enter the FQDN for the device in the finance department into the field under the **Device List (FQDN)** heading. To save the list to the question they click on **Set**.

Asking the question, by clicking on the **Ask the question** button, gets a response from the device named in the FQDN list.





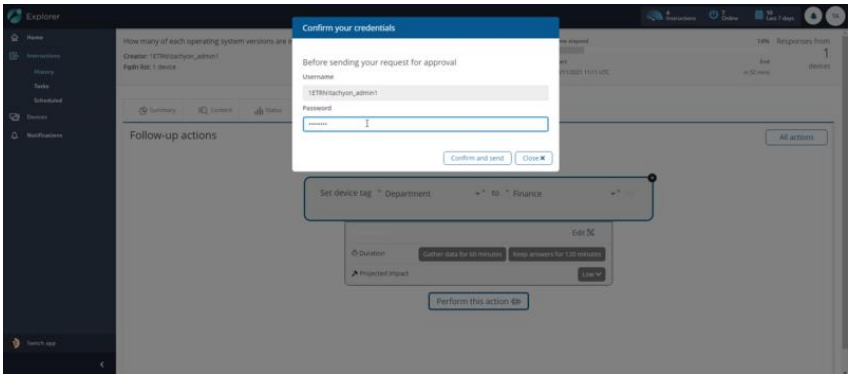
Having got back the responses they were looking for they now run the **follow-up actions** that will set the correct tag for that device. The action is selected from the **Actions** tab.

They type **set device** into the edit field and then select the **Set device tag <tagname> to <tagvalue>** action.

The parameters for the action are populated from the device tag and values that have previously been set. They set the **<tagname>** to **Department** and the **<tagvalue>** to **Finance**.

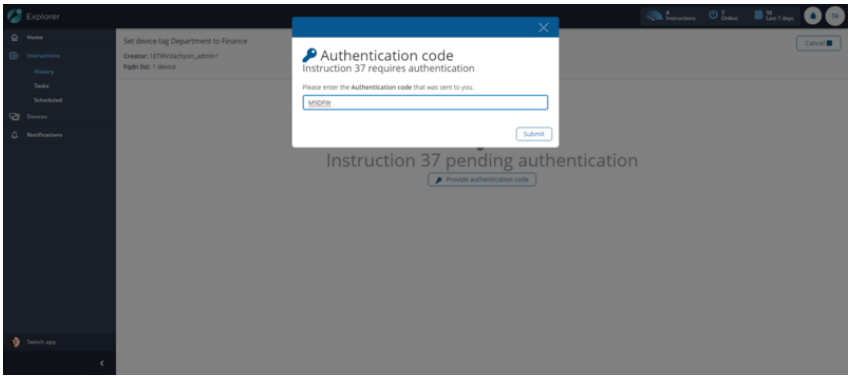
After setting the values they click the **Perform this action** button.

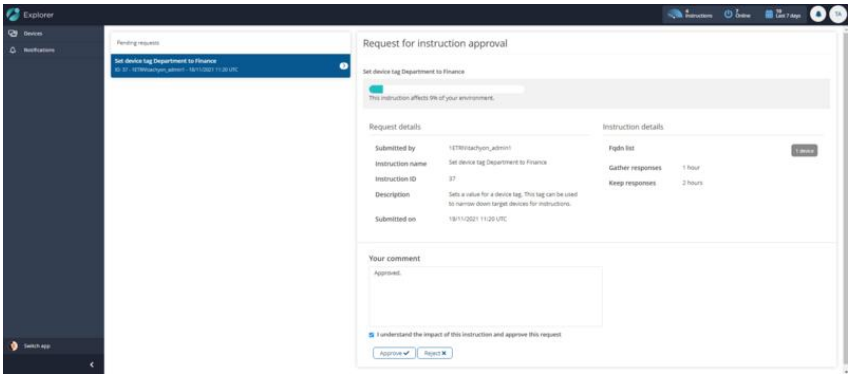
The action is subject to confirmation, authentication and approval. They first confirm their credentials by entering their password.



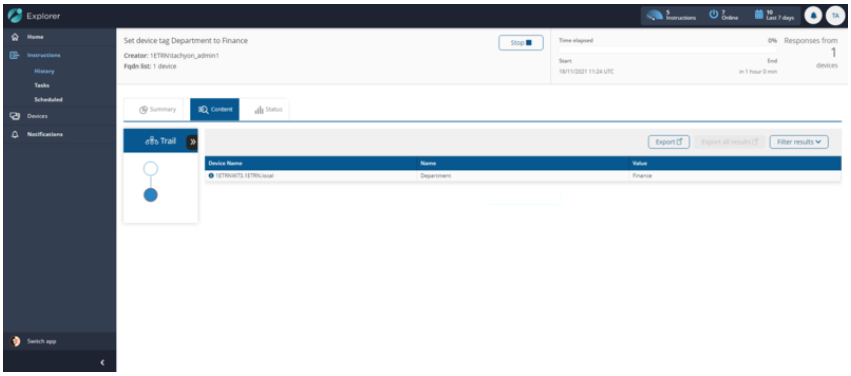
When challenged to provide an authentication code, **Tachyon_Admin1** then checks their email, copies the code and pastes it into the challenge dialog.

Now **Tachyon_adminG**, a global approver, will be sent an email, using the link at the bottom of the email they navigate to Explorerand approve the action.





The action now runs and the responses appear to **Tachyon_Admin 1**. Here you can see the device that was targeted using their FQDN has responded and the tag with the property name **Department** and a value of **Finance** has been set.



Having set the tag for the finance device, the exact same approach can be used to set the tags for the other two department's devices. Once all the tags have been set, questions can be asked with scopes that target the tags, as described in Using tags to set the coverage for a question - tutorial.

4.4.6.5 Using tags to set the coverage for a question - tutorial

A quick tutorial on using predefined tags when setting the coverage for a question.

Tachyon enables Device tag properties to be created and set on client devices, which can then be used when setting the coverage for a question. The basic workflow is:

A Full Administrator defines the name of a Device tag and one or more associated values. See Adding properties - tutorial for more details on this step.

Actioners with permissions to the Tachyon client tags Product Pack run actions that use the defined properties and values and assign them to particular client devices. See Actions to set tags - tutorial for more details on this step.

Questioners can then use the **Tags** parameter, when defining the coverage for a question, to constrain the coverage to particular properties and values thereby targeting particular client devices. See Using tags to set the coverage for a question - tutorial for more details on this step.

This page provides a quick tutorial on how to perform step 3.

4.4.6.5.1 Using tags in question coverage

4.4.6.5.1.1 The example

On the Actions to set tags - tutorial page we set the tags for the devices belonging to a number of departments in our organization. Now we're going to extend the example to deal with a particular scenario and show how the tags can be used when defining the coverage for a question.

In our environment we've just rolled out a software package for a product called **Sales Application**, this application is used by a number of departments - but we've realized that the **Finance** department use some extra features of the application that requires a special license. So we urgently want to find if the device in the **Finance** department has the software installed and apply the special license to only that device.

To find the device we want to treat we will ask the question **What versions of <appname> are installed?**

4.4.6.5.1.2 Using device tags

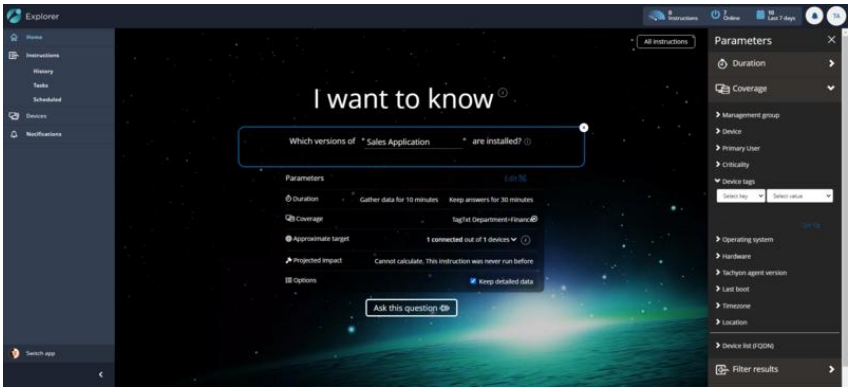
For our example the user **Tachyon_admin1**, with the Full Administrator role, is going to run the question to locate if the **Sales Application** is on the **Finance** department device.

Tachyon_admin1 types **Which versions** into the I want to know field and then selects **What versions of <appname> are installed?** from the list of matching questions.

Once the question is loaded they set the **<appname>** inline parameter to **Sales Application**, the application they want to track down.

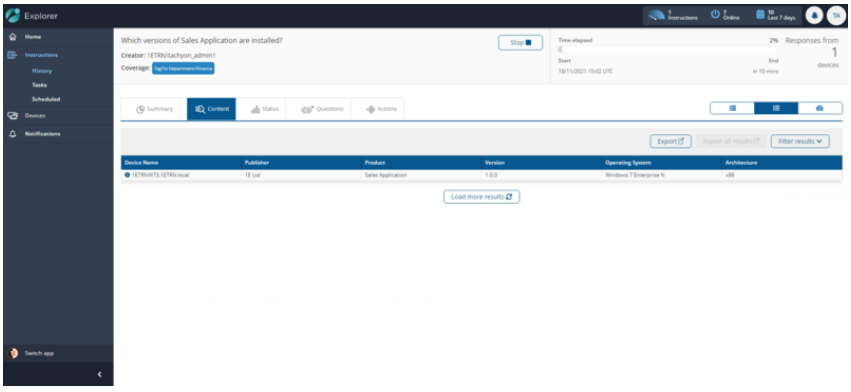
They then click on the **Edit** link to expand the **Parameters** rollout, click on **Coverage** to expand that heading and then on **Device Tags** to display the coverage tags controls.

They select **Department** from the **Select key** dropdown list, and **Finance** from the **Select value** dropdown list (populated when**Department** was selected) and click **Set** to save the coverage to the question.



Having set the coverage they then click **Ask this question**, which will ask the question of just those devices with the selected tag set.

The responses in our example shows the connected finance devices has the **Sales Application** software.



We can now target the **1ETRNW73.1etrn.local** device outside of Tachyon with the special license update.

In this tagging example we've seen how Extended Properties administrators define the properties that can be used for tagging, as described in Adding properties - tutorial. We've seen in turn how those tags can be set on Tachyon client devices by an actioner, as described in Actions to set tags - tutorial. Finally, on this page we've seen how those tags can be used to define the coverage for a question and help to target otherwise unassociated devices simply and effectively.

4.4.6.6 Creating the Tags instruction set

Steps for creating the Tags instruction set containing instructions for setting, deleting and querying Device tags and freeform tags.

4.4.6.6.1 Prerequisites

To create the Tags instruction set, you will need the following:

A Full Administrator will need the following role permissions:

Full Administrator role to upload the 1E-Explorer-TachyonCore Product Pack instructions and assign them to a new instruction set.

4.4.6.6.2 Creating the Tags instruction set

The steps below create an instruction set called **Tags**. Users who are members of the following built-in system roles will automatically then be able to use these instructions on all devices.

Full Administrator

All Instructions Questioner

All Instructions Actioner

All Instructions Approver

The **Tags** instruction set will contain 17 instructions from the **1E-Explorer-TachyonCore Product Pack** described in the table below. The product pack filename is **1E-Explorer-TachyonCore.zip** and is downloaded as part of the **Tachyon Product Packs** zip file from the 1E Support Portal. For more information about this product pack and its instructions, please refer to 1E Explorer TachyonCore product pack.

First upload the instructions:

Logon to the Tachyon Portal using a user account with the **Full Administrator** or **Group Administrator** role.

Open the **Settings** application.

Navigate to the **Settings**→**Instructions**→**Instruction sets** page.

Click on the **Upload** button.

In the Open dialog, navigate to the location of the **1E-Explorer-TachyonCore.zip** file.

Select **1E-Explorer-TachyonCore.zip** and click **Open**.

Over 100 instructions contained in the zip file will initially be added to the default **Unassigned** instruction set. Instructions in the **Unassigned** instruction set cannot be used, so you will need to select and add the tag instructions to a new instruction set:

Click on the **Unassigned** folder.

Enter **tag** into the search field to filter the tag instructions, some other instructions may also be visible.

Select the 17 tag instructions to add to the new set, by clicking the checkbox at the start of each instruction row in the list.

Click the **Add new set** button in the button panel to the right of the page.

In the **Add new instruction set** popup subsequently displayed, type **Tags** as the name.

Optionally select a **custom icon** file.

Ensure that the **Include 17 selected instructions** checkbox is checked.

Click the **Add** button to add the new instruction set, with the selected instructions.

4.4.6.6.2.1 Tag instructions in the 1E-Explorer-TachyonCore product pack zip

Instruction file name	Instruction text (ReadablePayload)	Type
1E-Explorer-TachyonCore-CreateEmptyFreeformTag	Create an empty freeform tag named <tagname>.	Action
1E-Explorer-TachyonCore-DeleteAllCoverageTags	Delete all coverage tags.	Action
1E-Explorer-TachyonCore-DeleteAllFreeformTags	Delete all freeform tags.	Action
1E-Explorer-TachyonCore-DeleteCoverageTag	Delete coverage tag named <tagname>.	Action
1E-Explorer-TachyonCore-DeleteFreeformTag	Delete freeform tag named <tagname>.	Action
1E-Explorer-TachyonCore-CheckIfCoverageTagExists	Does coverage tag <tagname> exist?	Question
1E-Explorer-TachyonCore-CheckIfFreeformTagExists	Does freeform tag <tagname> exist?	Question
1E-Explorer-TachyonCore-CountCoverageTags	How many coverage tags are there?	Question
1E-Explorer-TachyonCore-CountFreeformTags	How many freeform tags are there?	Question
1E-Explorer-TachyonCore-CheckIfCoverageTagHasGivenValue	Is coverage tag <tagname> set to <tagvalue>?	Question
1E-Explorer-TachyonCore-CheckIfFreeformTagHasGivenValue	Is freeform tag <tagname> set to <tagvalue>?	Question
1E-Explorer-TachyonCore-SetCoverageTag	Set coverage tag <tagname> to <tagvalue>.	Action
1E-Explorer-TachyonCore-SetFreeFormTag	Set freeform tag <tagname> to <tagvalue>.	Action

Instruction file name	Instruction text (ReadablePayload)	Type
1E-Explorer-TachyonCore-GetAllCoverageTags	What are the coverage tags?	Question
1E-Explorer-TachyonCore-GetAllFreeformTags	What are the freeform tags?	Question
1E-Explorer-TachyonCore-GetCoverageTag	What is the value of the coverage tag <tagname>?	Question
1E-Explorer-TachyonCore-GetFreeformTag	What is the value of the freeform tag <tagname>?	Question

4.4.7 Using Device Criticality

Assigning Criticality to devices according to their importance within your organization.

4.4.7.1 Overview

Device criticality is an attribute of a device that you define for its importance within your organization. You must first agree the criteria for importance within your organization, and ensure all Tachyon users have the same understanding of criticality and how they are expected to use it.

Criticality is set on devices using an instruction, as described below in Setting Device Criticality.

Tachyon allows you to use Criticality to define the following:

Rules to create Management Groups - see Management Groups page

Coverage for instructions, for example, you can choose to target an instruction to be sent only to devices whose criticality is set to any one of the following:

Undefined (or not set)

Non-critical

Low

Medium

High

Critical.

Criticality is displayed in a number of app pages in the Tachyon Portal, including the following:

Experience	Devices page (Device View - Identification tab)
	Experience Filters

Explorer	The Devices Table (Device View - Identification tab) Coverage parameters
Guaranteed State	Devices page (Device View - Identification tab) Guaranteed State Overview page
Content Distribution	Nomad app (Device View - Identification tab)
Patch Success	Device pages Targeted Devices tab
Settings	Management Groups page

4.4.7.2 Setting Device Criticality

Device criticality is set using the instruction **Set the criticality of my devices to <criticality>** where **<criticality>** is selected from the list above.

In Explorer, type the instruction and then choose the desired criticality from the dropdown.

Select the coverage for the instruction and submit it. After approval, devices which match the specified coverage value will have their criticality set to the specified value.

Any devices that do not have their criticality set are reported as **Undefined** or **Not set**.

There is a corresponding instruction **What is the criticality of my devices?**

> **Note**
>
> The two instructions **1E-Explorer-TachyonAgent-GetCriticality** and **1E-Explorer-TachyonAgent-SetCriticality** are available by uploading the Classic Product Pack **1E-Explorer-TachyonAgent**, which is included in the **Tachyon Platform** zip downloaded from the 1E Support Portal.

4.4.8 Using Location

Assigning Location to devices within your organization.

4.4.8.1 Overview

Explorer allows you to use Location when defining coverage for an instruction. For example, you can choose to target an instruction to be sent only to devices whose location has been set. Location is an attribute of a device. You must agree a naming convention for locations within your organization, and ensure all Tachyon users have the same understanding of location and how they are expected to use it. For example, it may simply be a city or town name, a known abbreviation used within your organization, an address, building name, that might include floor or room name.

In the case of a laptop, it might represent the office base of its owner instead of its physical location.

Location is currently displayed in the following pages in the Tachyon Portal.

Application	Page
Multiple applications	Device View
Explorer	The Devices Table The Devices Dashboard
Guaranteed State	Guaranteed State Overview page
Patch Success	Device pages Targeted Devices tab

4.4.8.2 Assigning a device to a location

You assign a device to a location by using the instruction
Set the location of my devices to <location> where <location> is entered as free-form text up to 99 characters.

In Explorer, type **location** in the search field and select the instruction. Enter the desired location name, select the coverage for the instruction, and then submit the instruction. After approval, devices which match the specified coverage value will have their location to the specified value, and responses will report the old and new location.

Devices are reported as blank if they are not assigned to a location.

There is a corresponding instruction **Get the location of my devices**.

> **Note**
>
> The instructions **1E-Explorer-TachyonAgent-SetLocation** and **1E-Explorer-TachyonAgent-GetLocation** are available by uploading the Classic Product Pack **1E-Explorer-TachyonAgent**, which is included in the **Tachyon Platform** zip downloaded from the 1E Support Portal.
>
> For more information about this Product Pack and its instructions, please refer to Tachyon Platform - 1E Explorer TachyonAgent product pack.

4.4.9 Exporting data from Explorer

Results visible in Explorer can be exported to files containing comma-separated values (CSV) or, in the case of the **Export all** option on the instruction response page, tab-separated values (TSV), and results can be marked for export at the point of asking a question to automate the process.

4.4.9.1 Exporting the responses instruction list

To export the responses instruction list, an administrator would follow these steps:

The instruction list displayed on the **Responses** page can be exported to a **.csv** file.

Clicking on the Export button exports the current page of instructions to a file called **instructionsList.csv**.

You can check the contents of the file in a text application such as **Notepad**.

4.4.9.2 Exporting instruction responses

Exporting the values enables the responses to be acted upon outside of Tachyon via a script, batch file or 3rd party application.

The information contained in the responses to a particular instruction can be exported in various ways:

On a single page basis to a **.csv** file from the Explorer. Single-page exports are output in comma-separated format. This is to enable the limited amount of data to be easily viewed in a spreadsheet application. Because of the small amount of data held in these files single-page exports are downloaded via the website to the browser's download cache.

Exporting the drill-down information held for a single item in the responses page.

Exporting all the responses to a **.tsv** file once the instruction has completed. Exporting all the responses outputs to a tab-separated format file. This is to enable the potentially large amount of data to be easily processed by a 3rd party application. Because of the potentially large amount of data these files are output to a share location that must be selected by the user. Please refer to Configure Tachyon to support the Export all responses feature for more details.

To demonstrate these types of export we'll use the responses for the question
Which Windows services are disabled?

4.4.9.2.1 Exporting one page of the top-level responses

To export one page of the top-level responses, follow these steps:

To export the current page of responses click on the **Export** button in the row just above the table heading where the responses are displayed. The **Export** button is shown highlighted in the picture opposite, and the resulting file, called **aggregatedResults.csv**, is downloaded to the browser's download folder, as seen in the bottom-left of the chrome browser shown in the picture.

For top-level responses the output file is always called **aggregatedResults.csv**. If the file already exists in the downloads folder the browser will usually rename the downloaded file by appending consecutive numbers to the end.

When you open the **.csv** file you will see the exported responses from the current page. The picture shows the **aggregatedResults.csv** file opened using notepad.

An administrator could then use these responses to identify any disabled services that should be running.

4.4.9.2.2 Exporting drill-down responses

Let's suppose that an administrator is interested in investigating and taking action on the devices where the **Internet Connection Sharing (ICS)** service is disabled.

To export drill-down responses, follow these steps:

Clicking on that top-level response for that service displays all the devices that have responded to say that it is disabled. In our example this shows a number of devices where the service has been disable, as shown in the picture opposite.

We can now select to export the drilled-down responses in order to use that information outside of Tachyon. The picture opposite shows the result of clicking the **Export** button. In the case of drilled-down responses the exported file is called **detailedResults.csv**.

Now when we open the file in notepad we can see the names of the devices and the service that is disabled. This can then be passed on to another resource to process those devices to get the service turned on.

4.4.9.2.3 Export all results from the completed instruction

To export all results from the completed instruction, follow these steps:

When an instruction has completed, that is when it has finished retrieving answers from the Tachyon client devices, the **Export all results** button will appear on the responses page.

Clicking the **Export all results** button displays the **Export all results** popup. Here you need to enter the location of an appropriately permissioned share where the results will be exported. Please refer to Configure Tachyon to support the Export all responses feature for more details. In our example we have a share called Tachyon located on the same server as our Tachyon Web Server. The path to the share is **\\ACME-TCN01\TachyonResponses** in our example the share has previously been entered so the dialog recalls the name for us.

After the share has been designated click the **Save** button to begin the export.

Once the export has finished, a file named **Response_<timestamp>.tsv** will be created in the specified share.

In our example, opening the exported **.tsv** file in Notepad shows all the results related to the **Which Windows services are disabled?** instruction.

You'll notice that exporting in this way includes far more information than the export of the single page shown earlier and the type of data displayed is different.

The single-page export shown earlier contains the processed values, as displayed when viewing the responses page, whereas the **.tsv** contains all the raw unprocessed data sent back from the Tachyon client devices.

4.4.9.3 Exporting device information

The information on the **Devices Table** page can also be exported to a **.csv** file, as described in the following steps:

From the **Devices Table** page, clicking the **Export** button exports the current page of devices to a file called **Devices.csv**.

The contents of the **Devices.csv** can be displayed using **Notepad.exe**.

4.4.10 Investigating Devices

Investigating devices that have connected to Tachyon using the 1E Client.

4.4.10.1 Overview

You can use the **Devices** section to browse a predetermined set of information for all the devices that are known to Tachyon, that is the devices that are currently connected to Tachyon or have connected in the past. This is in addition to the ability to explore devices using instructions to get back a range of information that is only limited by the instructions you have available to you.

The **Devices** section can be viewed by users assigned to any role that has permissions on any instruction set. This includes custom roles and the following system roles:

All Instructions Actioner

Full Administrator

All Instructions Approver

All Instructions Questioner

Viewer

There are two options for directly investigating the devices known to Tachyon: The Devices Table and The Devices Dashboard.

4.4.10.2 The Devices Table

Explorer lets you view details for devices on your network, including real-time visibility of which devices are currently connected (online) and can therefore be interacted with directly.

Device details are stored in the TachyonMaster database and not in the inventory repositories. They are updated each time a client connects to a Switch.

Please refer to Introducing Inventory for details of inventory repositories.

> **Tip**
>
> 1E Explorer TachyonAgent product pack contains Instructions that help with device connectivity and configuration.

4.4.10.2.1 The Devices table

The picture shows the devices that have connected to our example Tachyon system. They are all shown as currently online.

Each time you view or change the page, the table is refreshed. You can also click the **Refresh** button while viewing the table.

4.4.10.2.1.1 The Devices table

Property	Description
Status	Indicates the status of the device: **online** - the device is connected to a Switch **offline** - the device does not have a network connection to a Switch. This may be because the device is powered down, disconnected from the network, the Tachyon client is not running or is incorrectly configured.
Device name	The Fully Qualified Domain Name (FQDN) of the device, as presented by the device to the Switch. If the FQDN of a device changes then it will be updated in the TachyonMaster database, it does not create a duplicate entry. Each device is uniquely identified by a GUID which is not visible in any screens. You can view additional properties for a device by clicking on the information icon next to the device name - see The Device View Overview tab.
Criticality	The criticality of the device as determined by your organization. Please refer to Using Device Criticality.
OS	The Operating System name.
OS version	The Operating System version.
Manufacturer	The manufacturer of the device as it appears in the device BIOS. The name is not normalized.
Agent version	The version of the Tachyonagent.
Primary User	The Primary User that the Tachyon agent has determined is most clearly related to the device.
Last seen	The date and time when the device last reported a Keep Alive to the Switch, which is at least every 15 minutes by default, as defined in 1E Client - #UUID4b0c8700283e161c086960470cc47bc0_id_TachyonclientsettingsConnectionKeepaliveTimeInSecondsMax.

4.4.10.2.1.2 Sorting the table

Click on the **Sort by** button and select one of the following properties, to sort the Devices table.

Property	Description
Device name	Sorts on the device name in A-Z or Z-A order.
OS	Sorts on the OS name in A-Z or Z-A order.
Agent version	Sorts by the version number of the Tachyon client in ascending or descending order.
OS version	Sorts on the OS version number in ascending or descending order.
Criticality	Sorts on the device Criticality, ascending or descending according to the following order: Criticality Undefined Non-critical Low Medium High Critical

4.4.10.2.1.3 Filtering the table

You can filter rows of the table using the following properties. A button turns blue if it is being used. You can click on the **Reset** button to delete all the filters.

Property	Description
OS	A drop-down list let's you filter on one of the following:

Property	Description
	OS --- All Windows Linux Mac Android Solaris
Agent version	This drop-down lets you filter on the version number of the Tachyon client using a numeric condition, as described under the heading Numeric conditions.
OS version	This drop-down lets you filter on the OS version number using a numeric condition, as described under the heading Numeric conditions.
Device type	This drop-down lets you filter on one of the following device types: Device type --- All Desktop Laptops Servers Mobiles
Status	This drop-down lets you filter according to whether the device is currently Online or Offline.
Criticality	This drop-down lets you filter according to the Criticality set for the device. For more detail about this feature, please refer to Using Device Criticality.

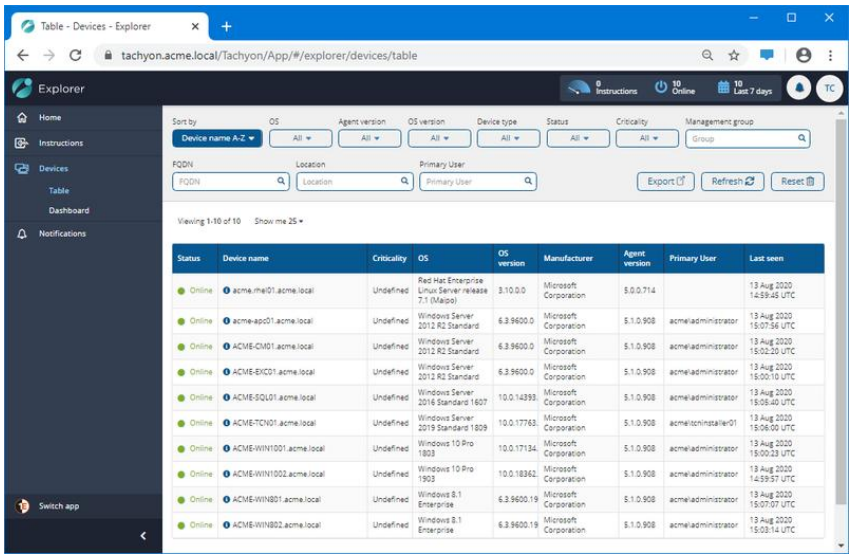
Property	Description
	Criticality Undefined Non-critical Low Medium High Critical
Management group	This entry field lets you filter according to a Management group that devices belong to. A list of Management groups is displayed when you click in the entry field, or you can type a name to filter the list as you type.
FQDN	This entry field lets you enter all or part of the Fully Qualified Domain Name for devices, and dynamically refreshes the table as you type.
Location	This entry field lets you filter on the location set for the devices, and dynamically refreshes the table as you type.
Primary User	This entry field lets you filter on the Primary User that the 1E Client has determined is most clearly related to the device, and dynamically refreshes the table as you type.

4.4.10.2.1.4 Numeric conditions

Condition	Description
Equals	Checks if the property is equal to the value you supply.
Greater	Checks if the property is greater than the value you supply.
Less	Checks if the property is less than the value you supply.
Range	Checks if the property lies between the upper and lower bounds you supply.

4.4.10.2.1.5 Exporting the table

You can export the devices data to a .csv file, as described in Exporting data from Explorer.



4.4.10.2.2 The Device View Overview tab

Clicking on the information icon next to the device name in the **Device Name** column of the **Devices Table** page displays the Device view for the selected device. The aim of the Device view is to provide a combined overview of all the information known about a device, along with the ability to retrieve information about the device in real-time. When displaying the Device view from the Explorer Devices Table page, the view defaults to the **Overview** tab. This tab contains the following panels.

4.4.10.2.2.1 The Details panel

This panel displays the basic details for the device. This is contained in a number of tiles, as described in the following table.

> **Note**
>
> If you upgrade macOS to a new major version (For example, 11 to 12) then the O/S install date will change. However, if the upgrade is a minor version, such as 12.2 to 12.3 then the install date remains the same as the original major upgrade.

Tile	Description	
Identification	Field	Description
	FQDN	The FQDN for the device.
	Name	The server name for the device.

Tile	Description
	Domain The device's domain. **Criticality** The Tachyon set criticality value for the device. **Serial Number** The device serial number. **1E Client** The version of the 1E Client installed on the device. **Tachyon GUID** The GUID used by Tachyon to uniquely identify the device.

Field	Description
Timezone	The timezone the device is operating in.
Offset	The offset from UTC for the timezone the device is operating in.
Location	The device location, if any has been set.
Locale	The language locale set for the device.

This table provides information on how the device has been tagged and grouped from a Tachyonperspective.

Field	Description
Tags	Indicates all Tachyon tags that have been set for the device.
Coverage Tags	Indicates Tachyon tags that have been set for the device that can be used to determine coverage for an instruction.
Mgmt. Groups	Indicates the Management Groups the device belongs to.

Hardware and Operating System

This table provides information on the device's hardware.

Tile	Description

Field	Description
Virtual/Physical	Indicates whether the device is virtual or physical. For virtual devices it indicates the type of virtualization. For example **Hyper-V**.
Manufacturer	Shows the hardware or virtual device manufacturer. For example **Microsoft Corporation** for Hyper-V virtual devices.
Model	The model of the hardware or virtual device. For example **Virtual Machine** for Hyper-V virtual devices.
Device Type	The type of device, whether it's a server, desktop or mobile device. For example for Windows 10 virtual devices this would be **Desktop**.
Chassis Type	The type of device, whether it's a server, desktop or mobile device. For example for Windows 10 virtual devices this would be **Desktop**.
RAM	The amount of RAM in MB.
CPU Type	The CPU Type for the device. For example, **Intel(R) Xeon(R) CPU E5620 @ 2.40GHz**.
CPU Architecture	The architecture for the CPU. For example, **x64**.
SMBIOS GUID	The GUID for the device. For example, **2e4533e6-ea92-4292-8b9c-ebae17edee75**.

This table provides information on the device's Operating System.

Field	Description
Type	Indicates the main type of the OS. For example, **Windows** or **Mac**.

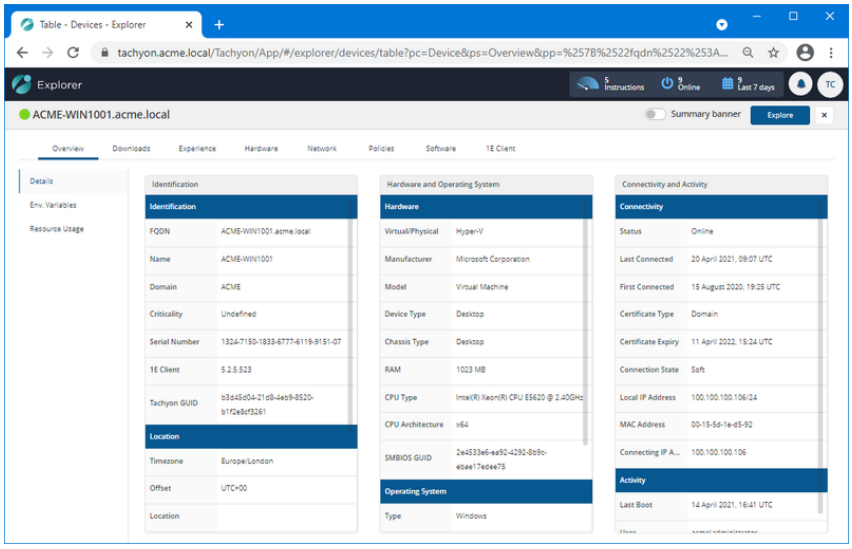
Tile	Description	
	Version	Shows the colloquial version for the OS. For example, **Windows 10 Pro 20H2**.
	Version Number	The version for the Operating System. For example: **10.0.19042.928**.
	Architecture	The architecture of the OS. For example, for 64-bit Windows systems, this would be **x64**.
	Installation	The UTC date and time the operating system was installed or updated.
Connectivity and Activity	This table provides information on the device's current connection status with Tachyon.	

Field	Description
Status	Whether the device is connected to Tachyon or not. This could be **Online** or **Offline**.
Last Connected	Shows the UTC date and time the device last connected to Tachyon.
First Connected	Shows the UTC date and time the device first connected to Tachyon.
Certificate Type	The type of certificate the device is using to connect to Tachyon.
Certificate Expiry	The UTC date and time the device certificate will expire.
Connection State	How the device connects to the Switch.
Local IP Address	The local IP address for the connecting device.
MAC Address	The MAC address for the client device interface used to connect to the Switch.

Tile	Description
	Connecting IP Address — The IP address for the connecting device.

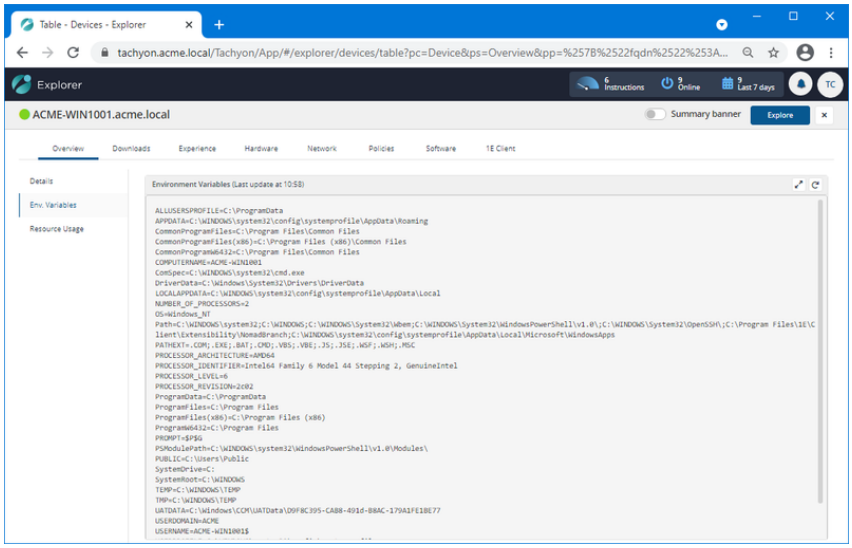
This table provides information on the device's current activity status.

Field	Description
Last Boot	The UTC time and date the device was last booted.
User	The username for the user most associated with the device.



4.4.10.2.2.2 The Env. Variables panel

Displays the list of environment variables set on the device. This information is updated each time the page is refreshed.



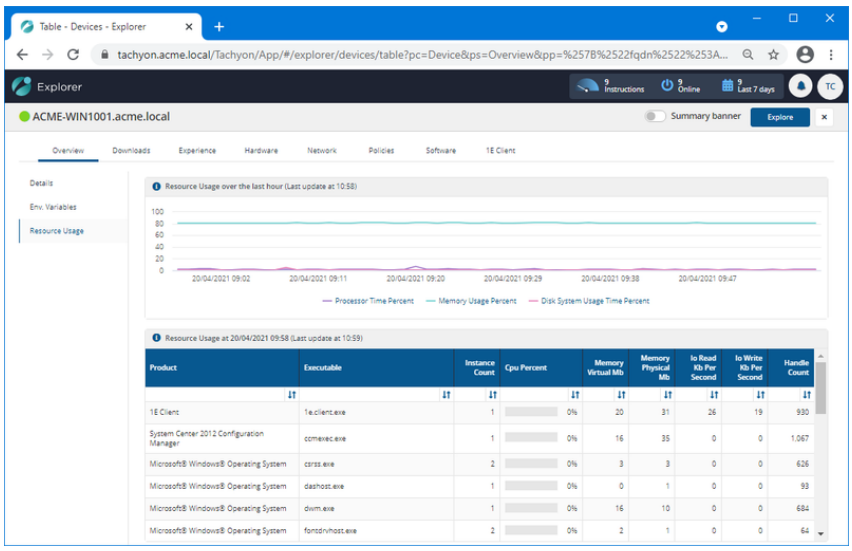
4.4.10.2.2.3 The Resource Usage panel

This panel displays the recent resource usage for the device.

Tile	Description
Resource Usage over the last hour (Last update time)	This tile displays a line graph showing the percentage of resource usage over time during the last hour. Selecting a point on the graph selects the data displayed in the **Resource Usage at date and time** tile. This can be useful if there is an outlying data point where you want to investigate the breakdown according to the products on the device. The three lines displayed show the **Processor Time Percent**, the **Memory Usage Percent** and the **Disk System Usage Time Percent**. You can toggle the display of these lines by clicking on the legend name at the bottom of the graph.
Resource Usage at date and time	This tile displays the product resource usage. Click on a point on the **Resource Usage over the last hour** tile to show the product resource usage at that particular time. The table shows the following data:

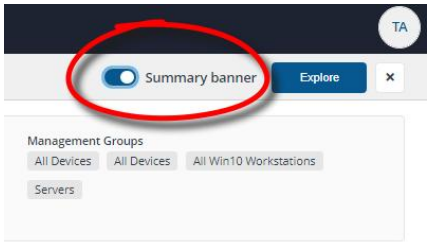
Column	Description
Product	Software product name.
Executable	Executable name.

Tile	Description	
	Instance Count	The number of instances of the product that are running.
	Cpu Percent	The percentage of CPU used by the product.
	Memory Virtual Mb	The virtual memory consumed by the product in MB.
	Memory Physical Mb	The physical memory consumed by the product in MB.
	Io Read Kb Per Second	The disk I/O read rate per second.
	Io Write Kb Per Second	The disk I/O write rate per second.
	Handle Count	The number of resource handles open for the product.



4.4.10.2.3 The Device View Summary banner

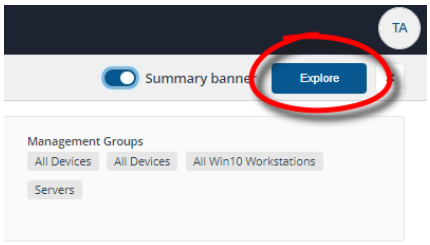
The Summary banner displays a quick summary of the information provided in the various tabs displayed in the Device View. It can be viewed by toggling the **Summary banner** switch to on.



The following image shows the Summary banner displayed for a particular device.

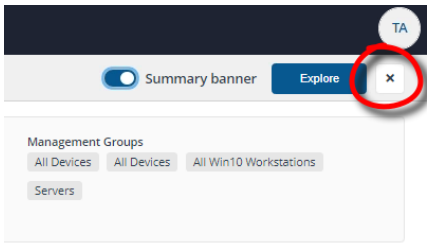
4.4.10.2.4 Launching the Explorer from the Device View

You can click on the **Explore** button in the Device View to launch Explorer with the current device set as the scope.



4.4.10.2.5 Closing the Device View

The Device View is a popup that is displayed when clicking on the name of a device on a page where devices are displayed. To return to the page you came from you need to click the x button.



4.4.10.2.6 Additional Device View tabs

In addition to the **Overview** tab, there are a number of other tabs, each corresponding to an app, feature or data set implemented in Introducing Tachyon:

The **Overview** and **1E Client** tabs are always present in the **Device View**. Other tabs are visible if an app has been installed and is licensed.

Each tab has one or more panels with tiles populated with data from various sources, some by instructions that are run instantly, with results cached for 3 minutes. An appropriate error message is displayed instead of a tile in the following circumstances:

If the device is offline, as indicated by the color of the icon in the top left

The user does not have at least Viewer permission to view use the license the tab or panel

The user does not have questioner permission to run the instruction

An instruction has not been uploaded.

The Device View tabs and panels page lists the names of tabs and their panels, and a description of each tile indicating how the tile is populated.

4.4.10.2.6.1 The Device View tabs and panels

<table>
<tr><th>Tab</th><th>Panel</th><th>Description</th><th>Data source</th></tr>
<tr><td>Overview</td><td>Details</td><td>Displays a number of tiles sorted into Identification, Hardware and Operating System and Connectivity and Activity columns that show information for the selected device retrieved from the online status information stored in the TachyonMaster database.

The columns and tiles are shown in the following table:

<table>
<tr><th>Column</th><th>Tile</th><th>Description</th></tr>
<tr><td>Identification</td><td>Identification</td><td>Display's the current device:

FQDN

Name

Domain

Criticality</td></tr>
</table>
</td><td>Data from TachyonMaster (the latest online status message)</td></tr>
</table>

Tab	Panel	Description		Data source
			Serial Number 1E Client Tachyon GUID.	
		Location	Displays the device's: Timezone Offset Location Locale.	
		Grouping	Displays the device: Tags - freeform tags applied to the	

Tab	Panel	Description		Data source
			device Coverage Tags - any coverage tags applied to the device Mgmt. Groups - lists the management groups the device is a member of.	
		Hardware and Operating System	Hardware	Shows hardware details for the device:

Tab	Panel	Description			Data source
				Virtual /Phyiscal	
				Manufacturer	
				Model	
				Device Type	
				Chassis Type	
				RAM	
				CPU Type	
				CPU Architecture	
				SMBIOS GUID.	
		Operating System	Shows operating system, type and version for example:		
				Type	

Tab	Panel	Description			Data source
				Version	
				Version Number	
				Architecture	
				Installation.	
		Connectivity and Activity	Connectivity	Shows current device connectivity status:	
				Status	
				Last Connected	
				First Connected	
				Certificate Type	
				Certificate Expiry	

Tab	Panel	Description			Data source
				Connection State Local IP Address MAC Address Connecting IP.	
			Activity	Shows Last Boot date and time and current user.	
Env. Variables	Shows a list of the environment variables set on the device.				
Resource Usage	Two panels: **Resource Usage over the last hour** - shows system disk, CPU and memory usage per minute for the last one hour **Resource Usage at** *day/month/year time* - shows executable resource usage for a specific minute:				1E-TachyonPlatform-Hardware-ResourceUsage 1E-TachyonPlatform-Hardware-ResourceUsageByMinute

Tab	Panel		Description	Data source
	Column	Description		
	Product	Resource name, for example 1E Client		
	Executable	Resource executable, for example 1e.client.exe		
	Instance Count	Number of currently running instances.		
	Cpu Percent	Percentage of CPU currently being consumed.		
	Memory Virtual Mb	Virtual memory consumed in Mb.		
	Memory Physical Mb	Physical memory consumed in Mb.		
	Io Read Kb Per Second	Number of associated read input/output operations per second.		
	Io Write Kb Per Second	Number of associated write input/output operations per second.		
	Handle Count	The number of object handles.		
Downloads	**Summary**		Download activity and status for the device. Whenever you click on an FQDN on any of the Nomad pages then the **Device View** will be displayed with the **Downloads** tab selected.	Data from Nomad.

Tab	Panel	Description	Data source
Content	Content Titles on the selected device, the default view is from **All Sources**, **All Types** and **All Status**. **Note** You may see a difference in the number of items in a device's Nomad cache versus that displayed in the Nomad app Device View. This is because if downloaded content has been deleted from Configuration Manager, the content titles cannot be resolved in the Nomad app and are not displayed. This is under consideration for re-design and may be revised in future versions of Nomad.	Data from Nomad.	
Nomad Configuration	**1E Nomad Branch Settings .**	1E-Nomad-NomadBranchSettings	
Experience	**Metrics**	Metrics are the data points that are collected by the 1E Client and sent to the Tachyon server. They are collected at different intervals depending on the type of data that is being collected.	Data from Experience metrics
Trends	The Trends tab shows the changes in the scores over time. Hovering over any of the bars shows the details for that time and event. If the user viewing the device details also has the ability to at least ask a question in Explorer the Explore button will be visible.	Data from Experience metrics	

<table>
<tr><th>Tab</th><th>Panel</th><th>Description</th><th>Data source</th></tr>
<tr><td>Logs</td><td>The Event Logs tab gives you a listing of the Windows Event log entries for that device. This brings that data to this view and is very useful when determining the root cause of an issue that has been reported on the device.</td><td>Data from Experience metrics</td><td></td></tr>
<tr><td>Application Interactions</td><td>Shows user interaction times and ratios across applications measured over the last 30 days</td><td>1E-Experience-ApplicationInteraction</td><td></td></tr>
<tr><td>User interactions</td><td>Shows user interactive sessions with activity over last 30 days.</td><td>1E-Experience-UserInteractionHistory</td><td></td></tr>
<tr><td>Hardware</td><td>Disk drives</td><td>Shows disk drives, including hardware and usage information.<table><tr><th>Column</th><th>Description</th></tr><tr><td>Drive</td><td>Drive letter.</td></tr><tr><td>Volume Name</td><td>Volume name, if set.</td></tr><tr><td>Drive Type</td><td>Drive type, for example:
Removable Disk
Local Disk</td></tr></table></td><td>1E-Tachyon Platform-Hardware-DiskDrives</td></tr>
</table>

Tab	Panel	Description		Data source
			Compact Disk.	
		Size Gb	Total disk size in Gb.	
		Free Space Gb	Current free space in Gb.	
		Usage Percent	Percentage used of total drive space.	
		File System	File system, for example NTFS.	
		Manufacturer	Standard or SSD drive.	
		Model	Drive manufacturer.	
		Serial Number	Unique disk serial number.	
		Partition	Drive and partition of the specific drive.	

<table>
<tr><th>Tab</th><th>Panel</th><th>Description</th><th>Data source</th></tr>
<tr><td></td><td></td><td>Firmware Revision</td><td>Drive firmware version.</td><td></td></tr>
<tr><td></td><td></td><td>Device ID</td><td>Device ID of the specified disk.</td><td></td></tr>
<tr><td>Peripherals</td><td>Shows the list of plug and play hardware devices (Windows only).

Column | Description

Device Type | Hardware device, including for example things like:
Battery
Monitor
Keyboard
Mouse
Ports
SoftwareDevice.

Name | Device name.

Instance Count | Number of instances of a peripheral device.

Service | Associated Windows service, for example atapi, serial, PCI, ACPI.</td><td colspan="2">1E-TachyonPlatform-Hardware-Devices</td></tr>
<tr><td>Network</td><td>Throughput</td><td colspan="2">Shows network throughput on all adapters for the last</td><td>1E-Tachyon Platform - Network -</td></tr>
</table>

Tab	Panel	Description	Data source
		hour, represented by the following tiles: **Average throughput** - including Timestamp, Bytes Received per Second, Bytes Sent Per Second **Bytes received per second** **Bytes sent per second**.	Average Throughput
Interface configuration	Returns the output from the native network interface configuration command (e.g. ipconfig or ifconfig).	1E-TachyonPlatform-Network-InterfaceConfiguration	
DNS	Shows the **Cache** and **Host file** tiles: **DNS Cache Contents** - with the entries from local DNS cache, **Host Name** and **Address**. **HOSTS file** - shows the content of the drivers/etc/hosts file.	1E-TachyonPlatform-Network-DnsCache 1E-TachyonPlatform-Network-HostFileContent	
TCP connections	Returns a list of established TCP connections.	1E-TachyonPlatform-Network-TcpConnections	

Column	Description
Process Name	Local process name.
Process Id	Uniquely identifies an active process.
Class	Class of Internet networking protocol.

Tab	Panel		Description	Data source
	Local Address	Local network address.		
	Local Port	Network port used by a specific process.		
	Remote Address	Source IP address from which the traffic came from.		
	Remote Port	Remote port used by a specific process.		
	Latency Ms	The time taken in milliseconds for data or a request to go from a source to a destination.		
Listening ports	Returns a list of processes which are listening for network connections.			1E-TachyonPlatform-Network-ListeningPorts
	Column	Description		
	Process Name	Local process name.		
	Process Id	Uniquely identifies an active process.		
	Class	Class of Internet networking protocol.		
	Local Address	Local network address.		
	Local Port	Network port used by a specific process.		
	Product	Related product, for example host process for Windows Services,		

Tab	Panel	Description	Data source
	Local Security Authority Process, SCNotification.		
ARP Cache	Returns a list of processes which are listening for network connections and also shows routing tables.	1E-TachyonPlatform-Network-ArpCache 1E-TachyonPlatform-Network-RoutingTable	
WIFI	Shows a list of visible wifi networks, including basic network properties.	1E-TachyonPlatform-Network-WiFiNetworks	

Column	Description
SSID	WiFi network name.
Is Connected	Shows as either true or false, dependent on whether the corresponding adapter is connected to the network.
Is Hidden	Shows as true if the WiFi network is not broadcasting a public SSID.
Is Secure	Shows as either true or false: true - if the WiFi network is secure false - if the network is open.
Signal	Shows WiFi signal quality; from 0 (worst) to 100 (best).
Authentication	The default authentication mechanism supported by the network.
BSSI IDs	The Service Set Identifier (SSID) of the network, it will

Tab	Panel		Description		Data source
		be empty if the network is hidden.			
	Encryption	Shows the default encryption mechanism supported by the network.			
	Adapter	Shows the WiFi network adapter name to which this network is visible.			
Policies	**Rules Compliance**		Column	Description	Data from Guaranteed State
			Rule Name	Name of rules applied to the current device. The viewable list relates to the selected Tachyon policy from the policy dropdown on the page.	
			State	If the device state is Compliant, Noncompliant or Not Applicable.	
			Type	Rule type:	

Tab	Panel	Description		Data source
			Check - allows you to verify that a device has a particular state, such as a registry key having a specific value Fix - allows you to define a desired state for the device and then enforce that state.	
		Effectiveness	Policy rule effectiveness is the usefulness of policy rules and is represented as either: Disabled - the rule has not yet been enabled from the Guaranteed State Rule	

Tab	Panel	Description	Data source
		Administration page, so it is not currently active Unassigned - the rule is enabled, but has not been deployed to any devices Ineffective - the rule has been deployed, but no devices have changed their compliance position for this rule in the last thirty days Effective - the rule has been deployed and at least one device has changed its compliance position	

Tab	Panel	Description		Data source
			for this rule in the last thirty days.	
			History Rule history.	
Software	**Installations**	Shows (per-device) installed software.		1E-Tachyon Platform - Software-Installations
		Column	Description	
		Product	Software product name.	
		Publisher	Software publisher.	
		Version	Product version number.	
		Architecture	Instruction set architecture (ISA) version.	
		Install Date	Software installation date.	
Windows services	Shows list of installed Windows services and their current state.	1E-TachyonPlatform-Software-Services		

Tab	Panel	Description	Data source

Column	Description
Name	Windows service name.
State	Windows service state, Running or Stopped.
Startup Type	Windows service startup type, for example Automatic, Automatic (Delayed Start), Manual, Disabled.
Process Id	Uniquely identifies an active process.
Description	Windows service description.
Logon Account	Windows service logon account context.
Type	Windows services type, for example file system driver, kernel driver, shared process.

Tab	Panel	Description	Data source
Env. Variables	Shows operating system environment variables.		1E-TachyonPlatform-Software-EnvironmentVariables
Processes	Shows detailed information about all running processes.		1E-TachyonPlatform-Software-Processes

Column	Description
Product	Software product name.
Executable	Executable name.

Tab	Panel	Description	Data source
	Version	Product version number.	
	Devices count	How many devices are reporting.	
	Crashes	Number of times this software crashed during the last 24-hour reporting period.	
	Hangs	Number of times this software crashed during the last 24-hour reporting period. **Note** Software crash and hang information is obtained from Windows event data. For background information on Windows events and the event viewer refer to https://support.microsoft.com/en-gb/help/302542/how-to-diagnose-system-problems-with-event-viewer-in-microsoft-windows	
	Performance anomalies	Number of performance anomalies detected in this software during the last 24-hour reporting period.	
	I/O write KB/s	Average disk I/O read rate per second during the last 24-hour reporting period.	

Tab	Panel	Description	Data source
	I/O write KB/s	Average disk I/O write rate per second during the last 24-hour reporting period. **Note** For background information on analyzing disk storage performance refer to https://docs.microsoft.com/en-gb/archive/blogs/cotw/analyzing-storage-performance	
	Virtual Memory Usage KB	Average Virtual Memory Usage KB during the last 24-hour reporting period. **Note** For an explanation of Windows Virtual Memory organization refer to https://answers.microsoft.com/en-us/windows/forum/windows_10-performance/physical-and-virtual-memory-in-windows-10/e36fb5bc-9ac8-49af-951c-e7d39b979938 and https://support.microsoft.com/en-us/help/2160852/ram-virtual-memory-pagefile-and-memory-management-in-windows	
	Processor Time Seconds	Each instance of the executable will burn processor time. This column gives the average of the total time consumed by each process instance per second. Each instance uses the sum of all time used by each core in parallel.	

Tab	Panel	Description	Data source
		Therefore, it is possible to see more seconds here than in a day (usually 60 x 60 x 24 = 86400) for the whole column, if your system is working extremely hard 24x7. The theoretical maximum would be somewhere near ***number of cores*** x ***seconds per day*** . Hence, 'Processor Time' rather than 'Human Time'	
	Processor Time %	This is an easier notion than Processor Time Seconds. This is the average of the processor consumption of each instance. Each instance of this process will have caused different percentages of compute resource in all the processors and cores to be used over time (unless they have specifically requested certain core affinity). For each minute each process is running, a profile of the usage is built for the whole day. This value is the average of all of those samples. There is no way to work out, for any one of the process instances involved, how long any particular instance was running for. This could indicate a process that is going wild with resources, but it would take more investigation on the device to discover for how long this is happening. It is perfectly possible to see all the values in this column adding up to more than 100% as the processes were not necessarily running at the same time. **Note**	

Tab	Panel	Description	Data source
		For further information on Processor time refer to https://social.technet.microsoft.com/wiki/contents/articles/12984.understanding-processor-processor-time-and-process-processor-time.aspx	
	Responsiveness Impact %	An indicator of how reactive a process is to activity by other processes on the device. Typically, anti-virus products watch and respond to potentially suspicious activity such as increased network traffic. Anti-virus products will differ in their impact on the overall performance of a device. **Note** Responsiveness Impact % is used to indicate how sensitive a process appears to be to the use of system resources by other processes on a device. For example, Security Protection software present on a device may reveal a spike in its activity whenever a new process is started on that device. This would typically be because the Security Protection software may wish to ensure that the new process starting on the device is present in a security white list. Other software may also react to activity by other processes and by reacting they impact system resource uses,	

Tab	Panel	Description	Data source
		thereby adversely affecting the user's experience. So it is useful to be able to identify software with the highest Responsiveness Impact on a device and potentially investigate further. **Note** Responsiveness Impact % represents the proportion of the increased CPU activity detected by the 1E Client as a result of performing a set of operating system-level operations that can be attributed to a given running process. Examples of these would be Windows registry and resource creation operations. It is reported as a percentage to normalize results across devices that offer a range of computing power. For example, if *software.exe* on a device is attributed a Responsiveness Impact of 53% this means that more than half of the spike in CPU usage caused by software monitoring activity on that device can be attributed to *software.*	

Tab	Panel	Description	Data source
	Handle Count	Average number of Windows handles used by this software during the last 24-hour reporting period. **Note** For further information on Windows handles refer to https://docs.microsoft.com/en-us/windows/win32/sysinfo/handles-and-objects For tips on examining open handles for any Windows process refer to https://docs.microsoft.com/en-us/sysinternals/downloads/handle and https://techcommunity.microsoft.com/t5/windows-blog-archive/pushing-the-limits-of-windows-handles/ba-p/723848	
	Physical Memory Usage KB	Average Physical Memory Usage KB during the last 24-hour reporting period. **Note** Please refer to https://docs.microsoft.com/en-us/sysinternals/downloads/rammap for a useful tool to examine physical memory allocation on a device.	
1E Client	**Binaries**	Shows a list of the binary files in the executable folder of the 1E Client.	1E-Tachyon Platform-Client-Binaries

Tab	Panel	Description		Data source
		Column	Description	
		File Name	Associated 1E Client file name.	
		File Version	Software version.	
		File Size	File size in bytes.	
		Description	File description	
		Date Created	The date the file was written to disk.	
		Date Modified	The date the file was last saved.	
Configuration file	Shows the full content of the 1E Client configuration file, including: Logging settings Communication settings Agent settings Module settings.			1E-TachyonPlatform-Client-ConfigFileContent

Tab	Panel	Description	Data source
Extensibility	Shows extensibility objects (modules and providers) loaded by the 1E Client. Column: Description **Type**: Module or Provider component. **Binary Name**: Associated 1E Client binary name, for example 1E.Client.Module.Interaction.dll **Name**: Name, for example Interaction. **Version**: 1E Client version, for example 5.2.5.251	1E-TachyonPlatform-Client-Extensibility	
Local Storage	Shows **Data Files** and **Client Inventory Database Use** tiles that display the list of: Data files (logs, databases, etc) created by the 1E Client Tables in the1E Client Inventory database, along with a row count per table.	1E-TachyonPlatform-Client-DataFiles 1E-TachyonPlatform-Client-InventoryDatabaseUse	

4.4.10.3 The Devices Dashboard

Explorer lets you view details for devices on your network including real-time visibility of which devices are currently connected (online) and can therefore be interacted with directly.

Device details are stored in the TachyonMaster database and not in the inventory repositories. They are updated each time a client connects to a Switch.

Please refer to Introducing Inventory for details of inventory repositories.

> **Tip**
>
> 1E Explorer TachyonAgent product pack contains Instructions that help with device connectivity and configuration.

4.4.10.3.1 The Devices dashboard

The devices dashboard provides a view of the devices that have contacted Tachyon.

There are two panes in the dashboard:

The left-hand pane displays a list of filters that appear as charts

The right-hand pane displays a list of devices that correspond to the currently selected filter, you can click on a row in the table to see the Device View for the device.

For more information on using the Devices dashboard please see Using the Devices dashboard - Tutorial.

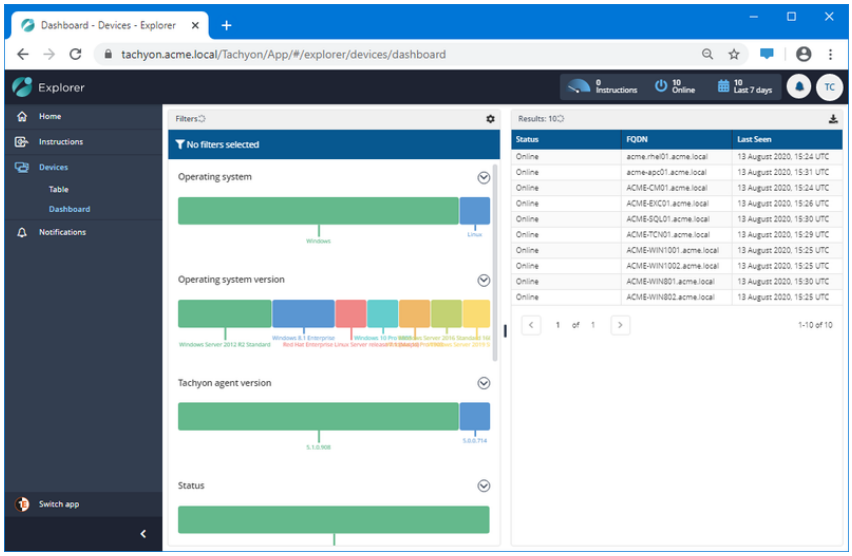
The available filters are:

Filter	Description
Operating system	Partitions the 1E Client devices according to the OS running on the devices.
Operating system version	Partitions the 1E Client devices according to the OS version running on the devices.
Tachyon agent version	Partitions the 1E Client devices according to the version of the 1E Client running on the devices.
Status	Partitions the 1E Client devices according to the current connection status of the devices.
Device type	Partitions the 1E Client devices according to the type of the devices.
Timezone	Partitions the 1E Client devices according to the time zone the devices are configured with.
Location	Partitions the 1E Client devices according to their location.

The available charts are:

Chart	Description
SmartBar	Displays a single horizontal bar where the distinct values in the data are represented by different colors. The individual colored blocks can be clicked on to select the corresponding devices that have that value.
Pie	Displays a pie chart where the distinct values in the data are represented by different colors. The wedges can be clicked on to select the corresponding devices that have that value.

Chart	Description
Column	Displays a column for each distinct value in the data. Each column can be clicked on to select the corresponding devices that have that value.
Bar	Displays a horizontal bar for each distinct value in the data. Each bar can be clicked on to select the corresponding devices that have that value.



4.4.10.3.2 Using the Devices dashboard - Tutorial

A quick tutorial on using the Devices dashboard to filter and highlight specific devices.

4.4.10.3.2.1 The example

To illustrate the process of selecting a specific device in Tachyon we use an example of locating Windows servers.

4.4.10.3.2.1.1 Setting filters

Our example shows the following steps:

In our example the **Devices Dashboard** page is already selected showing all **12** of our connected devices.

Click on the **Operating system type** bar with the **Windows** label. A new **OsType=Windows** filter appears in the top row and the **Results** then show only the **11** Windows server type devices.

Click on the **Device type** bar with the **Server** label. A new **DeviceType=Server** filter is added. This filters the **Results** table to show only the **5** Windows server type devices.

4.4.10.3.2.1.2 Removing filters

You can remove any of the filters that have been set by clicking on **x** button at the right-hand end of the filter displayed just beneath the **Filters** header. You can identify the set filters by their thicker border.

The animation at the top of the page shows the following steps:

Click on the **x** at the right-hand end of the **OsType=Windows** filter. This filters the **Results** table to now show **6** Server devices.

To remove the next filter, click on the **x** at the right-hand end of the **DeviceType=Server** filter. The **Devices Dashboard** now shows the default unfiltered **12** devices.

4.4.11 Tachyon Activity Record

A description of the benefits of Tachyon Activity Record feature and how the data can be retrieved.

Also known as Tachyon Inventory.

4.4.11.1 What is Tachyon Activity Record?

Tachyon clients capture certain types of event data in a local database (Persistent Storage) so that instructions can query later. Data is compressed and encrypted in a way that ensures a very low impact on device performance and security.

Tachyon Activity Record is similar to Windows Task Manager and Perfmon. On Windows client devices Tachyon continuously captures events, which enables all significant events to be captured as they happen. Other OS use polling, which requires the polling frequency to be regular enough to ensure brief events to be captured.

The type of data captured and is described below and the configuration options for each capture source are described in 1E Client - Tachyon client settings: Inventory module settings. There are Product Pack instructions for getting and setting these configuration options.

4.4.11.1.1 What are the capture sources?

The table below lists the capture sources supported by the Tachyon Activity Record feature, and on which OS they are supported.

Source Name	Description	Windows	macOS	Linux	Solaris
ARP	ARP cache entries - the Inventory module captures the results of cached IP address to physical address resolutions	3.2	n/a	n/a	n/a
BootPerformance	Windows boot performance metrics.	8.0	n/a	n/a	n/a
DeviceInteraction	User session input metrics (keyboard and mouse activity).	5.1	n/a	n/a	n/a
DevicePerformance	Device performance metrics for device performance by interrogating Windows Performance Counters.	5.0	n/a	n/a	n/a

Source Name	Description	Windows	macOS	Linux	Solaris
	These metrics cover disk, memory, network and processor performance. This capture source is required by the **Experience** application.				
DeviceResourceDemand	Disk, network, memory, and processor performance metrics.	5.1	n/a	n/a	n/a
DNS	DNS resolution queries - the Inventory module captures whenever a DNS address is resolved	2.1	2.1	n/a	n/a
OperatingSystemPerformance	Performance metrics for OS - the metrics executable runs every 4 hours by default This capture source is required by the **Experience** application.	5.0	n/a	n/a	n/a
PerformanceEvent	Distinct events which may be of relevance when diagnosing performance or end-user experience issues.	5.0	n/a	n/a	n/a
Process	Process execution - the Inventory module captures whenever a process starts on the device	2.1	2.1	2.1	2.1
ProcessStabilization	The time taken for a process execution to be considered stable whenever a monitored process starts on the device	3.2	n/a	n/a	n/a
ProcessUsage	A daily summary of the launches and terminations of processes. The Process Usage capture source is required by the	3.2	n/a	n/a	n/a

Source Name	Description	Windows	macOS	Linux	Solaris
	Tachyon Powered Inventory feature (Tachyon connector). **Note** Process Usage capture can generate high disk I/O while capturing process usage on virtual machine hosts with guests starting at the same time.				
SensitiveProcess	Performance metrics for sensitive processes - the metrics executable runs every 4 hours by default This capture source is required by the **Experience** application.	5.0	n/a	n/a	n/a
Software	Software installs/uninstalls/presence - the Inventory module captures whenever software is installed/uninstalled, and also captures which software is present on a device	2.1	2.1	2.1	2.1
SoftwareInteraction	Software process responsiveness and duration of active interaction.	5.1	n/a	n/a	n/a
SoftwarePerformance	Performance metrics for software - Software performance polling is every 10 seconds by default This capture source is required by the **Experience** application. Aggregated with SoftwarePerformance data: SoftwarePerformance.DiskUsage - Disk related metrics for each running process	5.0	n/a	n/a	n/a

Source Name	Description	Windows	macOS	Linux	Solaris
	SoftwarePerformance.ProcessNetworkUsage - Network related metrics for each running process.				
TCP	Outbound TCP connections - the Inventory module captures whenever an outbound TCP connection is made	2.1	2.1	2.1	n/a
UserUsage	A daily summary of all the logons and logoffs of users. This capture source is required by the **Tachyon Powered Inventory** feature (Tachyon connector).	3.2	n/a	n/a	n/a

4.4.11.1.2 How is the data managed?

The data is captured and stored to a local, encrypted persistent store and then periodically aggregated according to an ongoing daily, weekly, monthly window. This means that the data is held securely and the amount of data is minimized while still maintaining its usefulness.

4.4.11.1.3 How do I retrieve the data from the 1E Client devices?

Tachyon provides a number of Product Pack instructions that will let you interrogate your 1E Client devices for the data they hold.

4.4.12 Tachyon Quarantine

A description of the quarantine feature provided in the client and implemented in the quarantine instructions present in the 1E-Explorer-TachyonCore.zip file.

4.4.12.1 What is Quarantine?

On Windows, the Tachyon client is able to prevent communications to or from a target device. This is intended to be reserved for security breaches and other rare circumstances.

4.4.12.1.1 What will it do?

Quarantine will prevent all communications except those to the Tachyon server(s). This allows a Tachyon administrator to investigate and remove possible malicious software on the device.

Warning

Devices that have been quarantined will only be able to contact Tachyon. CRL checks must be set to soft. Certificate expiry can cause the client to fail to connect to the switch. If a client is no longer connected to Tachyon after quarantine, it will remain in quarantine. Please use with care, and please read this documentation carefully before use.

If the Tachyon Server has 1E Client installed (with Tachyon client features enabled) then it is possible to quarantine Tachyon Server like any other device. Therefore, please exercise caution before using this feature, and avoid targeting the server.

4.4.12.1.2 How do I quarantine a device?

Before you can use the Quarantine feature, you must upload the **1E-Explorer-TachyonCore.zip** Product Pack. This pack contains many instructions, amongst which are the Quarantine instructions described in the table below.

Instruction	Description
Are my devices quarantined? Warning: Please read the description before use.	This question returns a list of devices.
Quarantine selected devices. Warning: Please read the description before use.	This action quarantines all the devices in the scope of the action. Do not run this action without restricting the coverage to the devices you want to quarantine.
Release selected devices from quarantine. Warning: Please read the description before use.	This action releases all the devices in the scope of the action from quarantine.

Note

As you can see, there is a warning attached to the name of each instruction. Quarantine is a powerful solution for use in extreme circumstances and should be used with care. We therefore recommend these instructions have Actioner permissions assigned only to specific users, who are told the instructions must be used carefully.

Tip

If you used the Tachyon Product Pack Deployment Tool to upload the product pack, it will have created or updated an instruction set called **1E Explorer TachyonCore** , containing the above instructions. You can move the Quarantine instructions into their own instruction set, for example called **High Security**, and assign Actioner permissions to individual users or to a custom role.

4.4.12.1.3 What do I need to know before I quarantine a device?

Quarantine is available only on Windows, but not available on Windows XP.

Quarantine requires that at least one switch URI and one background channel URI each resolve to IPv4 addresses.

Quarantine will only work if a device's connection to the switch is over IPv4. This is because IPv6 is disabled by the quarantine mechanism.

The **CRLChecks** setting in the 1E Client configuration file should be set to soft.

As the device will be unable to contact anything but the tachyon server(s), the Tachyon client will be unable to retrieve CRLs for certificates requiring validation.

CRLChecks can be set to hard, but this can cause the Tachyon client to lose connection to the switch when the CRL validity period is exceeded.

Quarantine will persist until the **Release selected devices from quarantine** instruction is received.

If a Tachyon client cannot be connect to the Tachyon Server, it will not be possible to issue this command.

Any changes to the routing tables, IPv6 bindings or the hosts file made during quarantine will be reverted when the **Release selected devices from quarantine** instruction is received.

If the persistent storage of the client is deleted or modified by anything other than Tachyon whilst in quarantine, the client will not be able to release the device from quarantine properly.

Upgrading, uninstalling, installing or modifying the client installation during quarantine is not supported. Do not upgrade, uninstall or install Tachyon, or issue an extensibility update whilst the client is under quarantine.

After a release from quarantine the IPv4 loopback address will not be resolvable. A restart is required to fix this.

Quarantining a device will also stop it from being able to see Domain Controllers, so this may cause problems with logging on to the workstation. Cached logons should still work though.

4.5 Troubleshooting

A general methodology for investigating issues as well as identifying key issues and their resolutions.

4.5.1 Troubleshooting table

For known issues relating to specific components, please refer to the respective troubleshooting pages:

Clients	Platform	Applications	Integration
1E Client	1E	Endpoint Automation	1E Core for ServiceNow
1E Client Deployment Assistant		Experience Analytics	1E ITSM Connect for ServiceNow
PXE Everywhere		Endpoint Troubleshooting	1E Service Catalog Connect for ServiceNow
		Writing 1E Instructions (1E SDK)	

4.5.2 1E Support contact details

4.5.2.1 Support Web portal

Maintenance support customers can log onto the 1E Support Web Portal at https://support.1e.com/ using the login details provided with their maintenance contract. This provides issue tracking, product hotfixes, and knowledge base articles related to each product.

4.5.2.2 Telephone support

Maintenance support customers can contact the technical support department at 1E through the following support numbers. Just phone the relevant number for your area, so your call can be routed quickly and efficiently to the correct support group:

US/Canada:	1-866-349-4032 (Toll-Free)
	1-917-339-2360 (Standard)
UK/Europe:	+44 (0)208 326 3499
India:	+91 120 402 4002
Australia:	+61 739 111 118

4.5.2.3 Email support

Maintenance customers can use the following email for additional support:

support@1e.com

In this section:

4.5.2.3.1 Known issues

4.5.2.3.2 Server installation issues

4.5.2.3.3 Client issues

4.5.2.3.4 _Inventory issues

4.5.3 The technical support process

Read through the Troubleshooting pages to see if there are known issues, or quick resolutions to any problems you may have encountered.

Maintenance support customers can use the 1E Support Web Portal to review knowledge base articles and download hotfixes.

If still encountering problems, create a technical report (log files and details) and then contact the 1E technical support team.

4.5.3.1 Maintenance

You are recommended to review and apply hotfixes on a monthly basis. Hotfixes are provided in **Hotfix Bundles** and in **Monthly Updates**, which are installed using Tachyon Setup. Please refer to Maintenance.

4.5.3.2 Creating a technical report

If possible, please obtain the following details and log files before contacting 1E, to include in your technical report.

4.5.3.2.1 Version details

The OS, version number, and patch level for:

Tachyon Servers

1E Client

Configuration Manager - if used

Other 1E Server software, for example, Shopping, Nightwatchman, and WakeUp.

For Nomad and Shopping, please provide OS, version number, and patch level for:

Configuration Manager DPs

Nomad extensions used on Configuration Manager Consoles

ActiveEfficiency Server.

4.5.3.2.2 Environmental details

If there were any recent changes made to your configuration

The name of the machines, Configuration Manager Application and/or Package IDs for when the issue occurred

4.5.3.2.3 Problem details

When did the issue occur, ensure log files cover this period

The scope of the issue – did it affect a particular geographical location, group of users, or client machines

Details of any self-help troubleshooting steps you carried out

In the event of a service crash or if you are experiencing high CPU or memory usage, provide us with the dump file, event viewer logs, and traces. We will provide you with FTP details to upload these files.

4.5.3.3 Log files

Below is a summary, please refer to the Log files page for more details.

4.5.3.3.1 Tachyon Setup log files

Tachyon Setup creates a Setup log file for itself and an Install log for each of the components (if used) in the same folder as itself:

BIInstall.log

CatalogInstall.log

ContentDistribution.log

SLAInstall.log

Tachyon.Setup.log

TachyonInstall.log

4.5.3.3.2 Tachyon Server log files

For any issue, please provide a zip containing log files from the following locations:

%ALLUSERSPROFILE%\1E\Catalog*.log

%ALLUSERSPROFILE%\1E\ContentDistribution*.log

%ALLUSERSPROFILE%\1E\Platform Consumers*.log

%ALLUSERSPROFILE%\1E\SLA Platform*.log

%ALLUSERSPROFILE%\1E\Tachyon*.log

If you are having licensing issues, please include:

%ALLUSERSPROFILE%\1E\Licensing*

Please refer to the Log files page for more details.

4.5.3.3.3 1E Client log files

1E Client logs on Windows

1E Client logs on macOS

1E Client logs on other non-Windows platforms

Nomad client log

PXE Everywhere Agent log

Shopping WSA client log

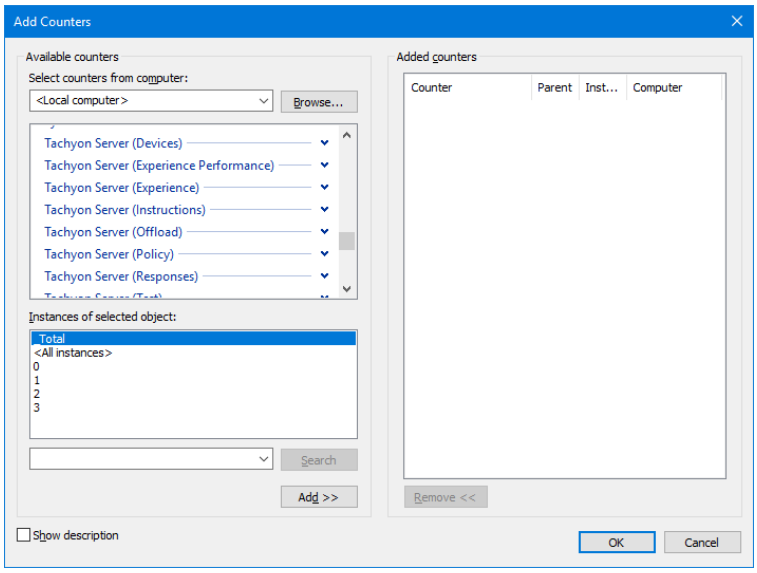
WakeUp client log

> **Note**
>
> By default, Windows resolves %ALLUSERSPROFILE% as C:\ProgramData\

4.5.3.4 Tachyon Windows Perfomance Counters

Tachyon now creates Windows Performance Counters that can be accessed using Performance Monitor. These are primarily for internal use and troubleshooting and need not be monitored, unless requested by 1E Support.

The counters are all under headings that start with **Tachyon**. The image shows the Performance Monitor **Add Counters** dialog with some Tachyon counters visible.



4.5.4 Known issues

Lists of the current known issues with implementing, configuring, and using Tachyon Explorer.

If you cannot find an issue and its workaround on this page, please:

Refer to Known issues for the Platform and other applications.

Try searching the 1E Support Portal https://support.1e.com/ for issues which have hotfixes.

If you need further help, please refer to the Troubleshooting page for how to contact 1E Support and the technical support process.

4.6 Reference

All the list type information, such as installer properties, in alphabetical lists etc.

4.6.1 Log files

Names and locations of log files created by Tachyon Server, 1E Client, and Tachyon tools.

4.6.1.1 Tachyon Setup logs

Tachyon Setup creates a Setup log file for itself and an Install log for each of the components (if used) in the same folder as itself:

AEInstall.log

BIInstall.log

CatalogInstall.log

SLAInstall.log

Tachyon.Setup.log

TachyonInstall.log

4.6.1.2 Tachyon Server logs

The default location for all Tachyon logs is the folder *%ALLUSERSPROFILE%\1E*

Subsystem	Component		
Tachyon Master	Tachyon Portal UI and applications (Tachyon)	1E\Tachyon\	`Tachyon.Portal.log`
Consumer API	1E\Tachyon\	`Tachyon.ConsumerAPI.log`	

Subsystem	Component		
Coordinator service	1E\Tachyon\	`Tachyon.Coordinator.log` `Tachyon.Instrumentation.log`	
Experience application	1E\Tachyon\	`Tachyon.Experience.log`	
Catalog	Catalog UI (CatalogWeb - Admin sync)	1E\Catalog\	*`Catalog.Integration.UI.log`*
Catalog API			
Catalog Update Service	1E\Catalog\	*`Catalog.UpdateService.log`*	
SLA	SLA/Platform APIs (Admin, Core External)	1E\Tachyon\	`Tachyon.AdminAPI.log`
SLA Platform UI (Platform)	1E\SLA Platform\	*`Web.log`*	
SLA Engine	1E\SLA Platform\	*`Engine.log`*	
SLA Integrate Services (Connector Manager)	1E\SLA Platform\	*`1E.SLAPlatformIntegrateAgent.log`* *`1E.SLAPlatformIntegrateManager.log`* *`1E.SLAConnector.<type>_sync.log`*	
SLA Inventory	n/a	n/a	

Subsystem	Component		
SLA Operations Provider (not currently used)	1E\Platform Consumer\	n/a	
SLA databases (Data, Integrate, Shared)	n/a	n/a	
BI	MDX API	SQL database	[SLA-BI].[BI].[Event Log]
Tachyon Response	Core	1E\Tachyon\	`Tachyon.CoreAPI.log`
Background Channel (Background)	1E\Tachyon\	*`Tachyon.BackgroundAPI.log`*	
Switch(es) (also includes a single Switch Host service)	1E\Tachyon\	`Tachyon.Switch.4000.SW1.log` `Tachyon.Switch.Host.log`	

Please refer to Services and NTFS Security if changing the location of log files.

In this version of Tachyon Server, some installers do not support the LOGPATH property and the logs folder is not configurable during installation.

Each component has a configuration file in the Tachyon Server installation folder structure, which contains log configuration details. Defaults are:

Filepath *%ALLUSERSPROFILE%\1E\<product>* where product is Tachyon, SLA Platform, and Catalog

Filename as shown in the table above.

Maximum size 10MB (2MB for Switch logs).

2 rollover files numbered 1 to 2 with the rollover number included as n.log (5 rollover files for Switch logs).

Date and timestamps are UTC to help troubleshooters synchronize logs on systems in different timezones.

Switch logs have the following names:

The first Switch installed will typically have a log filename **Tachyon.Switch.4000.SW1.log** (where 4000 is the port it is listening on and SW1 is the **config name** in the SwitchConfiguration table in the TachyonMaster database).

Other Switches on the same server will have different config names appended.

The log filename will be unique on a server, but there may be the same named log on a different server.

A Switch will continue to use the same log, unless the SwitchConfiguration table is modified so that a different ID is used.

If you see a Tachyon.Switch.log without a config name appended, this is a special case where a Switch cannot find its correct configuration, and has fallen back to using the template * row which has ID=1. In which case you will need to troubleshoot how that happened.

Rollover logs have numbers appended, for example Tachyon.Switch_A.1.log, up to a default maximum of 5.

Tachyon server components use the **log4net RollingFileAppender** class. Details can be found in http://logging.apache.org/log4net.

4.6.1.2.1 Summary of server log file locations

For any issue, please provide a zip containing log files from the following locations:

%ALLUSERSPROFILE%\1E\Catalog*.log

%ALLUSERSPROFILE%\1E\Platform Consumers*.log

%ALLUSERSPROFILE%\1E\SLA Platform*.log

%ALLUSERSPROFILE%\1E\Tachyon*.log

If you are having licensing issues, please include:

%ALLUSERSPROFILE%\1E\Licensing*

Please refer to the Log files page for more details.

4.6.1.2.2 Logging Levels

The table below describes the logging levels which are configurable for server components.

Value	Description
Error	Only outputs errors. An error is a serious problem, typically requiring operator intervention of some sort to restore full functionality.
Warn	Outputs errors and warnings. A warning indicates a potential problem, where the system can nonetheless function without intervention.
Info	Outputs general information in addition to errors and warnings. This is the default.

Value	Description
Debug	Outputs debugging information in addition to all the previous levels.

Warning

Logging levels should only be changed from **info** only if requested by 1E Support and reset to **info** after investigation is complete.

Tip

The method of configuring logging levels uses the above text values, where -log=0 is the default to mean the same as *-log=info*.

4.6.1.3 1E Client logs

1E Client logs on Windows

%ALLUSERSPROFILE%\1E\Client\1E.Client.log (used by 1E Client and Tachyon features, and Shopping client)

%ALLUSERSPROFILE%\1E\Client\NomadBranchUninstall-YYYY_MM_HHTMM_HH_SS_000Z.log

1E Client logs on macOS

/Library/Logs/1E.Client.Daemon.log (shows any service start errors)

/Library/Logs/1E.Client.log (shows the current operation of the 1E Client)

1E Client logs on other non-Windows platforms

/var/log/1E/Client/1E.Client.log

Nomad client log

%ALLUSERSPROFILE%\1E\NomadBranch\LogFiles\NomadBranch.log

PXE Everywhere Agent log

%ALLUSERSPROFILE%\1E\PXEEverywhere\PXEEverywhere.log

Shopping WSA client log

%ALLUSERSPROFILE%\1E\Client\WSA.log

WakeUp client log

%ALLUSERSPROFILE%\1E\Agent\WakeUpAgt.log

Note

By default, Windows resolves %ALLUSERSPROFILE% as C:\ProgramData\

4.6.1.4 Software Reclaimer logs

Every time the Reclaimer runs it will create a local log file of the process it is doing. The location and name of the log file depends on what task the reclaimer is doing.

Task	Logpath	Notes
Optout	**C:\Users\{USER}\AppData\Local\Temp\ AppClarity.SoftwareReclaimer.log**	Optout mode is normally run under user context so that the user can interact with the dialog. This means the log file will be in the users Temp folder within the user profile.
Mandatory	**C:\windows\Temp\AppClarity.SoftwareReclaimer.log**	Mandatory mode is normally set to run under system context, in order to process reclaim uninstall command

Task	Logpath	Notes
		s. Therefore, the log file will be under the system temp directory.
Reclaim	**C:\windows\Temp\AppClarity.SoftwareReclaimer.MSI.log**	For a mandatory reclaim, if a reclaim occurs using an MSI then an MSI log file is also created.

4.6.1.5 Configuration Manager Console Extensions log

%ALLUSERSPROFILE%\1E\Tachyon\Tachyon.CmConsole.log

%ALLUSERSPROFILE%\1E\Tachyon\Tachyon.RunInstructionUI.log

4.6.1.6 The Instruction Management Studio (TIMS) log

%ALLUSERSPROFILE%\1E\Tachyon\Tachyon.InstructionManagementStudio.log

4.6.1.7 Tachyon Product Pack Deployment Tool log

Tachyon.ProductPackDeploymentTool.log

In the same location as the tool.

4.6.2 Explorer reference

Reference information specific to Explorer.

4.6.2.1 Coverage parameters

Details of the parameters available when setting the coverage for a question or action.

4.6.2.1.1 Coverage parameters

When the Tachyon clients start and connect to Tachyon they provide some basic information about the devices they are running on that enables Tachyon to determine the coverage of a question and be selective about which devices get asked.

The information returned enables the coverage to be limited according to the following attributes:

Attribute	Description
Management group	Limits coverage to the devices specified by the selected Management group.
Device	Limits coverage according to complete or partial matches for the provided text found in the device's FQDN.
Primary User	Limits coverage to the devices where Tachyon has determined the selected user to be the primary user of each device.
Criticality	Limits coverage to the devices where the 1E Client has the selected Criticality set, or not set.
Device Tags	Limits coverage to devices where the 1E Client has the selected Device tag name and value set.
Operating System	Limits coverage according to the Type, Name and Version number of the device's Operating System.
Hardware	Limits coverage according to the device type, model, virtual platform or installed RAM.
Tachyon Agent Version	Limits coverage according to the device's installed Tachyon Agent or client version.
Last boot	Limits coverage according to whether the last time the device was rebooted was before or after a given date and time.
Timezone	Limits coverage to devices with the selected timezone set.
Location	Limits coverage to the devices where the 1E Client has a Location set, that matches with a specified search string.
Device list (FQDN)	Limits coverage to the devices specified in a comma-separated list of device FQDN.

Please read Limiting coverage using a Management group - tutorial for more information on other ways to set coverage to a group of devices.

4.6.2.1.2 Management group

You can search for and select a Management Group. If you do not select a group, then the default All Devices group is used.

For more information, please refer to the Tachyon Platform Management Groups page.

4.6.2.1.3 Device

Control	Description
Operator	This drop down list contains the following operators:
Edit field	Set this to any part of the FQDN for the devices you are trying to match

Operator	Description
=	Will match if the source string is equal to the contents of the edit field
Begins with	Will match if the source string begins with the contents of the edit field
Ends with	Will match if the source string ends with the contents of the edit field
Contains	Will match if the contents of the edit field can be found anywhere in the source string

4.6.2.1.4 Criticality

Control	Description
Operator	This drop down list contains the following operators:
Edit field	Set this to one of the following types:

Operator	Description
=	Equals
!=	Does not equal

Control	Description
	Criticality Undefined Non-critical Low Medium High Critical

For more information, please refer to the Using Device Criticality.

4.6.2.1.5 Tags

Chart	Description
Key drop-down list	Select from the list of currently defined coverage tag keys to match against any coverage tags set on the target devices
Value drop-down list	Select from the list of values for the selected coverage tag key to match against the value set for the selected coverage tag on the target devices

For more information, please refer to Tagging client devices.

4.6.2.1.6 Operating System

Chart	Description
Type	This drop down list lets you select from one of the following Operating System types: Operating System Windows Linux MacOS

Chart	Description
	Android Solaris
Name	This parameter lets you match string values in the name of the Operating System.

Control	Description
Operator	Operator: = — Will match if the source string is equal to the contents of the edit field Begins with — Will match if the source string begins with the contents of the edit field Ends with — Will match if the source string ends with the contents of the edit field Contains — Will match if the contents of the edit field can be found anywhere in the source string
Edit field	Set this to any part of the Operating System name you want to match

Version — This field lets you set a numeric comparison on the version number of the Operating System on the device. The drop-down list contains the following operators:

Control	Description
Operator	Operator: = — Will match if the source value is equal to the contents of the edit field >= — Will match if the source value is greater than or equal to the contents of the edit field <= — Will match if the source value is less than or equal to the contents of the edit field

Chart	Description
Edit field	Set this to the OS version you want to compare against

4.6.2.1.7 Hardware

Chart	Description
Device Type	Select from: Device Type Desktop Laptop Mobile Server
Model	Control: Edit field Description: Set this to any part of the Model name you want to match Operator: = Operator Description: Will match if the source string is equal to the contents of the edit field Operator: Begins with Operator Description: Will match if the source string begins with the contents of the edit field Operator: Ends with Operator Description: Will match if the source string ends with the contents of the edit field Operator: Contains Operator Description: Will match if the contents of the edit field can be found anywhere in the source string
Virtual Platform	If you want to constrain the coverage to a particular type of virtual platform, select one of the following from the drop-down list:

Chart	Description
	Virtual Platform
	Virtual Server
	Hyper-V
	VMWare
	VirtualBox
	Red Hat KVM
RAM (MB)	Set a comparison value for the amount of RAM in MB on the target devices.

Control	Description
Operator	Operator Description
	= Will match if the source value is equal to the contents of the edit field
	>= Will match if the source value is greater than or equal to the contents of the edit field
	<= Will match if the source value is less than or equal to the contents of the edit field
Edit field	Set this field to the value in MB you want to compare the target device's RAM against.

4.6.2.1.8 Tachyon agent version

Controls	Description
Operator	This drop down list contains the following operators:

Operator	Description
=	Will match if the source value is equal to the contents of the edit field

Controls	Description	
	>=	Will match if the source value is greater than or equal to the contents of the edit field
	<=	Will match if the source value is less than or equal to the contents of the edit field
Edit field	Set this to the Agent or client version you want to compare against.	

This coverage parameter allows you to set a version range by adding a less than or equal to and a greater than or equal to comparison using the **Add** option.

4.6.2.1.9 Last boot

Control	Description	
Operator	Operator	Description
	Before	Will match if the source date is on or before the date set in the date picker field
	After	Will match if the source date is on or after the date set in the date picker field
Date picker	Use the date picker control to select the date you want to compare the last boot date of the device against	

4.6.2.1.10 Timezone

Control	Description
Timezone drop-down list	Select from this drop-down list of timezones with their UTC values and locations to match against the timezones set for the target devices

4.6.2.2 Devices dashboard filters and charts

Details of the filters and charts available on the Devices dashboard.

4.6.2.2.1 Devices dashboard filters

Filter	Description
Operating system	Partitions the Tachyon client devices according to the OS running on the devices.

Filter	Description
Operating system version	Partitions the Tachyon client devices according to the OS version running on the devices.
Tachyon agent version	Partitions the Tachyon client devices according to the version of the Tachyon client running on the devices.
Status	Partitions the Tachyon client devices according to the current connection status of the devices.
Device type	Partitions the Tachyon client devices according to the type of the devices.
Timezone	Partitions the Tachyon client devices according to the time zone the devices are configured with.
Location	Partitions the Tachyon client devices according to their location.

4.6.2.2.2 Devices dashboard charts

Chart	Description
SmartBar	Displays a single horizontal bar where the distinct values in the data are represented by different colors. The individual colored blocks can be clicked on to select the corresponding devices that have that value.
Pie	Displays a pie chart where the distinct values in the data are represented by different colors. The wedges can be clicked on to select the corresponding devices that have that value.
Column	Displays a column for each distinct value in the data. Each column can be clicked on to select the corresponding devices that have that value.
Bar	Displays a horizontal bar for each distinct value in the data. Each bar can be clicked on to select the corresponding devices that have that value.

4.6.2.3 Responses Summary tab information

Details of the information displayed on the **Responses** page **Summary** tab.

4.6.2.3.1 The Statistics table

The following information for the running instruction is shown in the **Responses** page **Summary** tab statistics table:

Statistic	Description
Dispatch sequence	Displays the number for the instruction used in the workflow. This may be referenced against the Tachyon logs to track down issues related to running the instruction
Running time	The total time the instruction has been running for
Approximate target	The approximate number of devices the instruction has been sent to. This is an approximate value because a new device might register with Tachyon while the instruction is still running and be included in the instruction's target
Sent count	This displays the number of devices the instruction has been sent to
Responses count	Displays the number of devices that have responded to the instruction. This is displayed in the PERCENT SENT COUNT chart.
Awaiting responses count	Displays the number of devices that have been sent the instruction where Tachyon is still awaiting a response. This is displayed in the PERCENT SENT COUNT chart.

4.6.2.3.2 The Responses table

The following information for the running instruction is shown in the **Responses** page **Summary** tab responses table:

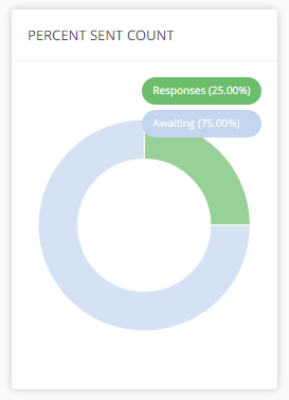
Reponses	Description
Success	Devices that have responded with a success status
Success - no content	Devices that have responded with a success status but did not provide a response to the instruction content request
Error	Devices that have responded with an error encountered when attempting to run the instruction
Not implemented	Devices that have responded where the feature contained in the instruction is not implemented on the device
Response too large	Devices that have not been able to respond to the instruction content request because their response was too large

4.6.2.3.3 The Performance table

Performance	Description
Average execution time	The average instruction execution time for the devices
Average bytes received	The average number of bytes received from each device in response to the instruction
Total bytes received	The total number of bytes received by all devices responding to the instruction
Total bytes sent	The total number of bytes sent by Tachyon when performing the instruction
Total number of rows inserted	The total number of rows inserted into the TachyonResponses databases (response, error and aggregated) as a result of performing the instruction
Total number of rows processed	The total number of rows processed by the core as a result of performing the instruction. **Note** This value may be higher than the Total number of rows inserted depending on whether the instruction results are aggregated or not.

4.6.2.3.4 The PERCENT SENT COUNT chart

This chart displays the percentage of the sent instructions divided into received **Responses** and **Awaiting** responses.

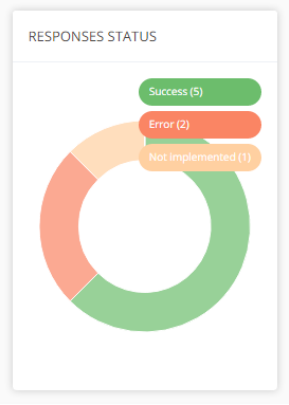


4.6.2.3.5 The RESPONSES STATUS chart

This chart displays the received response statuses. These may be one of the following:

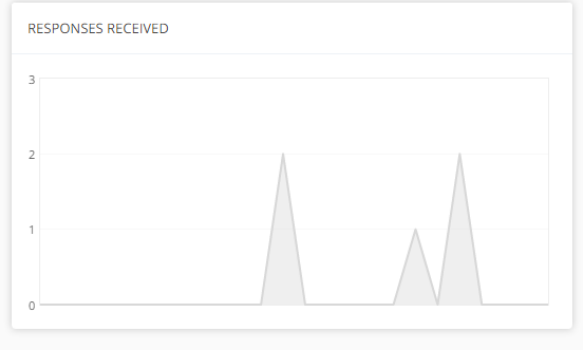
Reponses	Description
Success	Devices that have responded with a success status
Success - no content	Devices that have responded with a success status but did not provide a response to the instruction content request
Error	Devices that have responded with an error encountered when attempting to run the instruction
Not implemented	Devices that have responded where the feature contained in the instruction is not implemented on the device
Response too large	Devices that have not been able to respond to the instruction content request because their response was too large

This picture shows the RESPONSE STATUS chart with three types of response status displayed:



4.6.2.3.6 The RESPONSES RECEIVED chart

This chart displays in real-time the number of responses received while the instruction is active.



4.6.2.4 Explorer comparison operators

Details of the operators available when configuring comparisons for different data types, for example question coverage parameters.

4.6.2.4.1 String comparison operators

When configuring comparisons for string values, the following operators are available:

Operator	Description
=	Will match if the source string is equal to the contents of the edit field
Begins with	Will match if the source string begins with the contents of the edit field
Ends with	Will match if the source string ends with the contents of the edit field
Contains	Will match if the contents of the edit field can be found anywhere in the source string

4.6.2.4.2 Numeric comparison operators

When configuring comparisons for numeric values, the following operators are available:

Operator	Description
=	Will match if the source value is equal to the contents of the edit field
>=	Will match if the source value is greater than or equal to the contents of the edit field
<=	Will match if the source value is less than or equal to the contents of the edit field

4.6.2.4.3 Date comparison operators

When configuring comparisons for date values, the following operators are available:

Operator	Description
Before	Will match if the source date is on or before the date set in the date picker field
After	Will match if the source date is on or after the date set in the date picker field

4.6.3 Glossary

A glossary of Tachyon terminology.

4.6.3.1 Tachyon alphabetical glossary

Term	Definition
1E Client	1E Client provides client features and modules for 1E products including Tachyon. It replaces the Tachyon Agent.
Action	An Action is a specific type of instruction that is sent to client devices which can be used to modify the state of the target device. For example, setting a registry key, killing a process, deleting a file. Whereas a Question is an instruction that requests information from the target device, but does not change its state. Generally an Action needs to undergo an approval process before it is sent.
Agent	Agent is the old name for the client. The Agent has been replaced by the 1E Client which provides client features and modules for 1E products including Tachyon.
All Instructions Approver	This is a Tachyon system role which allows assigned users to approve actions for all Instruction Sets . Users can approve unless the action was requested by themselves.
All Instructions Questioner	This is a Tachyon system role which allows assigned users to ask questions and view responses for all Instruction Sets; use custom properties.
All Instructions Viewer	This is a Tachyon system role which allows assigned users to view instructions and responses for all Instruction Sets.
Audit information log	The Audit information log page displays audit information related to installation, permissions, instruction set and consumer related operations carried out using the Explorer and Settings applications. See Audit information log page
Historic Data Capture	The old name for Tachyon Activity Record.

Term	Definition
Agent Language	The Agent language is an interpretive programming language that is executed by the client in the form of an **instruction payload**. Instructions, and their payload, are based on instruction definitions which are stored in the TachyonMaster database. Definitions are uploaded into the database from the Administrator console by dragging and dropping one or more Instruction Definition files, a Product Pack or ZIP file containing Instruction Definition files. The language, called SCALE, uses Agent modules and methods and is documented in the SDK.
Agent Provider	A plug-in component for the 1E Client which communicates with an external component, such as an operating system facility (for example Windows registry) or a service-provider application (for example Content Distribution). 1E Client modules use Providers to get their work done. Examples: WMI provider Registry provider Nomad provider BASH provider
Auto-curation	Auto-curation is a Catalog function and refers to the automated process of creating match rules in 1E Catalog. These match rules are neither created by the customer not by the 1E curation team. The rules are created in the customer's local 1E Catalog copy using automated logic built by 1E.
Background Channel	The Background Channel is a mechanism by which the Tachyon client can download resources via HTTPS without loading the Switch. Since this traffic does not go through the Switch, the client is still able to receive and process instructions instructions while performing these downloads. From v2.0 onwards, the client is able to download resources via Content Distribution. The Background Channel is a web application on the Tachyon Server Website and provides the following:

Term	Definition
	Stores Tachyon content from the Consumer API in the Background Channel for clients to retrieve Responds to clients retrieving Tachyon content from the Background Channel See Tachyon Architecture and Communication Ports.
Client module	A plug-in component for the 1E Client which encapsulates business logic. Modules contain Methods, which can be invoked by SCALE. Modules (and their methods) effectively provide a platform independent API. To that end, Modules and their Methods do not (generally) talk about anything platform specific (Windows, Linux, Android etc). Examples: FileSystem OperatingSystem Network Software
Column filters	Some tables contain a column filter that lets you easily filter the information displayed in the table.**Using column filters**The picture opposite shows an example taken from AppClarity. In our example we want to filter the table to show only those items where the **Edition** contains the text **Prof**.To filter the table on the **Edition** column:Click on the filter iconjust beneath the header row in the **Edition** column.The filter popup is displayed.Now select the operator. In our example this will be **contains**.Then type the text **Prof** into the text field.Click **Apply** and a new filter will be added to the table.The table will be filtered to just those items whose **Edition** contains the text **Prof**.**Adding another filter**You can add another filter by clicking on the filter icon for any of the columns. The picture opposite shows another filter added selecting table rows where the **Type** also contains the text **License**. The table will also be filtered accordingly.**Removing filters**You can remove filters by clicking on the filter close icon at the end of the filter.
Column Picker	**Using column picker**Where the column picker control is shown you can choose which columns are displayed. In the following example on

Term	Definition
	the **Microsoft Core License Demand** page we hide the **Unknown Installs** column and move the **License Demand** column to the left of the page.To pick the displayed columns:Click on the Choose columns iconto the right of the header row to view the visible columns.To exclude **Unknown Installs**, select the Unknown Installs row and click **Exclude columns** button.The **Unknown Installs** column is now hidden.To move the **License Demand** column to the top of the list, hover your mouse over **License Demand** and using the direction control drag it to the top of the list.The Microsoft Core License Demand page has now been automatically updated with our changes.
Column sorts	Some tables contain column sorts that let you easily re-order the information displayed in the table.**Using column sorts**The picture opposite shows an example taken from AppClarity. In our example we want to sort the table on the **Cost** column from the highest cost at the top to the lowest at the bottom. To sort the table on the **Cost** column:Click on the sort iconjust beneath the header row in the **Cost** column.The sort popup is displayed.Now select the sort direction. In our example this will be **Sort descending**.After selecting this the data in the table is now sorted on the **Cost** column from highest to lowest and the sort icon has changed to a sort descending icon**Clearing the sort**You can clear the sort by clicking on the sort icon again and selecting the **Clear sorting** menu item from the sorting popup.
Configuration Manager Extensions	The Configuration Manager Extensions currently include. Configuration Manager Agent emergency stop and resume actions Configuration Manager Agent actions Client Health Check Tachyon Run Instruction utility (used by the each of the above right-click actions to request Tachyon to run an instruction) Tachyon Instruction Runner (a mini UI version of the Tachyon Explorer) This feature is included in the Tachyon Toolkit. Documentation for installing and using the Configuration Manager Extensions will be available soon.
Consumer	A Consumer is any application that connects to and uses the Consumer API. An example is the Explorer application.

Term	Definition
Consumer API	The Consumer API is a documented set of API endpoints provided by a web application on the Tachyon Web Server called Consumer. It is referred to as the Consumer API in order to avoid confusion with Tachyon Consumers, which are 'consumers' of the API. The Consumer API is a web application on the Tachyon Server Website, actually named Consumer, and provides the following: Processes the consumer requests from the Explorer and other Consumers Publishes Tachyon content to the Background Channel Forwards requests for instrumentation data from the Explorer to the Tachyon Instrumentation component Forwards workflow commands from the Explorer to the Tachyon Workflow component See Tachyon Architecture and Communication Ports.
Consumer requests	A Consumer sends requests to the Consumer API.
Coordinator Service	The Coordinator Service has two modules: Instrumentation module Workflow module See Tachyon Architecture and Communication Ports.
Coordinator Instrumentation module	The Coordinator Instrumentation module is part of the Coordinator Service on the Tachyon Server which processes instrumentation data from the following components: Core Coordinator Workflow module Switch And responds to requests for instrumentation data from the Consumer API. See Tachyon Architecture and Communication Ports.

Term	Definition
Coordinator Workflow module	The Coordinator Workflow module is part of the Coordinator Service on the Tachyon Server that provides the following: Forwards workflow commands from the Consumer API to the Core Stores workflow in SQL Connects to remote SMTP to send emails used in the approval process for actions See Tachyon Architecture and Communication Ports.
Core	The Core is a Tachyon Server web component that does the following: Forwards workflow commands from the Coordinator workflow module to the Switch Forwards responses from the Switch to the Responses database (this task requires high throughput) Generates and sends instrumentation data to the Instrumentation service See Tachyon Architecture and Communication Ports.
Core Internal	Core Internal is the part of the Core which allows fast internal communication with the Switch using HTTP instead of HTTPS, restricted to the Switch server's local IP Address only. See Tachyon Architecture and Communication Ports.
Custom Role	Tachyon roles that define which Users have access to which Instruction Set. These roles can be modified in the Administration pages by users assigned to the Full Administrator role.
Custom Properties	Full Administrator can manage the custom properties using the Properties page in Explorer. The only custom property type available after installing the Tachyon server is Coverage tags, further types may be added during installation of other Consumers.

Term	Definition
Device tags	Device tags can be used when setting the coverage for a particular question so that only client devices with a particular tag name and value get the question. The names and values of Device tags must be pre-configured by a Full Administrator before setting them on a client device using Device tag actions. Device tags can also be queried directly by Device tag questions. Device tags were previously known as Coverage tags. In 1E Client log files, Device tags are also referenced as scopable tags. Please also see Freeform tags.

DNS Name	DNS Name FQDN is the term used in this documentation to represent the name of a Tachyon Server. Typically a Tachyon Server will have only one DNS Name, which will be the CNAME or an (A) Host record that uniquely represents a server's IP Address. 1E normally recommends using an CNAME record.
	
	In a Tachyon system, each Tachyon Server will have a DNS Name FQDN.
	
	In a single-Switch installation the Switch is on the same server and uses the same DNS Name. When a Response Stack has more than one Switch, each Switch has its own IP Address, so you can choose if the will share the same DNS Name, or if each will have its own DNS Name. The Tachyon Server certificate must have all
	
	`NAME TYPE VALUE`
	`----------`
	`tachyon.acme.com. CNAME tachyon.acme.local.`
	`tachyon.acme.local. CNAME foo.example.com.`
	`foo.example.com. A 192.0.2.23`
	
	`tachyon.acme.com is an Alias record`
	
	`tachyon.acme.local is a CNAME record`
	
	`foo.example.com is a (A) Host record`

Event Subscription	A type of instruction that can be sent to the client. An Event Subscription tells the client to monitor an arbitrary event source for a period of time (defined by the Instruction's TTL), to capture events as they occur and to report them back via the Switch.

Term	Definition
Guaranteed State application	The Explorer application is the web portal used by users and administrators. It is an example of a Consumer application. **Note** Explorer can be reached directly using the following URL: `https://<tachyon DNS Name FQDN>/Tachyon/App/#/explorer/` where <tachyon DNS Name FQDN> is the one set up during the preparation phase, as described under the heading DNS Names. It is a web application on the Tachyon Server Website and provides the following: Browser connection providing the Explorer and Administration pages Sends consumer requests to the Consumer API See Tachyon Architecture and Communication Ports.
Filters	There are two kinds of filter: Question filters are used to reduce the responses from the clients; View filters reduce the information displayed in Explorer on the Responses page.
Freeform tags	Freeform tags may be used to set properties on client devices that can subsequently be used in Freeform tag questions. They cannot be used when defining the coverage for a question. Freeform tags can be set with arbitrary names and values that are defined only when running a Freeform tag action. In Tachyon log files, Freeform tags are also known a non-scopable tags. Please also see Device tags.
FQDN	Fully Qualified Domain Name. This is the complete domain name for a specific IP-connected device, and is unique within the network and unambiguous. The FQDN consists of two parts: the hostname and the domain name. For example tachyon.acme.com.
Full Administrator	This is a Tachyon system role which has the combined rights of all the other system roles.

Term	Definition
Group Administrator	This is a Tachyon system role which allows assigned users to create, modify and delete Management groups and modify their membership.
Guaranteed State application	Guaranteed State application is used to ensure endpoint compliance to enterprise IT policies. It is an example of a Consumer application. **Note** Guaranteed State can be reached directly using the following URL: `https://<tachyon DNS Name FQDN>/Tachyon/App/#/guaranteedstate/` where <tachyon DNS Name FQDN> is the one set up during the preparation phase, as described in DNS Names.
Instruction	Instruction is the generic term used to describe: Questions Actions An Instruction is sent to one or more clients, and will yield one or more responses.
Instruction Definitions	Instruction Definitions are retrieved from the Core by the Switch. They define the type and functionality of the instructions and are used to control the clients to respond in the appropriate way.
Instruction Definition Files	Instruction Definition files are XML format files that contain definitions for Instructions and any associated resources.
Instruction Sets	Instruction Sets provide a way of organizing instructions and setting permissions on those instructions. They can be created, modified and deleted from the Tachyon Administration console.
Instrumentation data	Each of the Tachyon components creates instrumentation data that can be used to display how the Tachyon system is performing.
JSON Provider	This is an internal provider within the Tachyon agent library, used to deserialize and return a JSON string as a data table. Analogous to the Windows specific PowerShell Provider.

Term	Definition
Legacy OS	In this documentation, Windows XP, Vista and Windows Server 2003 are referred to as legacy OS. Microsoft has withdrawn support for Windows XP and Windows Server 2003, but 1E includes Vista in this list because it is not significantly used by business organizations. For details of limitations and additional considerations for these OS, please see Supported Platforms.
License file	1E will provide you with a **Tachyon.lic** license file that defines the applications, tools, and features your Tachyon System is able to use, for how long, and how many devices it supports, this may be an evaluation or subscription license. The license must be activated. Once activated, it may be used only by the Tachyon System that activated it. Licenses can be renewed or updated, but if allowed to expire, then the affected products or features will not be usable. For a new installation, the Tachyon Setup program will let you select the license file from any folder on disk. For an existing installation, the license file is copied into the folder: %PROGRAMDATA%\1E\Licensing on your Tachyon Server. Ensure the following URL is whitelisted: https://license-v1.1e.com This URL must be accessible from the Tachyon Server during setup and running of Tachyon. The Tachyon license must be validated on a regular basis via internet contact with the 1E license service. The regular validation period is set when the license is requested. For whitelisting purposes, the Tachyon Server (specifically the Coordinator Workflow module in the Master Stack) requires an Internet connection to the 1E license service, as defined in the license file itself. If activation fails, then the system will install but not be usable until activation is completed. **Upgrading**

Term	Definition
	When upgrading, you are recommended to get a new license file and update your whitelist with the new URL. The old URL (https://license.1e.com) is suitable only for 8.0 and earlier. However, if you are upgrading and your license file has the old URL then you should also whitelist the old URL.
License Service	The License Service is hosted in the cloud by 1E, and accessible via an internet connection.
Method	Methods are documented in the SDK.
Normalization	Normalization is a Platform function that refers to the process of finding (or not finding) a match rule in 1E Catalog, then deduplicating and rationalizing the information using Platform logic, and publishing the information on the 1E Catalog UI. Partial Matching for example does not have a match rule in 1E Catalog but it's still normalized and published on the UI using Platform logic.
Patch Success application	Patch Success application is used to report on and ensure successful patching of your enterprise. **Note** Patch Success can be reached directly using the following URL: `https://<tachyon DNS Name FQDN>/Tachyon/App/#/patchsuccess/` where <tachyon DNS Name FQDN> is the one set up during the preparation phase, as described under the heading DNS Names
Permissions	How the Role-Based Access Control feature assigns Users to Roles, providing access to Instruction Sets and Administration pages.
Persistent Storage	The client stores information in Persistent Storage which it needs each time it starts. For example the last processed instruction. A hash value of each item of information is stored in the registry, which the client uses to ensure it trusts each item. Persistent storage includes a local database that is compressed and encrypted in a way that ensures a very low impact on device performance and security. This database is used to store data for the Tachyon Activity Record feature.

Term	Definition
PowerShell Provider	This is a Windows specific internal provider within the Tachyon agent library. It provides functionality to execute powershell.exe from a fixed location (System32\WindowsPowerShell\v1.0) on a PowerShell (.sp1) script and return the result. Some earlier versions of Windows (such as Windows XP) do not support PowerShell.
Product Pack	Product Packs contain instructions or other things which extend the capabilities of Tachyon. Product Packs which are required to support Tachyon features out-of-the-box are provided in the Tachyon Platform zip downloaded from the 1E Support Portal. Other Product Packs are available for download from the 1E Exchange. There are two types of Product Packs described in the following table. **Classic Product Packs**: Classic Product Packs contain instructions (actually Instruction Definition files) for use in Explorer and other Tachyon applications. Classic Product Packs can be uploaded into Tachyon using either of the following methods: Tachyon Product Pack Deployment Tool - which will upload the instructions in the pack and create an Instruction Set for them based on the name of the zip (with hyphens converted into spaces) the Tachyon Portal Settings app→ Instructions → Instruction Sets, described in Instructions Menu. This method requires instructions to be organized into Instruction Sets by an Instruction Set Administrator. Settings can also be used to export instructions.

Term	Definition	
		Either method requires an Instruction Set Administrator to configure permissions for accessing the instructions.
	Integrated Product Packs	Integrated Product Packs contain policies, rules and fragments for use by Guaranteed State, and may also include instructions. If the Integrated Product Pack contains instructions associated with the policies, the tool creates an Instruction Set using the name in its manifest file. Integrated Product Packs are uploaded using the PPDT.
Tachyon Product Pack Deployment Tool	A tool for uploading Classic and Integrated Product Packs. Please see Tachyon Product Pack Deployment Tool.	
Providers	Providers can be used by applications to leverage external tools to perform specific operations. For example the reclaim provider enables software to be uninstalled, thereby extending the functionality of the platform to include uninstallation.	
Question	In Tachyon a Question is a specific type of instruction that requests information from client devices. The information is returned to Tachyon as responses.	
Report Refresh	You can refresh reports from individual AppClarity screens as well as using the Settings App. Where this is available you can do this by using the refresh icon next to the **Last Refreshed** box: 	
Response	The data resulting from a client executing an instruction.	
Role-Based Access Control	Also known as RBAC. This is a general term for assigning users to roles which allow them access specific features of Tachyon.	

Term	Definition
	Roles can be assigned to AD users and groups added in the Administration Security page. A role can be either of the following: System role Custom role
SCALE	The Agent Language.
SDK	The Tachyon SDK describes the following and is available here: /document/preview/736743#UUID-33c212b3-863e-21bc-bc5d-52e41a0492b3 Agent Language (SCALE) Agent modules and methods
Securable	Refers to an item that may be secured by Tachyon using RBAC.
Server installation account	This is the account used to run Tachyon Setup (and the MSI installer) when installing or upgrading a Tachyon Server. The account is automatically defined as a Tachyon admin user with limited rights which cannot be edited (called a system principal). The installation account only has sufficient rights to add other users, assign them to roles, and install Tachyon applications. The users and roles created by the installation account are then used for ongoing use and management of Tachyon. If you need the installation account to have additional roles or be a Full Administrator, then the recommended approach is: First create a role-based AD Security group, and add the installation and other accounts to this group Then, the installation account: Logs into Tachyon and navigates to Settings → Permissions → Users and Groups Creates a new user for the role-based AD Security Group Assigns the relevant system role(s) to the new user - this can be Full Administrator.

Term	Definition
	When installing a Tachyon Server, the account must be an Active Directory domain account with various rights on the Tachyon Server and the SQL Server instance. For more detail see Tachyon Server Installation Account. For a new installation, only the Server installation account is able to use the Explorer and assign user rights to other users and groups. Once these other users or groups have been assigned, then the Server installation account can be optionally disabled in AD pending future updates and upgrades. The Server installation account is a system principal and cannot be deleted or granted additional rights; it is able to manage additional users and groups, create and edit custom roles, which are then used for ongoing use and management of the system. However, the account may be included in any AD security group assigned to a Tachyon system or custom role.
Server instructions	A special type of instruction, which cannot be run in Explorer. They are for internal use only, run on the server, and used to carry out on-demand or scheduled processing of data across various datasources, such as SQL databases. For example, the Dashboards app uses them to populate tiles and charts with data from the TachyonMaster and Experience databases. They are also called server-side instructions, to differentiate them from client-side instructions which run on client devices.
Settings application	Settings application is used to configure Tachyon system and application settings. It is an example of a Tachyon Consumer application. **Note** Settings can be reached directly using the following URL: `https://<tachyon DNS Name FQDN>/Tachyon/App/#/platform/` where <tachyon DNS Name FQDN> is the one set up during the preparation phase, as described under the heading DNS Names.
Single-Switch installation	A **single-Switch installation** is a type of single-server installation which has only one Switch. This is the simplest Tachyon Server configuration.

Term	Definition
Single-server installation	A **single-server installation** is where all Tachyon Server components are installed on the same Web Server, with one to five Switches, and SQL Server either local or remote. A single-Switch installation is the simplest configuration. More than one Switch requires additional hardware resources. If SQL Server is remote then it is also referred to as a **split-server configuration**. Best performance is achieved using a local SQL Server installation. See Tachyon Architecture and Communication Ports.
SMTP gateway	Systems such as the Tachyon Server connect to the gateway in order to send emails. Also known as SMTP relay.
Switch	The Switch component on the Tachyon Server provides the following: Sends instructions to and retrieves responses from the clients Forwards responses to the Core component Receives workflow commands from the Core component Retrieves instruction definitions from the Core component Sends instrumentation data to the Instrumentation component On the Tachyon Server, the Switch Host service is responsible for managing all the local Switches The Switch configuration is stored in the SwitchConfiguration table of the TachyonMaster database. This includes the number of slots and workers used by the Switch which controls the maximum number of devices that can be managed by each Switch. A Switch restart will fail if the Switch failed to de-register itself, therefore the registration entry in the TachyonMaster database will need to be manually removed after troubleshooting. See Tachyon Architecture and Communication Ports.
Switch Host	The Switch Host service is a Windows service that manages local Switches

Term	Definition
	automatically starts each Switch and if a Switch stops, the Switch Host analyses the reason and attempt to restart it has a configuration file contains entries for one or more Switches has its own log file See Tachyon Architecture and Communication Ports.
System Principal	A system principal is a Tachyon user which cannot be modified in the Administration pages, and is assigned to a system role. The Server installation account is a system principal which is assigned to the Consumer Administrator, Security Administrator and Instruction Set Administrator system roles.
System Role	Tachyon roles which cannot be modified in the Administration pages. Tachyon users can be assigned to these roles. For more information about System and Custom roles, please refer to Roles and Securables. The following are built-in system roles. All Instructions Actioner All Instructions Approver All Instructions Questioner All Instructions Viewer Full Administrator Group Administrator Guaranteed State Administrator Guaranteed State Policy Assigner Guaranteed State User Installer Inventory Administrator Inventory User Tachyon System

Term	Definition
Tachyon Activity Record	This is a client feature, also known as inventory, previously known as Historic Data Capture. This feature captures data from a number of sources on the client device, encrypts and stores in compressed form on the client device. Raw and summarized (aggregated) data is stored and can be queried using instructions. See Tachyon client settings.
Tachyon client	Client features are provided by the 1E Client. The 1E Client includes client features and modules for other 1E products including Tachyon. Tachyon enables rapid response to instructions using the client, which supports the retrieval of information, running actions and device tagging. The client can also be extended to support additional features. The client connects to the Switch and the Background Channel. See Tachyon Architecture and Communication Ports.
Tachyon content	Tachyon content is: files (such as scripts) associated with a particular instruction via their which the client will download when it performs that instruction. extensibles (normally in the form of DLLs on Windows), which the client will download when it self-updates. This allows additional client functionality to be deployed. Tachyon content is downloaded on demand via the Background Channel.
1E Exchange	The 1E Exchange is a community platform and library of automation modules (Product Packs) for systems management created by 1E. Our goal for this community is to democratize the development and optimization of automation processes to simplify work. Leveraging SCALE, Tachyon's native language, and the Tachyon Platform we wish to grow into a community that builds powerful modules to serve each other's needs. https://tachyonexchange.1e.com/ You can browse the 1E Exchange but you will need a 1E Support login to download.

Term	Definition
Tachyon Instruction Management Studio (TIMS)	This feature is included in the Tachyon Toolkit. TIMS provides a user interface for developing and testing instructions using SCALE. It includes an isolated copy of the 1E Client so that you can develop instructions for that client version, independent of the 1E Client version that may be installed on your computer. By default TIMS and its Tachyon client run under the security context of the user that started it. To use the context of **Local System**, as used by a normal Tachyon client, you can start TIMS using PSexec. More information about TIMS is available in the Tachyon Community on the 1E Support Portal. TIMS should be used to edit and save Instruction Definition files.
Tachyon Instruction Runner	This feature is the graphical user interface part of the Configuration Manager Extensions which is included in the Tachyon Toolkit. It is a mini UI version of Explorer. It is an example of a Tachyon Consumer. It should not to be confused with the Tachyon Run Instruction utility available in the Tachyon Toolkit.
TachyonMaster database	The SQL Server database which contains: Configuration details of the Tachyon System instruction definitions and Instruction Sets Users (Principals) Permissions Roles Devices Audit log The configuration files for the following components contain SQL Connection strings for the TachyonMaster database. Core

Term	Definition
	Coordinator Workflow module Consumer API
Tachyon Master Stack	A Tachyon Master Stack is part of a Tachyon System. There is one Tachyon Master Stack that all the Tachyon Response Stacks communicate with. A Tachyon Master Stack contains the following components: SQL Server instance with TachyonMaster Database (local or remote/split) Consumer API Coordinator Explorer Authentication Registration
Tachyon Portal	The Tachyon Portal is the home page for Tachyon applications, which can be reached using the following URL: `https://<tachyon DNS Name FQDN>/Tachyon` where <tachyon DNS Name FQDN> is the one set up during the preparation phase, as described under the heading DNS Names. The following buttons appear on all application pages of the Tachyon Portal. The refresh button is used to refresh the contents of the page. The expand button toggles the size of the page inside the browser by hiding or showing the menu and main title bar.

Term	Definition
TachyonResponses database	The SQL Server database which contains: Responses
Tachyon Response Stacks	A Response Stack is part of a Tachyon System. This is where one or more Response Stacks talk back to a single Tachyon Master Stack. Multiple Response Stacks are necessary when additional Switches are required for scale, security or for geographic or other network reasons. Each Switch can handle 50000 devices, so each Response Stack can handle a maximum of 250000 devices. Each Response Stack has the following components: Switch Host Switches (up to 5, local or remote/split) Core SQL Server instance with Tachyon Responses database (local or remote/split) Background Channel A Response Stack will typically host Switches and Background Channel using the same DNS Alias.
Tachyon Role	Tachyon roles are used to implement Role-base access control (RBAC) and assign permissions to users and restrict access to areas of Explorer and ability to use instructions in Instruction Sets .The roles may be system roles or custom roles related to specific Instruction Sets .
Tachyon Run Instruction utility	This command-line utility is included in the Tachyon Toolkit and is targeted at 3rd party integration, and can be used by scripts. It is an example of a Tachyon Consumer. It is used by the Configuration Manager Extensions which is also available in the Tachyon Toolkit. More information about the Tachyon Run Instruction utility is available in the Tachyon Community on the 1E Support Portal.

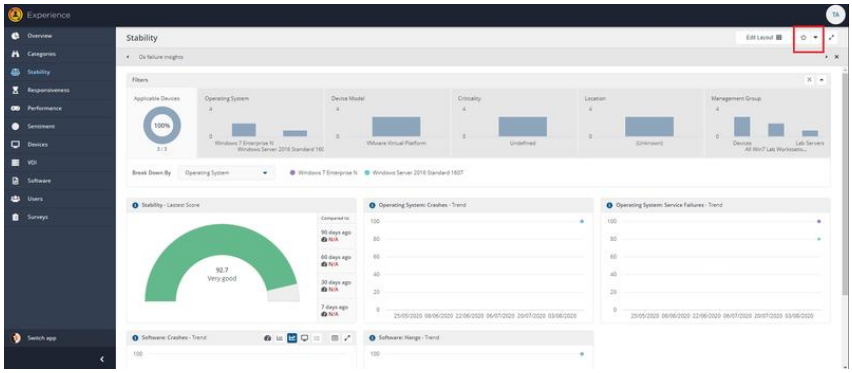
Term	Definition
Tachyon Server	A Tachyon Server is any server on which a Tachyon Server component is installed. The following are Tachyon Server components. Coordinator service (Instrumentation and Workflow modules) Switch Host Switches Website (including Explorer and Core) A Tachyon Server can have one or more Switches. See also single-server installation and single-Switch installation. See Tachyon Architecture and Communication Ports.
Tachyon Stack	There are two types of Stack: Master Stack and Response Stack. Every Tachyon system has a single **Master Stack**, which provides web services for Tachyon applications. Master Stack components are typically all installed on a single **Master Server**. Tachyon real-time features require **Response Stacks**, which are made up of one or more **Response Servers**. A **DMZ Server** is an example of a Response Server. Each Response Stack has at least one **Background Channel** for sharing resources, and a single **Core** component that supports an associated set of up to five **Switches**. Switches are the primary mechanism for rapidly requesting and retrieving responses from the **clients**. As each Switch can handle up to 50,000 devices there is a limit of 250,000 devices per Response Stack. Higher numbers can be achieved if you contact 1E for guidance. Switches may be local or remote to the other components in the Response Stack. **Databases** for Tachyon, Catalog, Content Distribution, Experience, SLA and BI, are installed on SQL Server database instance(s) that may also be local or remote to their respective Master and Response servers. It is also possible for multiple Response Stacks to share the same Responses database. The **Cube** used by Patch Success (SLA-BI) is installed on a local or remote SQL Server Analysis Services (SSAS) instance. For more details about architecture and components, please see Tachyon Architecture. Also see Architectural requirements.

Term	Definition
Tachyon System	At the top-most level, a Tachyon System consists of Tachyon Server components, grouped into Tachyon Stacks, and a set of clients that are deployed onto the devices that you want to manage. In addition, a system can have one or more Consumers (the built-in Consumer is Explorer). See Tachyon Architecture and Communication Ports. Tachyon System is also a system role, used by Tachyon for service an equivalent account to perform Tachyon system operations.
Tachyon Toolkit	The Tachyon Toolkit is a collection of the following tools, which can be installed on a Windows computer for use by a User who has appropriate permissions. Configuration Manager Extensions - this can be installed only on a computer that has already installed a Supported Platforms Tachyon Instruction Management Studio. .Tachyon Run Instruction utility The toolkit is available for download from the Tachyon Community in the 1E Support Portal. Documentation for installing and using the Toolkit will be available soon.
Tachyon User	A domain account that is authorized to access Explorer portal and/or the Tachyon Administration pages. Authorization is achieved by adding the AD account or group and assigning it to a role.
Tags	There are two types of tag: coverage tags and freeform tags. In Tachyon log files, these tags are also known a scopable and non-scopable tags.
Two-factor authentication	Also known as 2FA. See Two-factor authentication.
Website	The Tachyon Website hosts the following web applications:

Term	Definition
	Master: Admin Consumer - Consumer API CoreExternal Platform Tachyon Response and DMZ: Background - Background Channel Core Optional applications on Master: ContentDistrbution Experience The Website has an HTTP binding and HTTPS binding. The HTTP binding uses the server's hostname FQDN as a host header, and is used only by SLA components - please refer to Removing the HTTP binding from the Tachyon website One or more HTTPS bindings - these use the Tachyon Web Server certificate, the server's DNS Alias as the host name, and has SNI enabled. See Tachyon Architecture and Communication Ports.
Workflow commands	Workflow commands determine how the Coordinator Workflow module processes an instruction, particularly in terms of the permissions required to run the instruction.

5 Tachyon Experience

Tachyon Experience helps you visualize your end-users' experience of IT service delivery across your enterprise.



5.1 Introducing Tachyon Experience

Tachyon Experience helps you visualize your end-users' experience of IT service delivery across your enterprise. It is centered around the experience score, which is based on metrics covering four categories:

Stability - derived from the frequency of operating system and software crashes, hangs and service failures.

Responsiveness - based on the speed of operating system startup, system resource creation and availability.

Performance - a weighted indication of load and throughput for device processor, memory and disk resources.

Sentiment - an aggregated measurement of users feelings or opinions of their device's performance, stability and responsiveness based on user surveys.

5.1.1 Tachyon Experience Features

5.1.1.1 The Tachyon Experience Overview page

This page shows a dashboard of the Experience score.

> **Note**
>
> For more information on the **Overview** page please refer to:

Overview page.

5.1.1.2 Categories page

The Categories page shows a dashboard of the Stability, Responsiveness, Performance and Sentiment scores.

> **Note**
>
> For more information on the **Categories page** please refer to:

Categories page

5.1.1.3 Stability page

The Stability page shows a dashboard of the Stability score.

Note

For more information on the **Stability page** please refer to:

Stability page.

5.1.1.4 Responsiveness page

The Responsiveness page shows a dashboard of the Responsiveness score.

Note

For more information on the **Responsiveness page** please refer to:

Responsiveness page.

5.1.1.5 Performance page

The Performance page shows a dashboard of the Performance score.

Note

For more information on the **Performance page** please refer to:

Performance page.

5.1.1.6 Sentiment page

The Sentiment page shows a dashboard of the Sentiment score.

Note

For more information on the **Sentiment page** please refer to:

Sentiment page

5.1.1.7 Devices page

The Devices page lists all the devices that are reporting into Experience.

Note

For more information on the **Devices page** please refer to:

Devices page.

5.1.1.8 Software page

The Software page shows all the software titles that are installed in the entire environment.

Note

For more information on the **Software page** please refer to:

Software page.

5.1.1.9 Users page

The Users page shows metric data for the users in the entire environment.

Note

For more information on the **Users page** please refer to:

Users page

5.1.1.10 Surveys page

The Surveys page shows all the surveys created in the entire environment, and allows for surveys to be created, cloned, deleted, enabled, disabled, and assigned to management groups.

Note

For more information on the **Surveys page** please refer to:

User Engagement page.

5.1.1.11 Filters bar

The Filters bar is at the top of each page and is used to change the view of the tiles on that page.

Note

For more information on the **Filters bar** please refer to:

Filters.

5.1.1.12 Tile buttons

There are a set of Tile Buttons on the Stability, Responsiveness, and Performance pages, they can be used to show different views on the tiles or open other windows for details.

Note

For more information on the **Tile Buttons** please refer to:

Tile Buttons.

5.2 Implementing Tachyon Experience

Everything you need to know about getting Experience installed and running in your network. This section is structured in a way that leads you through the three phases of a typical implementation project.

Design, including requirements

Install

Verify.

5.2.1 Requirements

What you will need to prepare in advance of implementing a Tachyon Server in your network. Typically, these are tasks that may take some time to organize, depending on how your organization works.

You will already have installed Experience using Tachyon Setup. To do this, you required the following:

A full installation of Tachyon including deployments of clients

Experience must be a licensed and enabled consumer

Guaranteed State must be a licensed and enabled consumer

The Inventory module of the 1E Client must be enabled on the devices.

> **Note**
>
> Experience and Guaranteed State do not need to be licensed to install Experience, but they must be licensed to use Experience. See Tachyon License file details.
>
> Guaranteed State does not need to be configured to install or enable Experience, nor do any **Guaranteed State policies** need to be created. For customers that are not using Guaranteed State in their environment, the **Deploy** button in Guaranteed State must be clicked one time to allow **Experience policies** to be deployed and enabled on the devices.
>
> **Note**
>
> Experience does not require SQL Server Analysis Server (SSAS) because it no longer uses a Cube. It continues to require SQL Server for its database.

5.2.1.1 Supported Platforms

Please refer to:

Planning for Tachyon

Planning for 1E Client.

5.2.1.2 Active Directory and Tachyon users

A **domain account** or **security group** that is a **Tachyon user** is required with the following Tachyon roles applied, depending on what you want to do with Experience.

To use Experience, you must assign the role:

Experience Viewers

To view Experience Surveys and Survey responses you must additionally assign the role:

Survey Viewer

To create Surveys, you must additionally assign the following roles:

Event Subscription Administrators

Event Subscription Viewers

Survey Administrators (also includes the Survey Viewer role).

To initially deploy a policy to clients so that they report information back to Experience you must assign the role:

Guaranteed State Administrators.

These roles do not have to be assigned to the same Tachyon user. Enabling (deploying) Experience policies in Guaranteed State is a one-time task that should be performed before using Experience, please refer to Installing Experience for more information.

5.2.1.3 Tachyon License details for Experience

Ensure your Tachyon License file has the Experience consumer enabled. Please contact 1E in order to obtain a license for Tachyon Experience.

You can view your Tachyon license details using either of the following methods:

in the Tachyon Portal, navigate to **Settings→Configuration→License information**, look in the **Products** section and expand **Features** and instructions items

in the license file **Tachyon.lic** found in **C:\ProgramData\1E\Licensing**

If this section does not exist, then the Experience application will not be installed during the Tachyon installation. You may have an old version of Tachyon, or your license needs to be updated.

```
</Feature>
     <Feature name="Experience">
       <Consumer name="Experience" enable="on"> </Consumer>
```

5.2.2 Installing Experience

Warning

You should select to install Experience at the same time as installing Tachyon, even if your license file does not include Experience. As the only way to install it post-Tachyon installation is to uninstall and then re-install your Tachyon system.

Without a license present, after installation, the Experience application will be installed but not visible in the Tachyon Portal. When you get and activate a new Tachyon License file with Experience included, Experience will then become visible in the Tachyon Portal.

Note

Tachyon Experience is only for Windows Devices.

Tachyon Setup automatically configures Experience, as long as your Tachyon license file enables Experience.

After the installation of Tachyon is complete you will need to add at least one user in Tachyon to the **Experience Viewers** role.

5.2.2.1 Installing Tachyon Experience

Tachyon Experience is an application installed using Tachyon Setup. Please refer to Tachyon Setup for more details.

5.2.2.2 Post-Installation

Experience deploys the following types of policies:

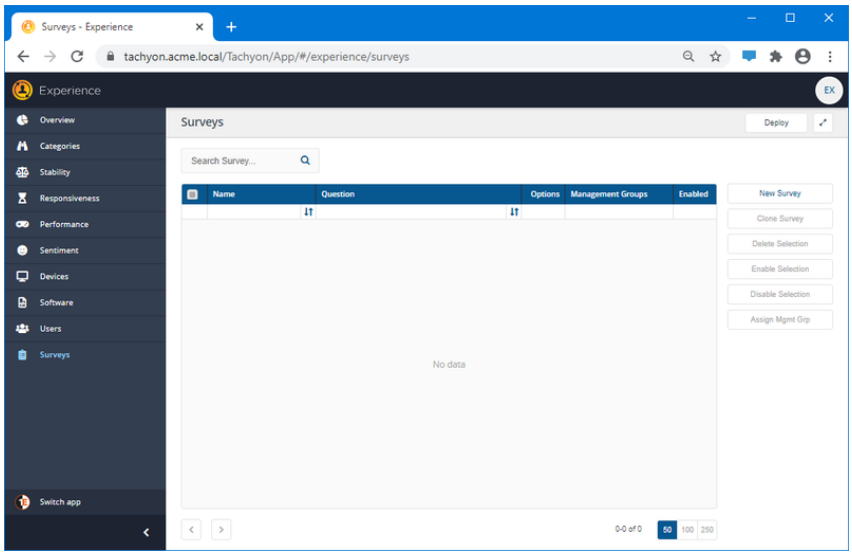
Metrics - these are built-in, and cover Stability, Responsiveness, Performance and Sentiment categories

Surveys - these are optional User Sentiment and General Purpose surveys

To kick start gathering metrics, you must deploy Experience policies.

Open Experience as a user with the **Survey Administrators** role, navigate to the **Surveys** page, and click the **Deploy** button, even if you are not intending to implement any Surveys in your environment, or you have not deployed 1E Client.

This step only needs to be done once. This will use the default **All Devices** Management Group and send the Experience policies to all devices that are reporting into Tachyon. In this release of Experience there is no ability to exclude any devices and may deploy the policies to mission critical devices, including servers.



5.2.3 Verifying

Basic verification tests that cover a single-server installation of Tachyon Server. These tests only cover Tachyon and do not verify the configuration of 1E client modules with other 1E products.

Note

> Please ensure you complete all verification tests. They not only confirm your system is operational, but they also introduce you to concepts and tasks that you will use later when using Tachyon.

These tests should be run in series. They start with basic server checks, then testing 1E Clients, and finally, use the verification instructions from the **1E-TachyonPlatform** product pack to do end-to-end tests that confirm all components are working. Depending on the decisions you have made during the design phase of your implementation, you may need additional tests to verify your Tachyon implementation.

To run these tests, you need:

Tachyon Server installed with Tachyon Experience configured.

At least one test device on which the 1E Client has been installed.

The Tachyon platform has already been verified following the Verifying page which requires a Tachyon User with various administration rights.

Access to the SQL Server database instance and SQL Server Analysis Services instance to check the Experience database.

To complete the test below requires a Tachyon User assigned to **Experience Administrators** role.

5.2.3.1 Verify Tachyon and Experience installation

Ref	Test	Expected	Remediation
TCNE01	Check the configuration of the Experience Consumer	In **Settings - Configuration - Consumers** **Experience** should be licensed and Enabled	Check your **Tachyon** License file for the Experience consumer **Enable = on**. If this is not present or not enabled, contact SalesOps@1E.com for a new license file.
TCNE02	Check the TachyonExperience Database	Open **SQL Management Studio**. Connect to the *Database Engine* and expand Databases - TachyonExperience should be listed.	

5.3 Using Tachyon Experience

Tachyon Experience helps you visualize your end-users' experience of IT service delivery across your enterprise.

It is centered around the experience score, which is based on metrics that cover four categories:

Stability - derived from the frequency of operating system and software crashes, hangs and service failures.

Responsiveness - based on the speed of operating system startup, system resource creation and availability.

Performance - a weighted indication of load and throughput for device processor, memory and disk resources.

Sentiment - an aggregated measurement of users feelings or opinions of their device's performance, stability and responsiveness based on user surveys.

> **Note**
>
> Experience can be reached directly using the following URL:
>
> `https://<Tachyon DNS Name FQDN>/Tachyon/App/#/Experience`
>
> where <Tachyon DNS Name FQDN> is the one set up during the preparation phase, as described in DNS Names.

5.3.1 Personas

Tachyon Experience was built with the following three personas in mind, these personas are an example of typical users:

End User Computing Manager (EUC Manager)

Level 1/Level 2 Service Desk Analysts

Level 3 Service Desk Analysts.

The pages in the Using Experience section show the different ways that each of these personas use Experience to achieve specific goals related to their role.

5.3.2 Monitoring and investigating enterprise-wide experience

This scenario outlines a typical day for an **end-user computing (EUC) manager**. It shows how they use Tachyon Experience to monitor their overall Experience score, drill-down to view details and finally pinpoint the devices with the worst scores - so they can take action to improve their end-users' experience.

5.3.2.1 A typical day for the EUC Manager

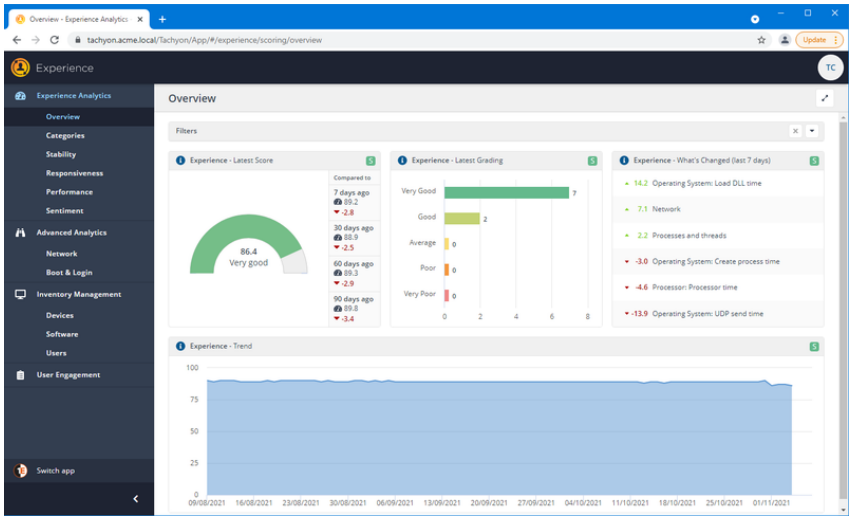
The EUC Manager is concerned with how the network performs for their end-users. They are constantly looking to improve stability, responsiveness and performance so that their end users are happier with the IT Service they receive.

5.3.2.1.1 Looking at the Experience Overview page

To start their day, the EUC manager loads up their Experience application and looks at the **Overview** page. Here they check the latest Experience score to see how their network is doing overall right now. The score of **86.4** is looking good, but is there anything more they can do to improve service? Checking the **Compared to** section of the **Experience Latest Score** tile, they can

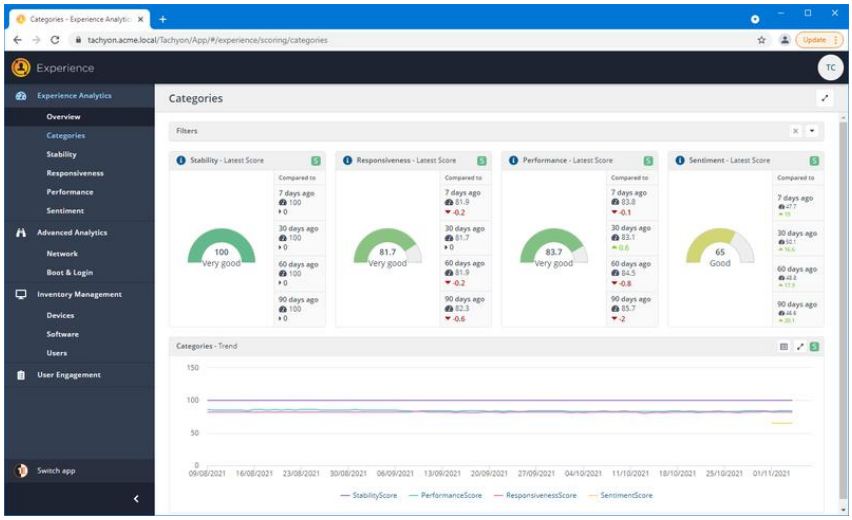
see that in general the Latest Score is moderately down against the results from 7, 30, 60 and 90 days ago. The EUC manager is interested in how the scores changed, particularly if the scores are decreasing - since this may be indicative of a problem that needs action.

So is there anything in the makeup of the latest Experience score that merits investigation?



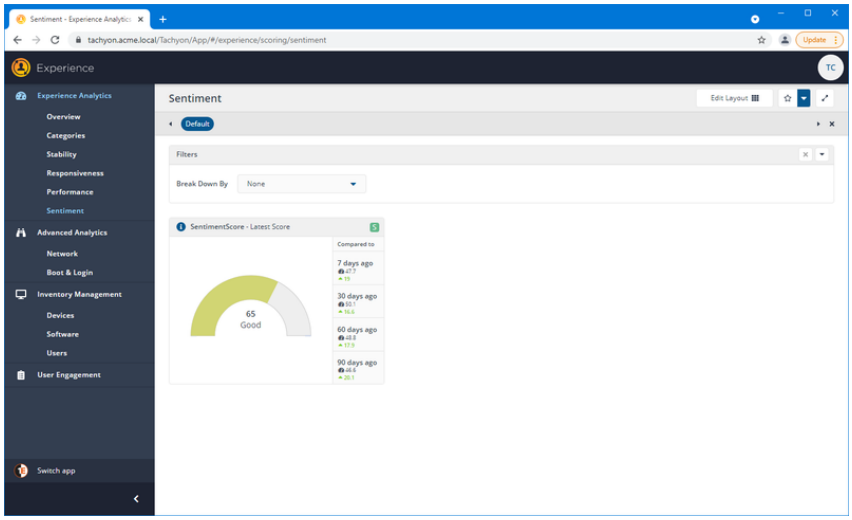
5.3.2.1.2 Looking at the constituent scores

Clicking on the **Experience - Latest Score** tile drills down to display the constituent scores on the **Categories** page. Here the EUC manager checks the **Stability**, **Responsiveness**, **Performance** and **Sentiment** scores. Scanning across, the **Sentiment - Latest Score** of **65** is good, but lower than the others. The comparisons with 7, 30, 60 and 90 days ago shows there has been an overall improvement - but the fact that the score is the lowest, is there still an issue that may be affecting end-user sentiment?



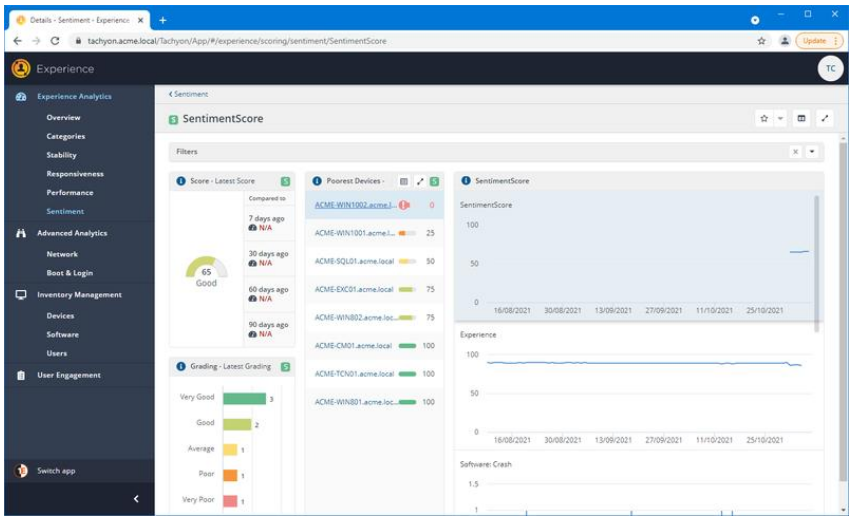
5.3.2.1.3 Investigating Sentiment

Clicking on the **Sentiment - Latest Score** tile drills down to the **Sentiment** page, here the EUC manager can drill down again by clicking on the same tile.



5.3.2.1.4 Reviewing the Poorest Devices

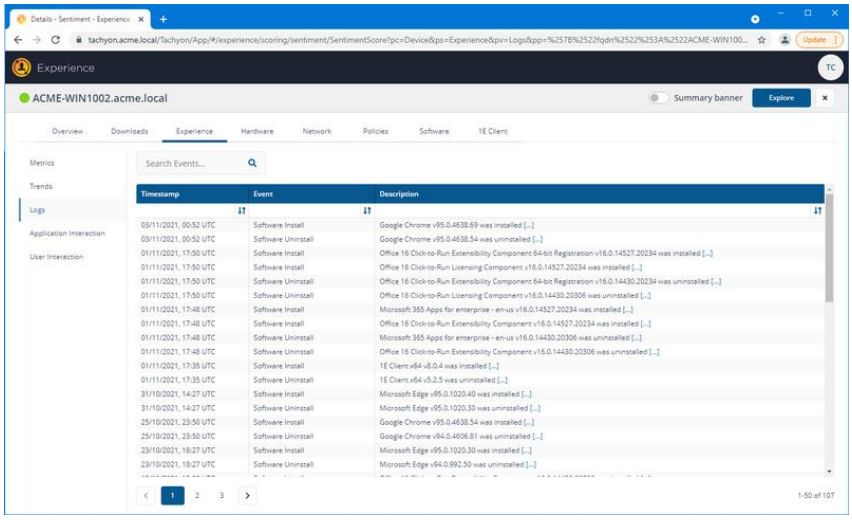
On the **Sentiment** page, the EUC manager scans the **Poorest Devices** tile. The items in the **Poorest Devices** tile are ordered from the poorest to the best performance. They see that the topmost item seems to have a much lower score than the others, so they decide to take a closer look.



5.3.2.1.5 Zooming in on the lowest score

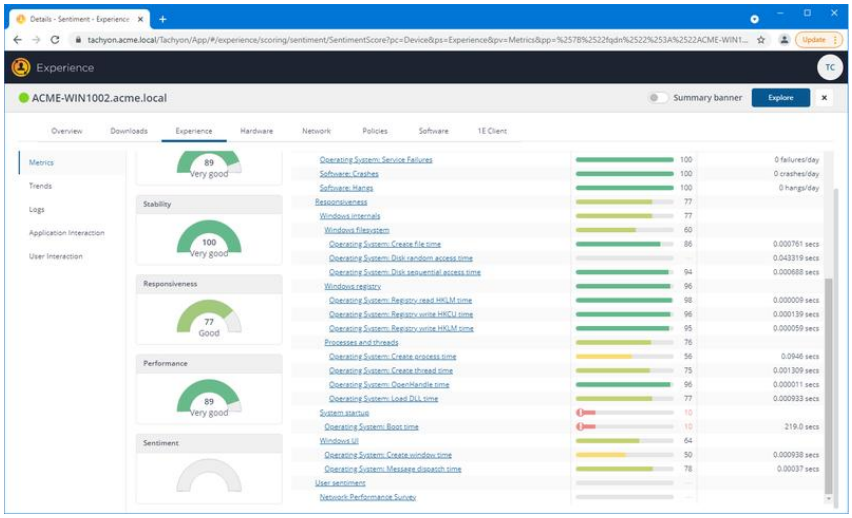
Clicking on the name link for the device in the **Poorest Devices** tile, displays the **Device Details** for the selected device. This view displays information for the device that is derived from all the Tachyon applications you are licensed for, as well as displaying real-time information that is gathered immediately from the device. This information is gathered by instructions that are automatically triggered when displaying a tab or chart and show you the current status for the device.

When navigating from the **Poorest Devices** tile, **Device Details** initially opens on the **Logs** panel, as seen in the picture. Here, the EUC manager can view information about the device that is retrieved from the device logs.



5.3.2.1.6 Investigating the Metrics for a particular device

Clicking on the **Metrics** table the EUC manager scrolls down and sees that there are issues reported for the device related to the **System** startup, specifically the **Operating System Boot time** - where the score is only **10**. They can also see that this is affecting the **User sentiment** for the device. At this point they could click the **Explore** button and investigate the issue further using Tachyon's real-time system, or assign the task to one of their IT team. Whichever they choose, they are now ready to take action.



5.3.3 Focusing on specific device experience

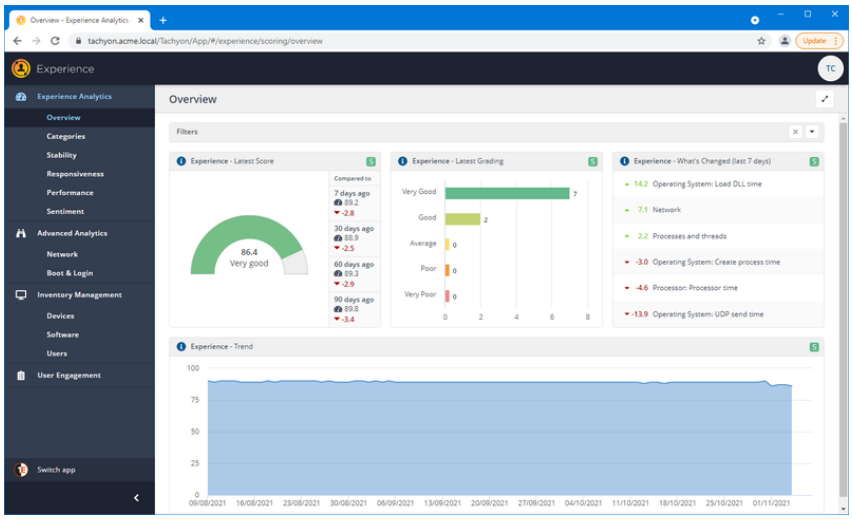
In this scenario we show how a **level 1 helpdesk analyst** would use Experience and Explorer together as part of their daily routine. A level 1 helpdesk analyst usually focuses on a specific device at any particular time. Here the user of a device is on the phone with the analyst describing the symptoms. Experience will enable the analyst to troubleshoot primary causes, and Explorer will let them interact directly with the device to further investigate and resolve the issue.

5.3.3.1 A case for the level 1 helpdesk analyst

An end-user, **Gary Hayes**, calls the IT helpline, gets put through to the level 1 helpdesk analyst, and reports that their device is running slowly.

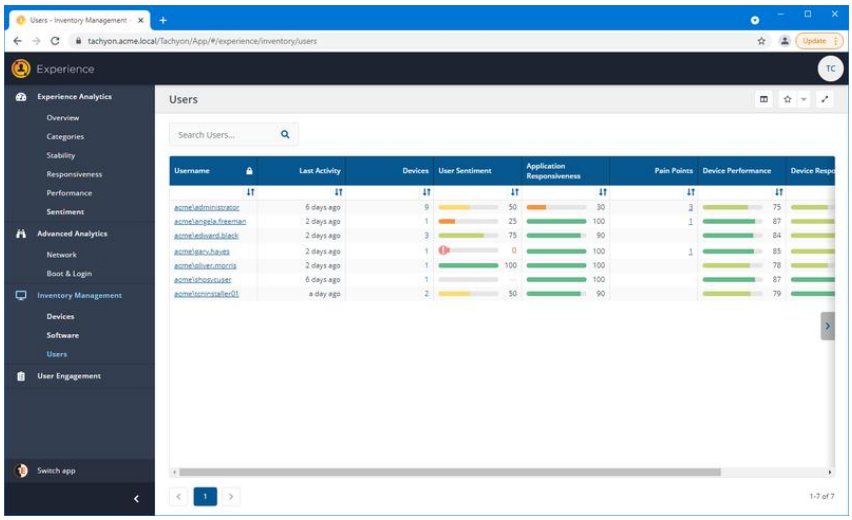
5.3.3.1.1 Tracking down the issues in real-time

While the user is on the phone, the Level 1 helpdesk analyst checks the **Experience** tab they have open in their browser.



5.3.3.1.2 Getting information via the Users page

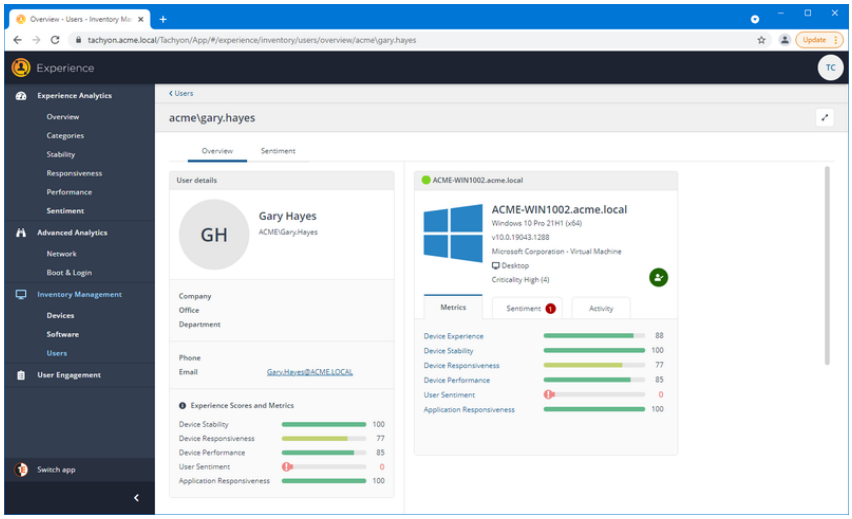
They navigate to the **Experience→Inventory Management→Users** page, which provides an overview of all the users currently known to Tachyon. To check the device the user is working on, they click on their link in the **Username** column.



5.3.3.1.3 Information on the devices associated with the user

The user's page shows all the devices known to be associated with the user by Tachyon. In this example it shows that **Gary Hayes** is associated with the device **ACME-WIN1002.acme.local**. The

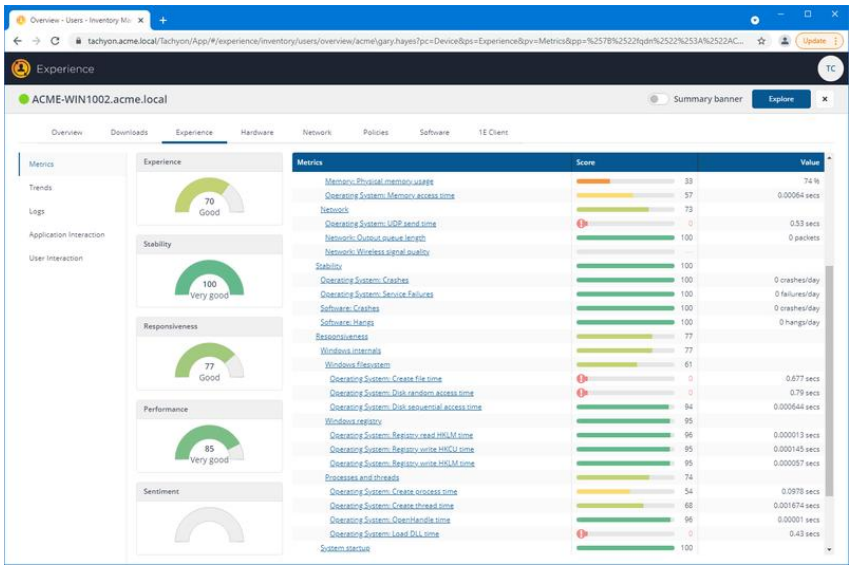
analyst can also see that this user has given some negative **User Sentiment** feedback on this device.



5.3.3.1.4 Investigating the device

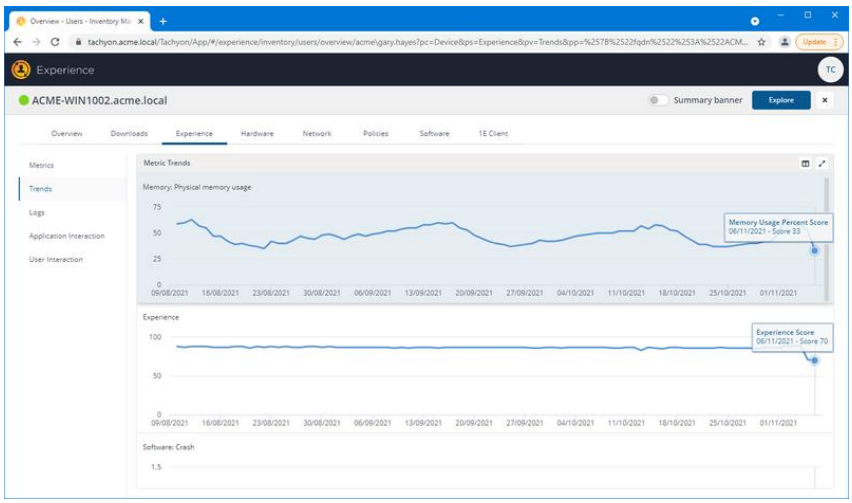
Clicking on the panel for the device shows its **Device View**. Here on the left of the pane you can see the summaries for the device's overall **Experience**, **Stability**, **Responsiveness**, **Performance** and **Sentiment** scores. On the right, you can see the **Metrics** that have been captured for the device.

Scrolling down through the metrics the analyst can see critical values for the **Operating System: UDP send time**, **Operating System: Create file time**, **Operating System: Disk random access time**, and **Operating System: Load DLL time** metrics. The **Memory: Physical memory usage** metric also has a low score, perhaps there's a memory related issue that is causing the other issues and slowing the device down.



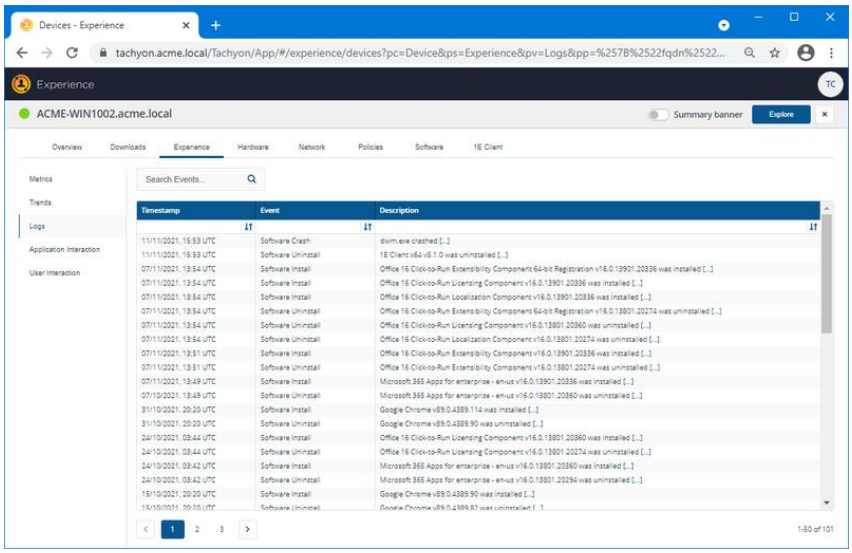
5.3.3.1.5 Memory usage trends, a possible cause?

Clicking on the link for the metric drills down show to show the **Trends** for that parameter. Here, the analyst can see that the general trend (even though the measurement has only been taken for just a few days) is headed downwards. So could be worth investigating more, the analyst makes a note and continues investigating.



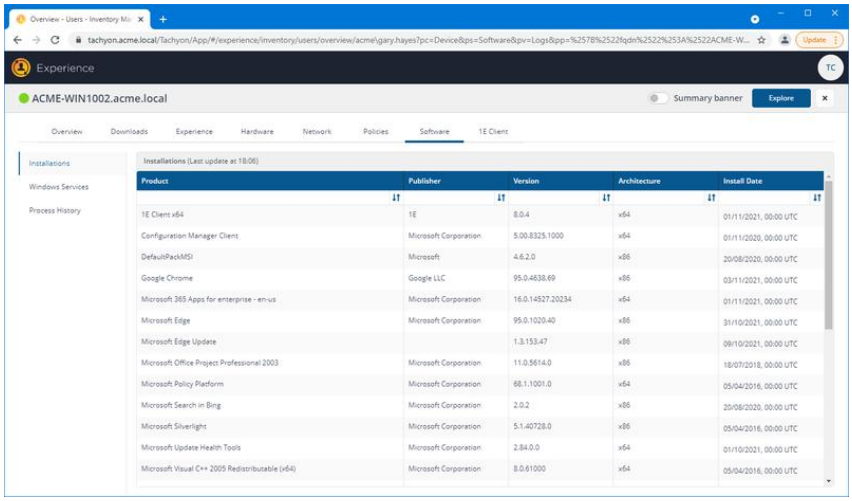
5.3.3.1.6 Checking the Event log

Clicking on the **Logs** tab displays any significant events that have been stored in the Event log on the device. In this example, the analyst can see that there's been one crash - which might or might not be significant, but worth noticing at least.



5.3.3.1.7 Checking the Software installed on the device

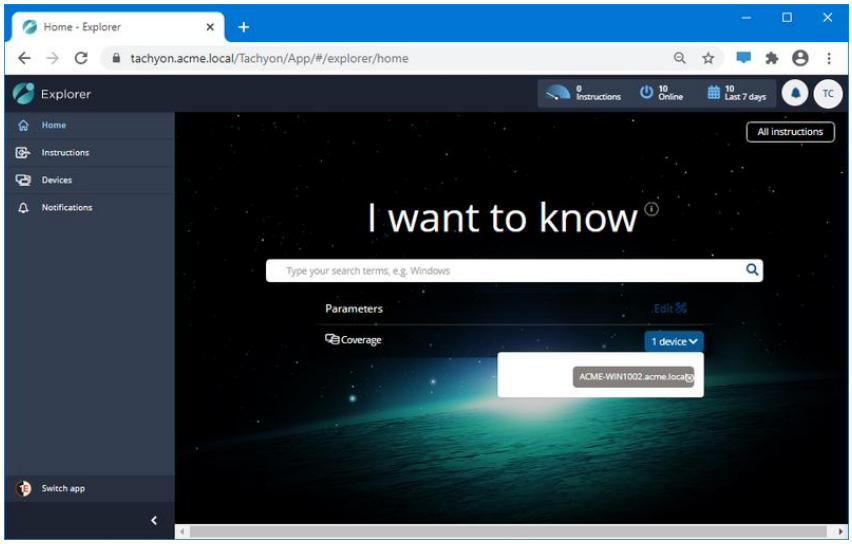
Clicking on the **Software** tab displays all the software reported as being installed on the device. This may be useful information in general, but doesn't show anything out of the ordinary as far as the analyst can tell.



5.3.3.1.8 Further investigating the device using Explorer

Having reviewed all the information retrieved for the device by the 1E Client, a reasonable next step for the analyst is to query the device directly to get some extra info that's not captured by default. They have an idea that memory issues might be causing the slowdown and something they would like to check is what processes are running on the device.

Clicking on the **Explore** button in the **Device View** navigates to the Explorer application, assuming that the analyst has the required Questioner and Actioner permissions. In the Explorer application the analyst can confirm that the Coverage for the question is constrained to the **ACME-WIN1002** device. This means that the instruction they select will be run on that target device.

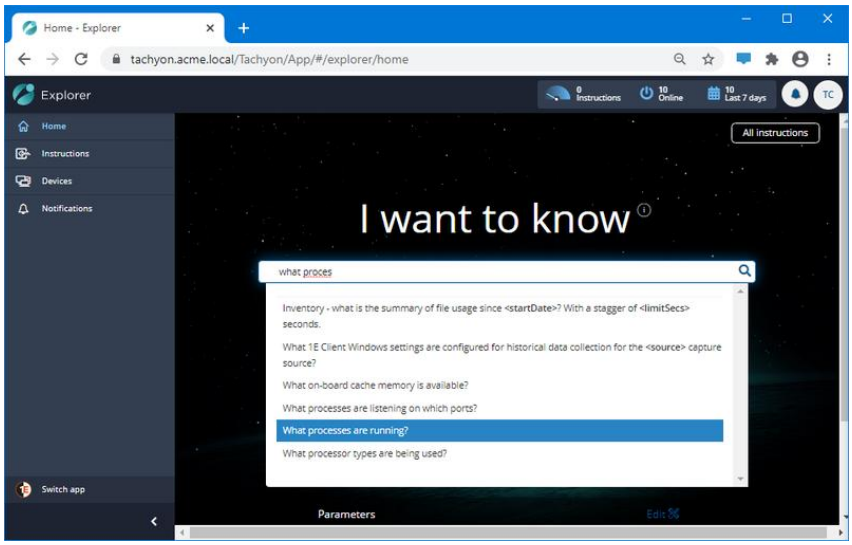


5.3.3.1.9 Finding out what processes are running on the device

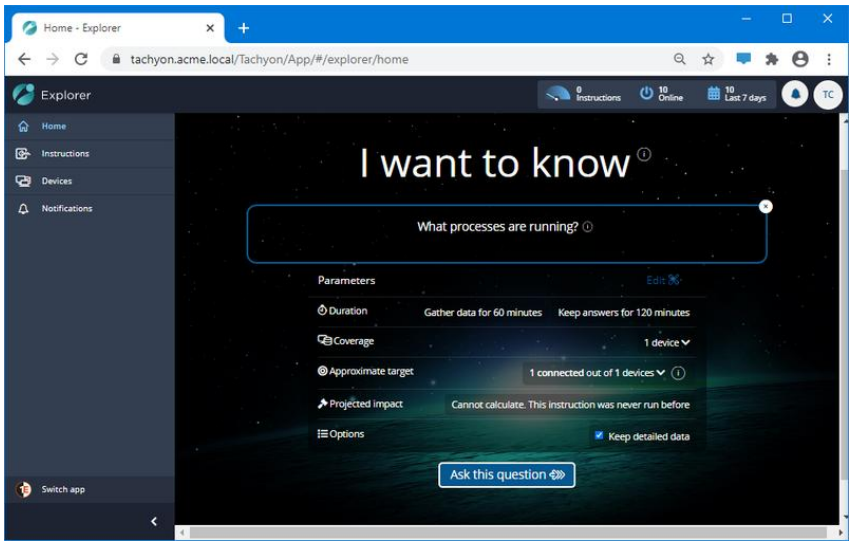
The analyst starts typing **What proces** into the search field, as they know that's involved in the instruction text. They could have typed **process** or **processes** if they were less sure and just wanted to find all the instructions related to processes.

When the list of suggested matches comes back the analyst selects: **What processes are running?**

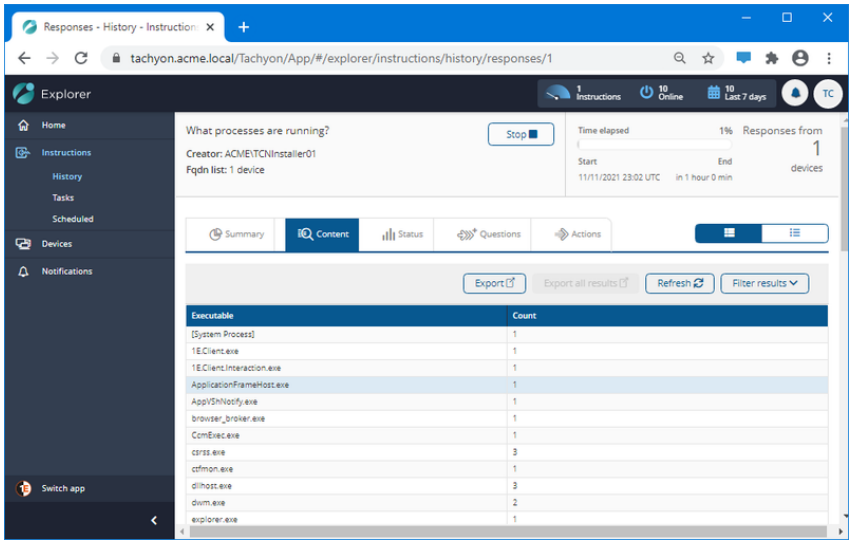
There is also a useful product pack on the Tachyon Exchange called: Windows Process Management which includes instructions to give a verbose listing of all running processes (List running process details) and another is List resource consumption details to identify what is impacting the end-user experience.



The instruction is loaded into the Explorer home. All the analyst needs to do is click **Ask this question** to fire it off to the selected device.

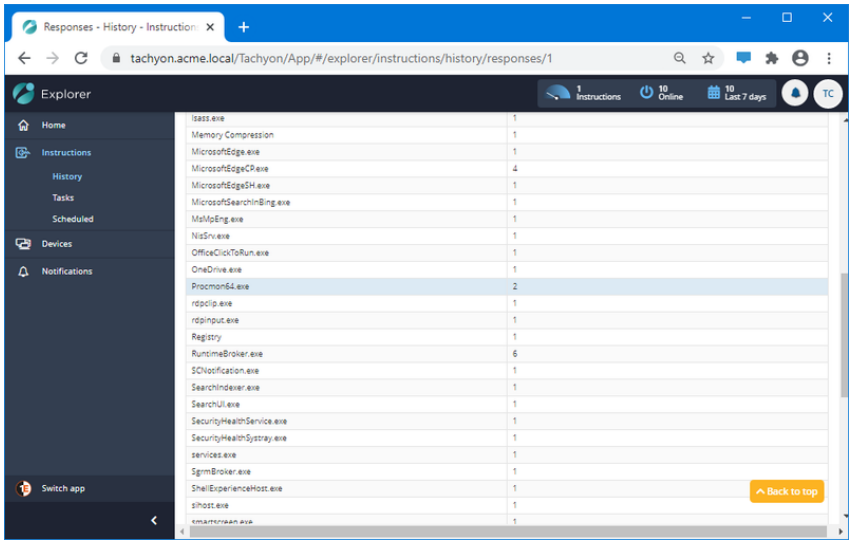


The list of running processes comes back almost immediately.



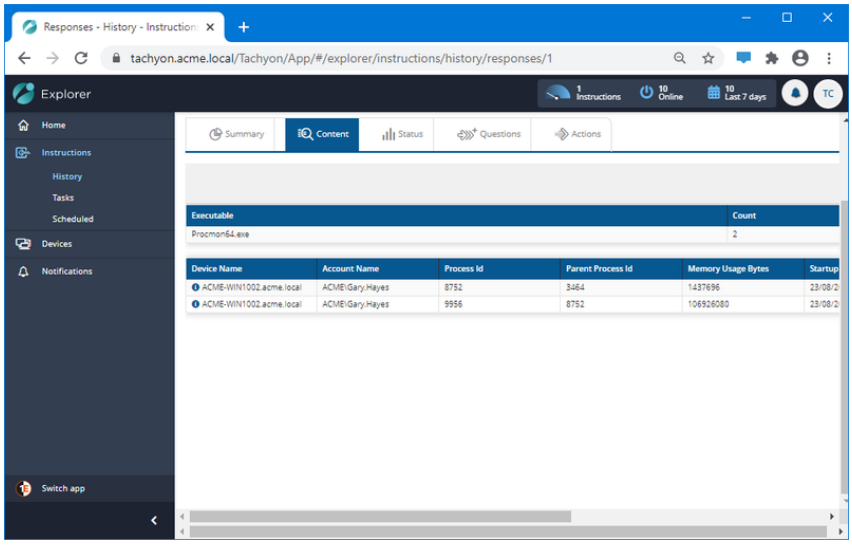
5.3.3.1.10 A possible culprit process?

The analyst scrolls down through the list until they find one that might be a cause of the issue. **Procmon64.exe** is a good candidate as it can use up large amounts of memory and may still be running even if the front-end is not being displayed. In this instance the effect could be exaggerated by the fact that there are two copies of this process running.



5.3.3.1.11 Details reveal that the process is using large amounts of memory

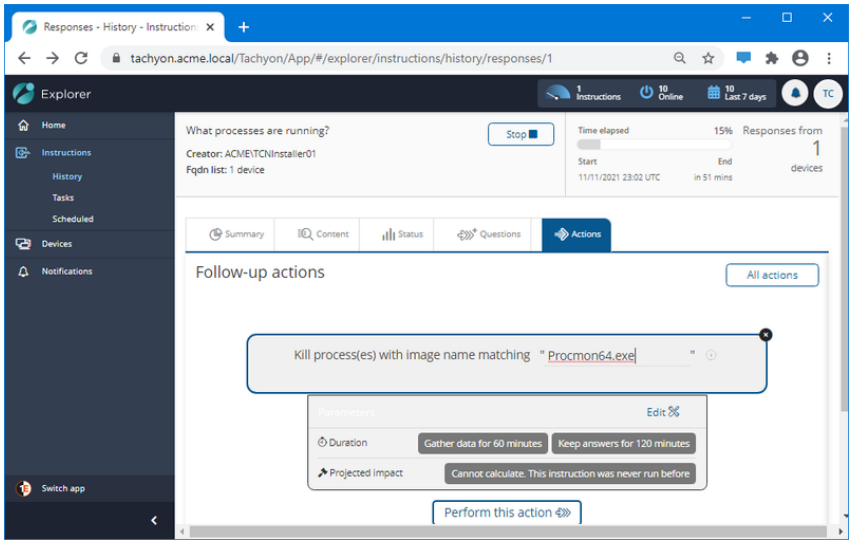
Clicking on the number link in the **Procmon64.exe** row in the results table, displays details for those results. Here the analyst can see that the pair of processes running are consuming a lot of memory. If the user is sufficiently skilled we can check over the phone whether the Procmon interface is visible and therefore these are just background processes that are consuming resources. Now it's time to kill the processes and hopefully return the device to its proper state.



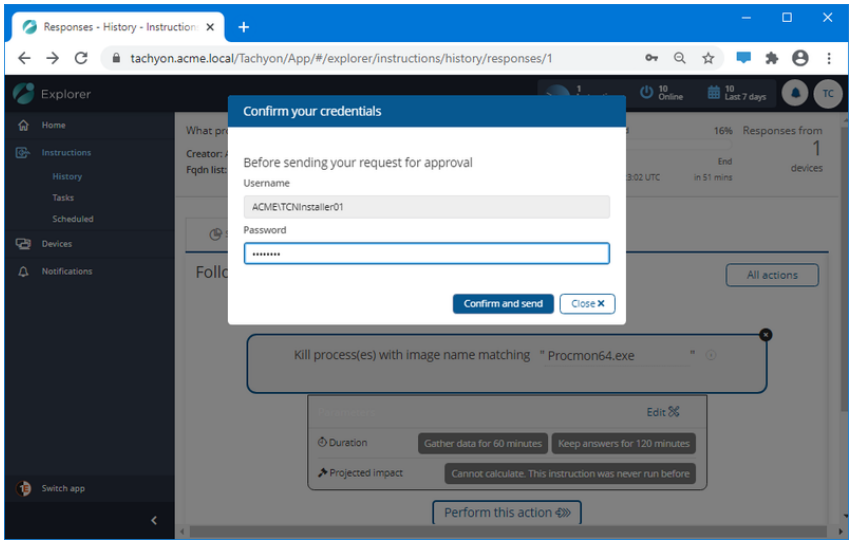
5.3.3.1.12 Resolving the issue

You can kill a running process from Tachyon using the **Kill process(es) with image name matching...** action. The analyst selects to run a **Follow-up action**, by clicking on the **Actions** tab on the results page, searching for the kill action and then filling out the image name parameter with the text **Procmon64.exe**.

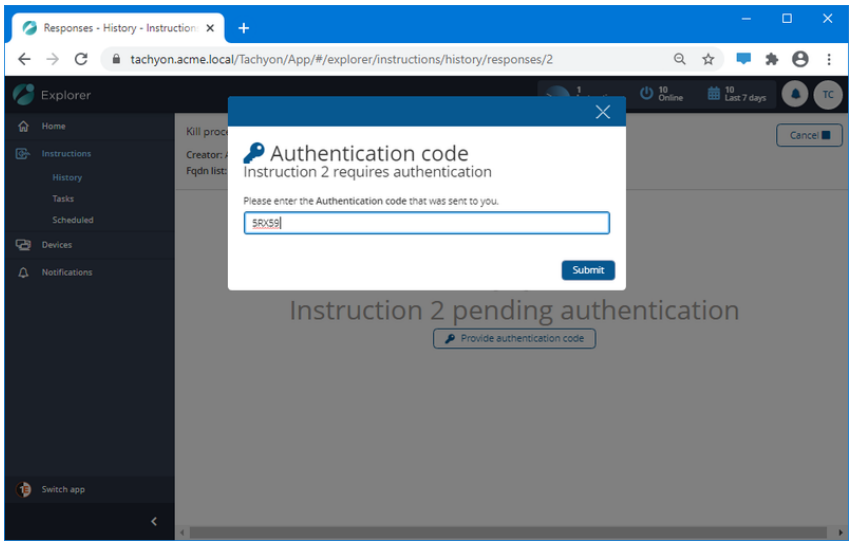
They run the action this way because the scope has already been set to the right device.



After clicking **Perform this action** Tachyon puts them through the authentication and approval process. First they have to confirm their credentials.



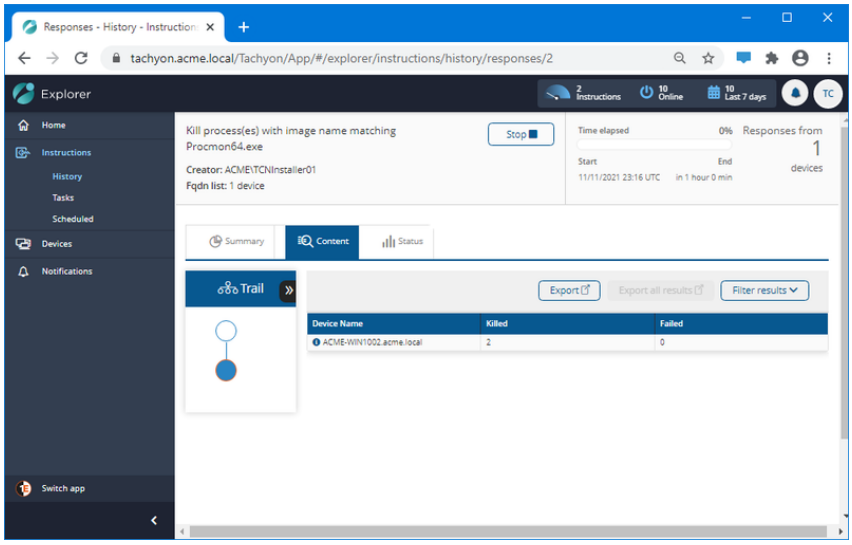
Then they have to supply the **Authentication code** that has been emailed to them.



The action must then be approved by another user with Approver permissions. When all this is done, the action runs and the **Procmon64.exe** processes are killed on that device. Hopefully that was the cause of the problem, the analyst goes back to the user on the phone and gets them to confirm that things have improved.

5.3.3.1.13 In conclusion

This is a simple scenario that shows how Experience can be used to detect a problem and Explorer can be used to investigate and resolve the problem. It shows how the two applications working together can be used as part of the analyst's process for solving end-user device issues reported to the IT helpline.



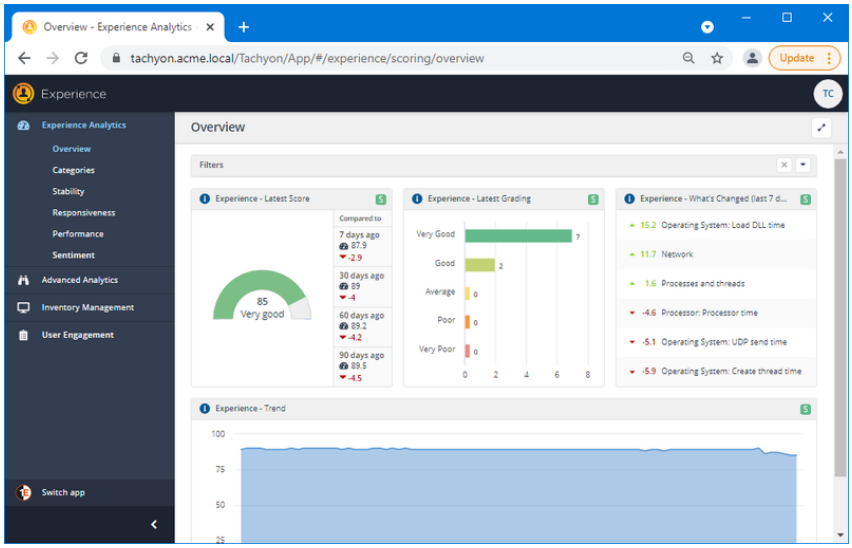
5.3.4 Investigating enterprise-wide software experience

The scenario described here covers a typical Experience journey for a **level 3 support engineer**. Typically, the Level 3 support engineer focuses on resolving global or wide-spread issues. We show how they would look for the applications in the environment that are crashing most often, and then how they would investigate the impacted devices to find a resolution.

5.3.4.1 How a level 3 support engineer uses Experience to investigate enterprise-wide software issues

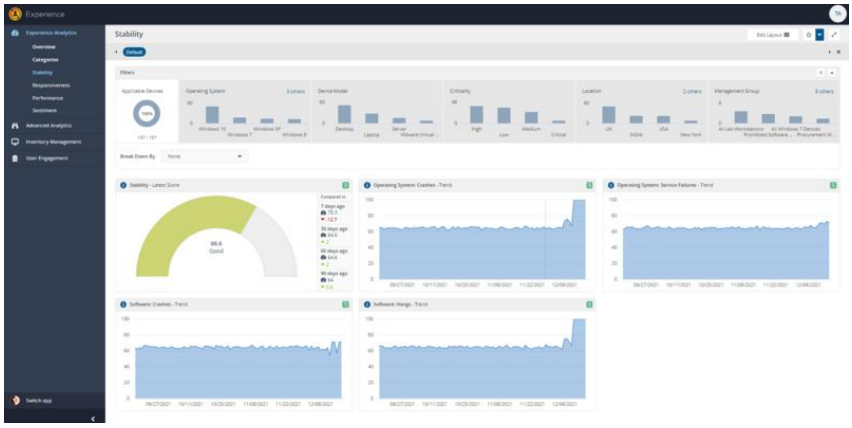
In this scenario the level 3 support engineer is performing a routine check to see if there are any devices where software crashes have been experienced. To do this they make use of Tachyon Experience to view the software installed across all the 1E Client enabled devices in their network and then focus on the ones that have the most crashes. Having found some problems they then use Explorer to run further questions on any affected devices to help pinpoint the exact issue and find a possible solution.

To start their journey, the engineer opens Experience in a browser. It has been reported that users are experiencing software crashes, and so from the Overview page the engineer navigates to the Stability page.



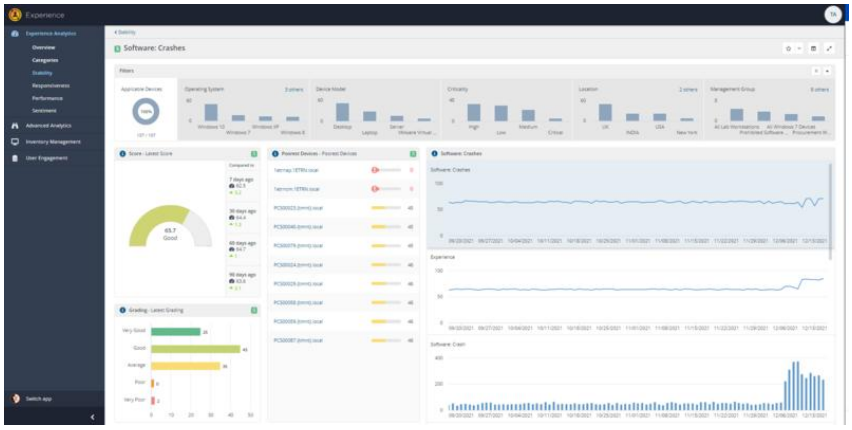
5.3.4.1.1 Navigating to the Stability page

They then navigate to the **Experience → Stability** page. Here they can see tiles that show how the environment is behaving with respect to Operating System Crashes, and Service Failures trends, and also the Software Crashes and Hang trends. They could use the filters along the top of the page to filter the results being shown.



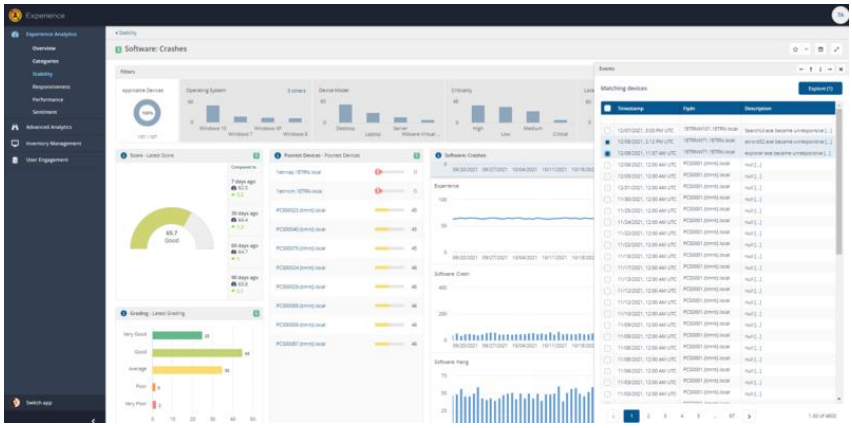
5.3.4.1.2 Viewing the Software Crashes page

To carry out the investigation they then click on the **Software Crashes: Trend** tile and are taken to the Software: Crashes page, they now need to locate any event that is causing the score to decrease, and so click on the bar graph showing the Software Crash information which is the third tile on the right, and the events pane is displayed.



From the events pane they are able to view what software has crashed and which devices have been affected, selecting the offending software enables the Explore button, and clicking this will open Tachyon Explorer, which if the user has either All Instructions Actioner, or All Instructions Questioner, they are then able to run instructions against the device to validate whether the offending software or process is still installed. A useful instruction for this is List Software Installations, which can be pre filtered with the product name if you have it, or if not clear then use the Get the count of a process "processname" that has been started in the last "x" days which is available from the Tachyon Exchange, which is available here:

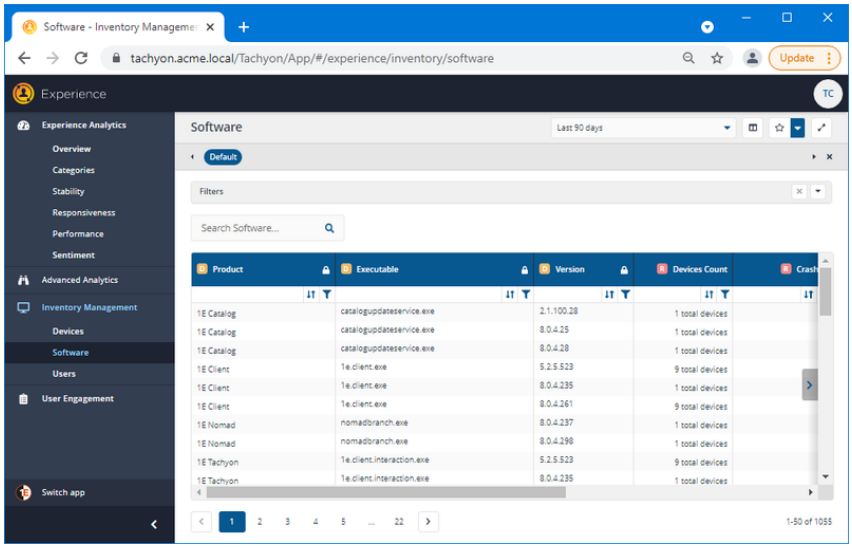
https://tachyonexchange.1e.com/product-packs/windows-process-management/



Alternatively the engineer could follow the path below

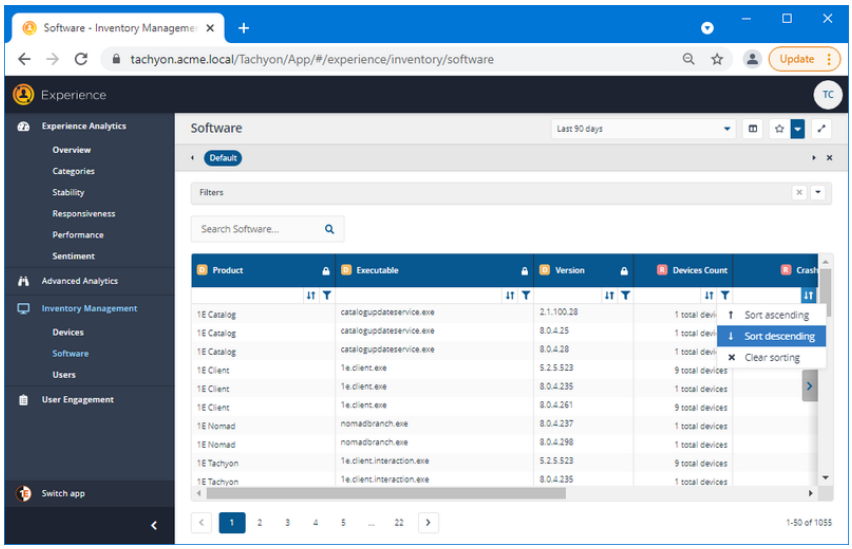
5.3.4.1.3 Navigating to the Software page

They navigate to the **Experience→Software** page. Here they can see all the software that is installed in the environment and a count of the devices that have each title.

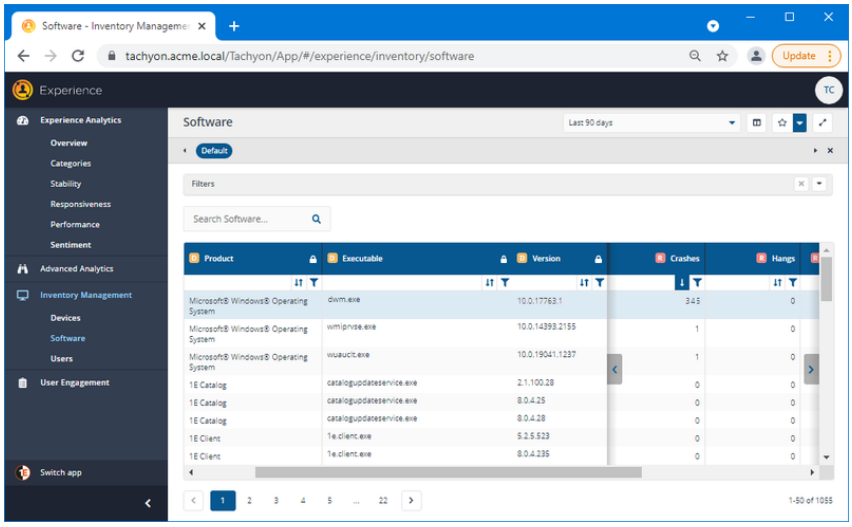


5.3.4.1.4 Sorting the Software table to show the software with the most crashes

To investigate software crashes the engineer clicks on the sort icon on the **Crashes** column and selects to **Sort descending**, which will bring the software with the most crashes to the top of the table.

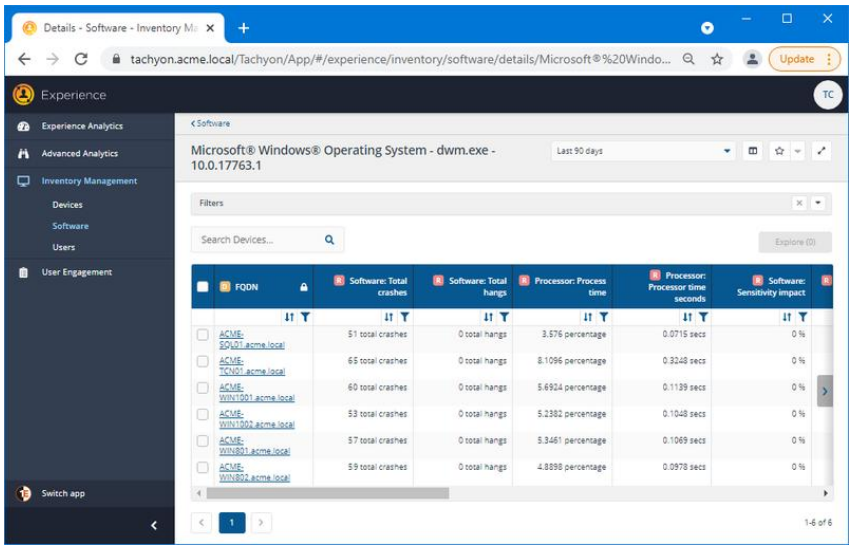


Here they can identify the top offending software for crashes. In this case it is the Desktop Window Manager process **dwm.exe**. The large number of crashes, **345**, indicates that a likely suspect would be the driver software for the graphics card. They can also see that these crashes have occurred within the **Last 90 days**, as shown in the time range selector in the header for the page. The **Devices Count** column shows that these crashes are happening for, at most, **6** devices in the environment.



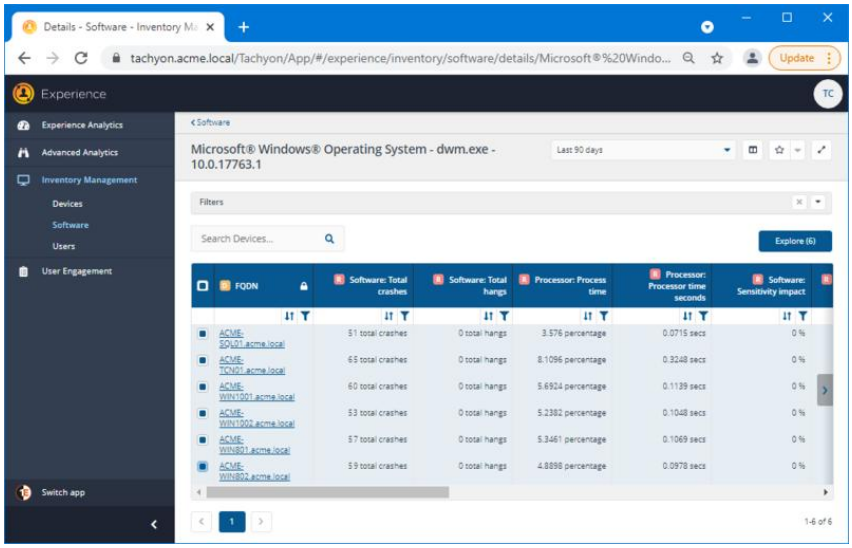
5.3.4.1.5 Viewing the devices where the software is installed

Clicking on the software row displays the list of devices with that software installed. Here they can see that the **345** crashes are distributed fairly evenly across the devices with that version of the software.

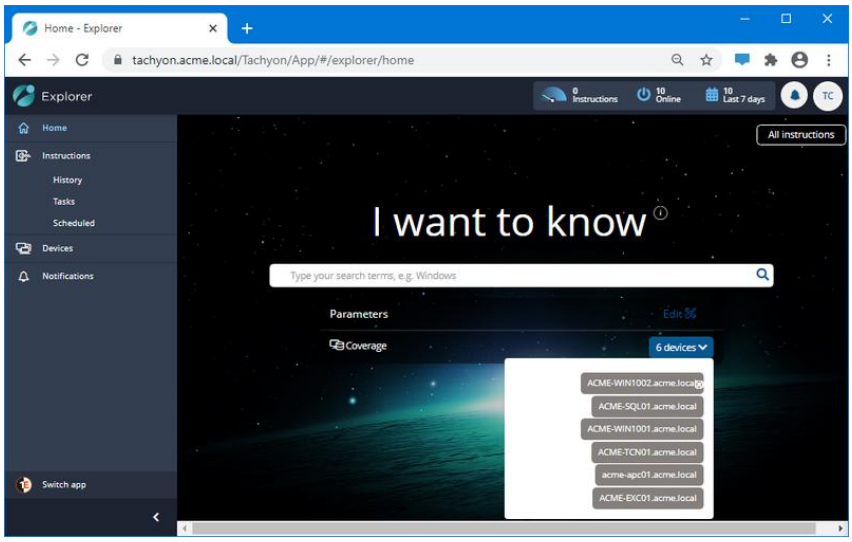


5.3.4.1.6 Exploring the devices in real-time

Having seen the devices that are affected by the issue the engineer can then investigate further. They do this by clicking the checkbox in the header row for the table to select all the devices and then the **Explore** button just above the table - notice how the text of the button has changed to indicate the number of devices that have been selected.

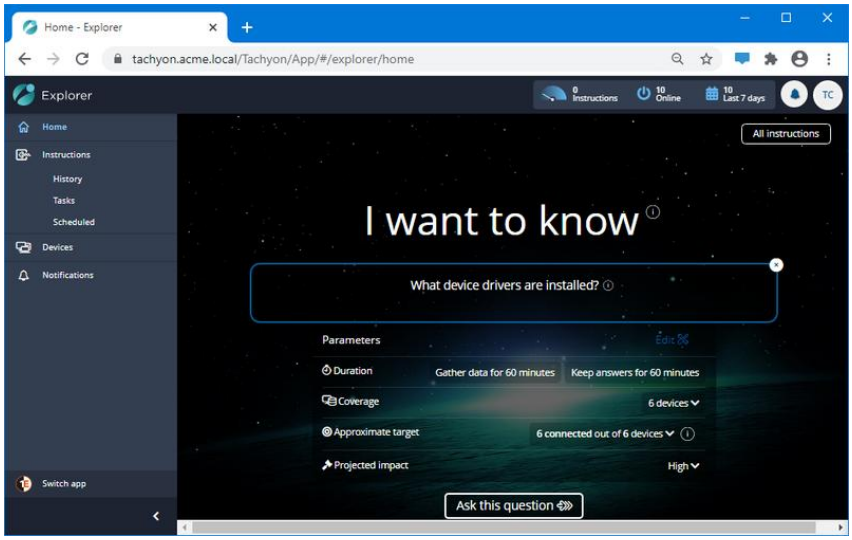


The **Explorer** application is displayed with the **Coverage** set to the selected devices. Now the engineer can question all the devices at the same time to find out what drivers are installed. Typing drivers into the search field lets them select the **What device drivers are installed?** question.

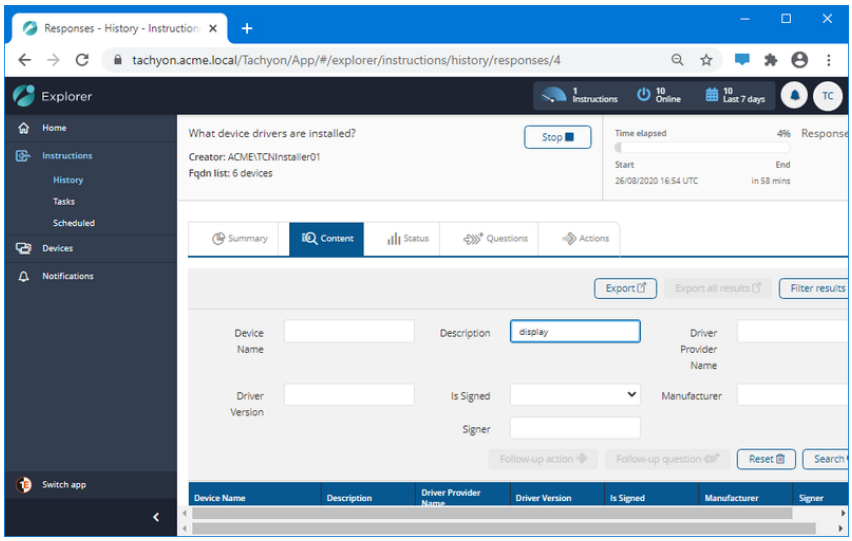


5.3.4.1.7 Checking what device drivers are installed

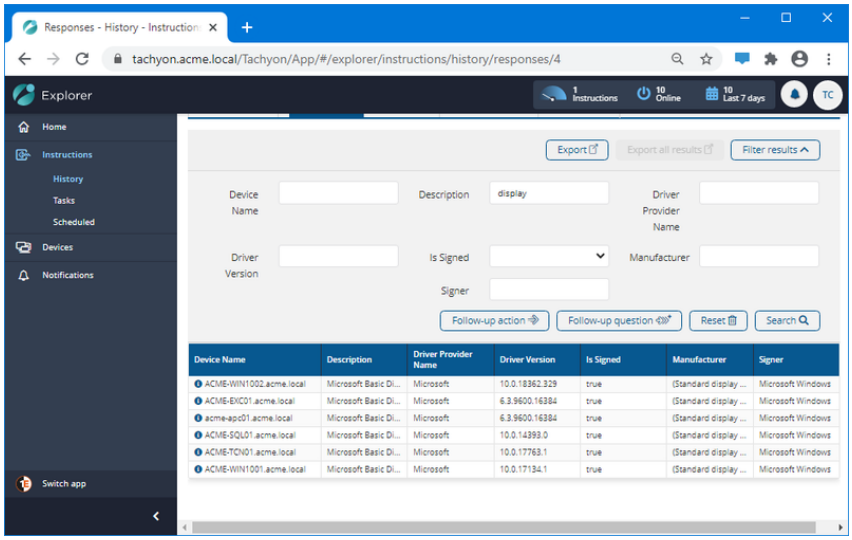
After the question has been selected they click on the **Ask this question** button at the bottom of the page.



As you can imagine the query returns many results from the 6 devices, to help pinpoint the type of drivers they are looking for the engineer uses the filter to show only the results that have the text **display** in the driver **Description** field.

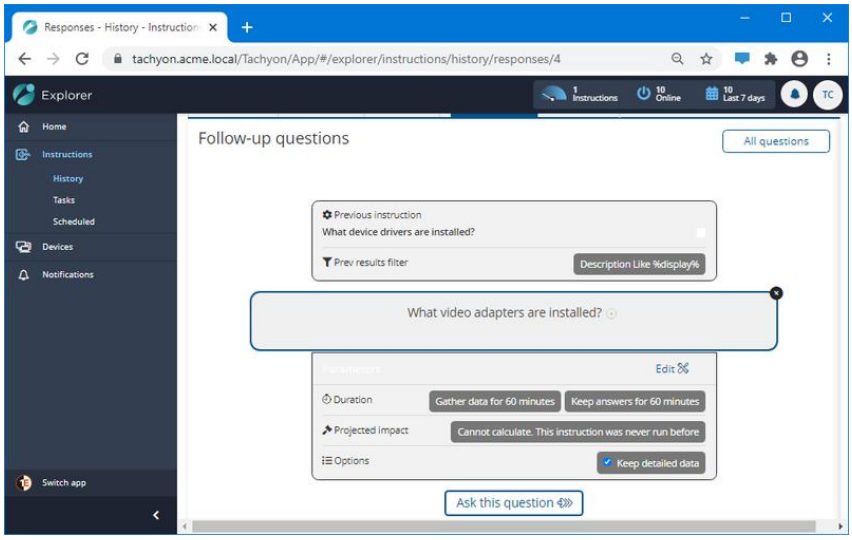


Clicking the **Search** button filters the rows displayed. Here they can see that the driver for all the devices is **Microsoft Basic Driver**, perhaps there is a compatibility issue that needs to be resolved.



5.3.4.1.8 Following up to find what video adapters are installed

The engineer decides to run a follow-up question to find out what video adapters are installed on the devices by clicking the **Follow-up question** button just above the results table. They then type video and select the matching **What video adapters are installed?** question.

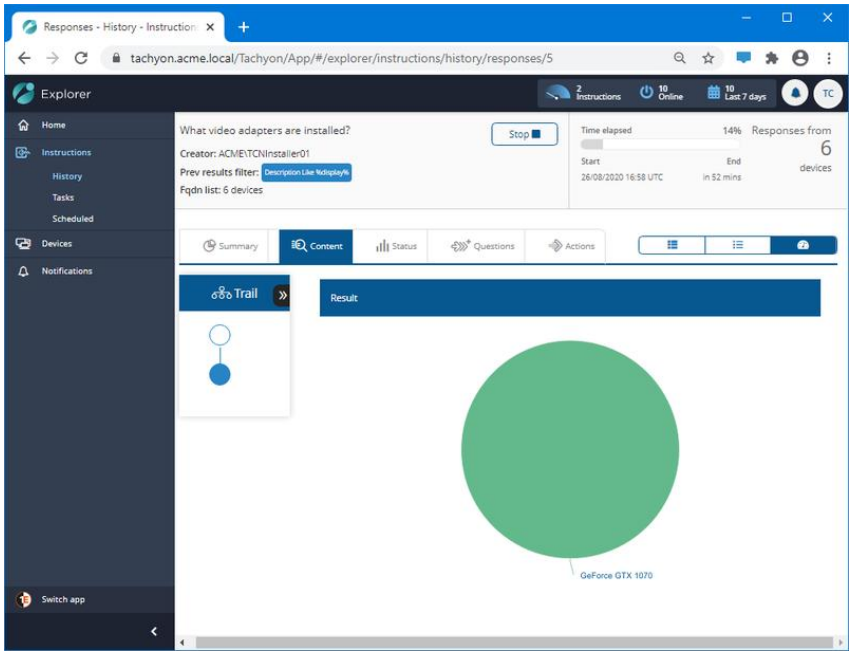


After asking the question they see that all the devices where the Desktop Windows Manager was crashing have the same graphics card installed. This is likely incompatible with the **Microsoft Basic Driver** that is also being used on all those devices so the best course of action would be to find the latest drivers for that graphics card and apply them to all the devices where the crashes are occurring.

5.3.4.1.9 Conclusion

In this scenario the level 3 engineer used the **Experience** pages to check the software installed in their environment. They sorted the table to see the software with the most crashes. Clicking on the worst one, enabled them to view the devices that had been most affected by the software crashes. Selecting all of those devices they were then able to launch Explorer and question the devices to find out what device drivers they had installed and follow that up with a question that

showed the devices' video adapters. Matching those bits of information they concluded that the software driver for the video adapter needed to be updated to the latest for all the devices.



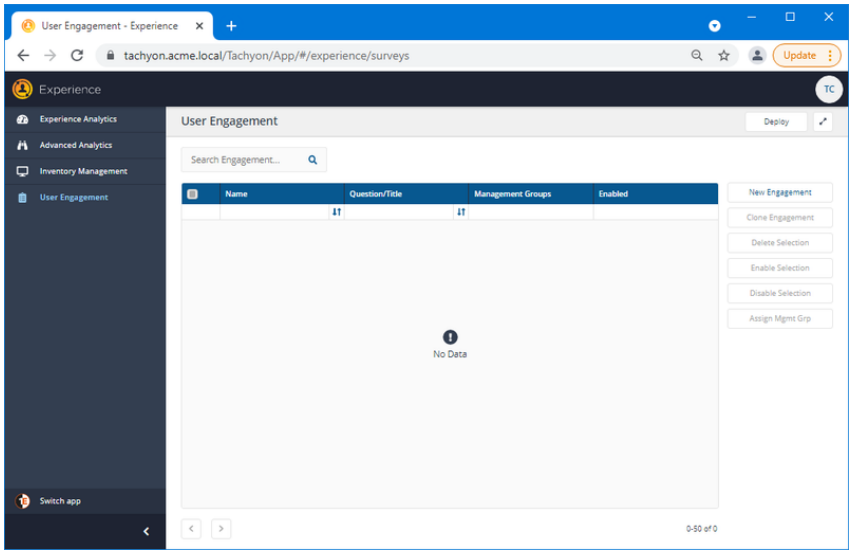
5.3.5 Getting feedback via Sentiment Surveys

In this scenario the IT team have just completed some improvements to their network. The **end-user computing (EUC) manager** uses Experience to gather some continuous feedback to see if the improvements have made a difference to the end-user's experience of their service. This is done using a daily survey that gathers responses that contribute towards the Sentiment score, enabling progress and improvements to be monitored over time.

5.3.5.1 Creating a new Sentiment Survey

The **Experience→User Engagements** page is where you manage all the Sentiment, Info Surveys and Announcements that have been created in Experience. You can easily see for each Survey the **Question** and **Options** that it has been configured with, what **Management Groups** it has been assigned to and whether it's **Enabled** or not. In the picture, you can see the initial state where no Surveys are currently defined, as would be the case for a newly implemented Tachyon system.

Click the **New Engagement** button to begin.

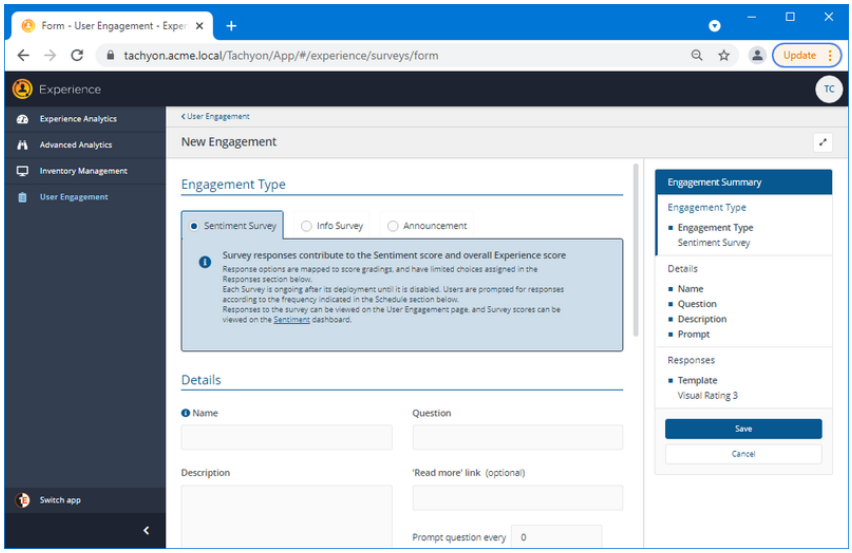


5.3.5.1.1 Sentiment or Info Surveys?

The first choice you face is whether to create a **Sentiment Survey**, an **Info Survey** or an **Announcement**. Announcements expect no response from users.

If the EUC manager wanted to create a one-off survey to gather some user feedback due to a particular event without wanting to monitor the results as part of an ongoing assessment of user experience, they would likely choose an Info Survey. The responses for Info Surveys can be modified to a larger extent than Sentiment Surveys, making them great for doing an arbitrary quick poll, but they don't contribute to the Sentiment Score and therefore cannot be monitored over time. For more information on Info Surveys please refer to Getting feedback via Info Surveys.

Sentiment Surveys are more limited than Info Surveys in the range of possible responses you can select from, but this also means they can be consistently measured and reported on. In our scenario, the EUC manager wants to create a survey that contributes towards the Sentiment score they'll be able to monitor from the Experience Overview page, this means they need to create a **Sentiment Survey**.



5.3.5.1.2 Names, Questions, Descriptions and Frequency

Having selected the **Sentiment Survey** type the next steps are to set a **Name** for the survey, the **Question** and **Description** that will frame the purpose of the survey and the range of **Responses** that will be allowed.

The **Name** for the survey will be stored as a metric that Experience can then report on. This **Name** must be unique amongst all the metrics that are used by, or have been defined for Experience. In this scenario this is set to **Network Performance Survey**. But, be aware that **Network** on its own could not have been used as the **Name**, as this is already a metric that Experience reports on.

The **Question** frames the meaning and purpose of the survey, if the question you choose has not been thought through carefully you will likely confuse your end-users and skew the results. You should also consider the responses you are setting for the survey as they should relate directly to the question. For example, if, like in our scenario, you choose **Visual Rating 5** - which gives you five options ranging from **Very Good** to **Very Poor** - you would have problems if your question was: **Is your network performing badly?** How would you map that question onto the range of chosen responses? Here the question text has been defined as:
How would you rate your network connection? You can see how each of the possible responses could be a suitable answer, so this seems an appropriate question.

The **Description** lets you provide some additional context for the question, and can be used to engage the end-user and provide some guidance as to how the question should be considered. Here the **Description** is defined as:
We've recently made some improvements to the ACME network and wanted to get your feedback on how it's performing for you. This sets the scene for why the question is being asked and gives a small indication on how it could benefit the end-user. The survey is part of a process for improving the performance of the network, and the user's response could help in that process and encourages them to work with the IT department. This aspect of the survey is subtler than determining the question but can still be important in terms of encouraging the maximum number of responses possible.

The **Description** is limited to 512 characters, if you have a site where you can provide additional information with more context for the survey question you can add a link in the **'Read more' link (optional)** field.

Prompt question every x days lets you select how often the survey will be presented to the end-users. We've mentioned that Sentiment Surveys are a way of assessing progress or change from the perspective of the end-users. They are part of a continuous process, and the frequency determines how often data points are taken in order to measure the process. By repeating the question, end-users get the chance to change their responses according to the ongoing performance. But timing is critical, set a schedule that is too often and the end-users may get tired and not respond as often as you would like. Set a schedule that is too seldom, and you may miss out on some changes that occur between polls.

In our scenario, the IT department has just made the improvements to the network, and they are keen to get immediate feedback on how those changes are working and how the systems are adjusting to the changes. So the EUC manager sets the most frequent **Schedule** of prompting the question every day with the view that as the changes mature the **Schedule** for the question can be adjusted to a larger interval.

5.3.5.1.3 Responses

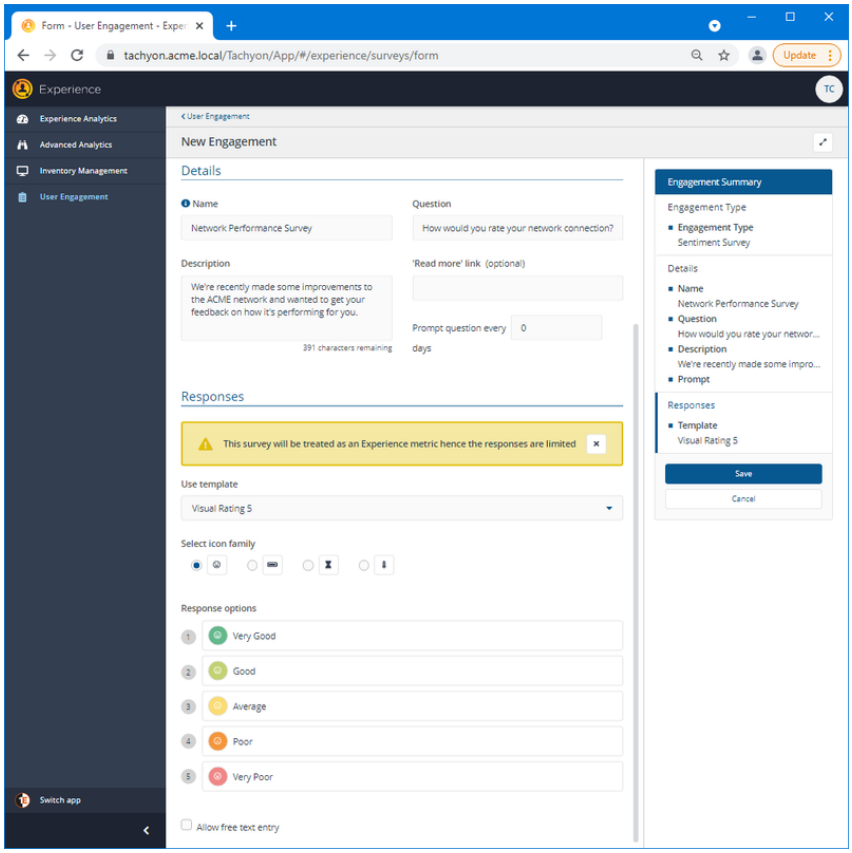
As mentioned earlier, the **Responses** must be closely linked with the **Question** text, and you will likely need to adjust both before you get a suitable fit that is obvious, simple and effective.

For Sentiment Surveys, you can choose a range of 3 or 5 responses, and they can be displayed with several sets of icons or just numbers. You can't change the text of the Responses or the order. Limiting the **Responses** in this

way enables the survey to be measured consistently and contribute to the Sentiment score and ultimately forms a part of the overall Experience score.

Info Surveys let you choose a greater range, edit the response text and select from a wider palette of colors and icons. But, because of that flexibility, they cannot be measured consistently and therefore cannot contribute towards the Sentiment score and have no bearing on the overall Experience score.

The **Allow free text entry** checkbox gives the end-users the opportunity to qualify their responses by typing in any text they feel would help clarify their choice. This does not contribute towards the score but can be invaluable in helping you to interpret the results of the survey. In our scenario, the EUC manager chooses to let the responses speak for themselves and leaves the box unchecked.



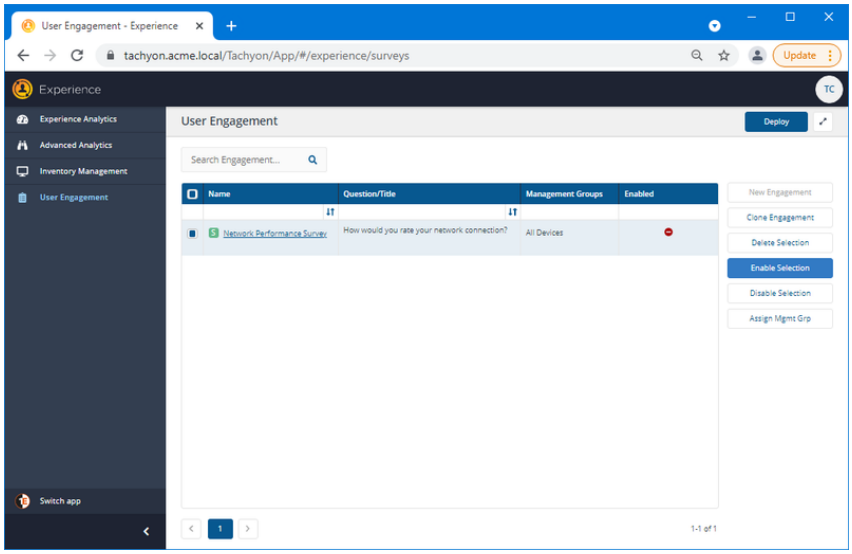
5.3.5.1.4 Saving the new survey

When you're happy with the settings you've made in the survey editor, you can click **Save** to commit the changes and continue to the next step.

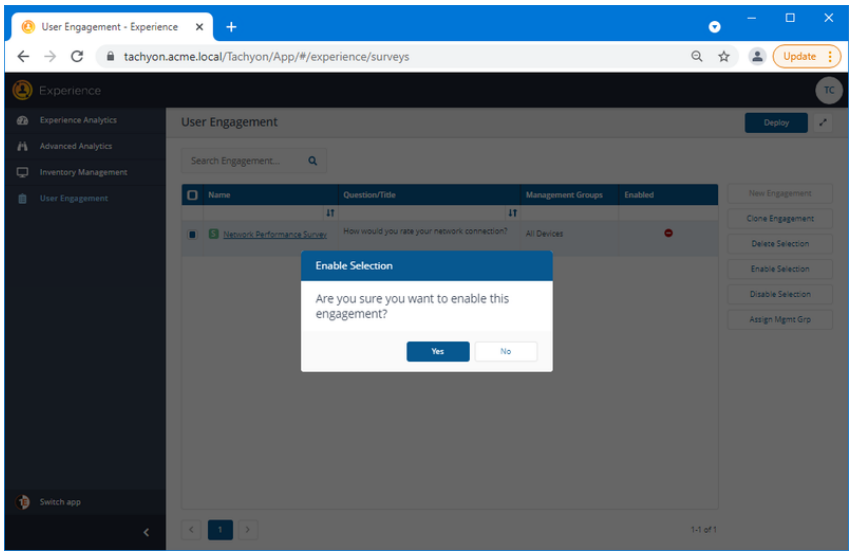
5.3.5.1.5 Enabling surveys

Before a new survey can be deployed, it must first be enabled - this is an extra gateway that prevents the survey being sent out too soon before it's ready.

To enable one or more engagements, select the checkbox at the left-hand end of each engagement's entry in the Engagements table and then click the **Enable Selection** button.



Doing this displays an **Enable Selection** confirmation popup that you must acknowledge before the selected survey(s) are actually enabled. Click **Yes** to confirm the operation and **No** to cancel it.



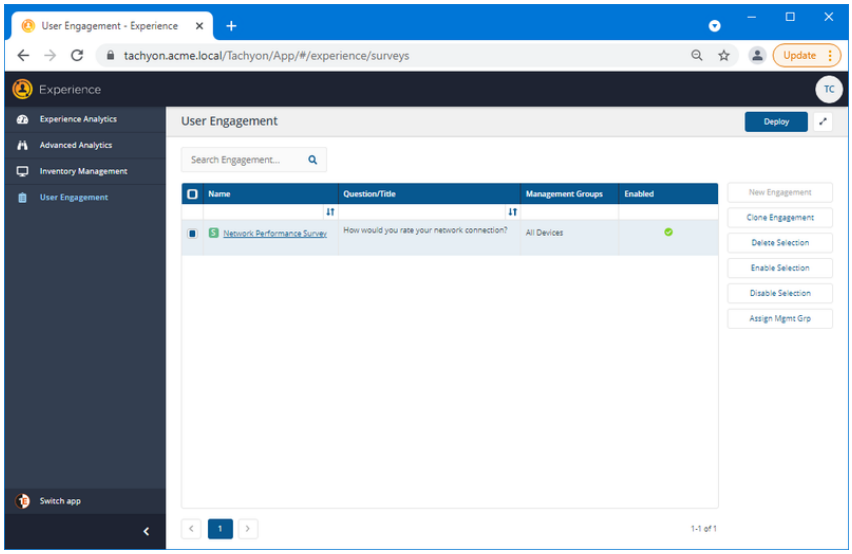
5.3.5.1.6 Deploying surveys

The new survey has been enabled, it can now be sent to the end-users' devices by clicking the **Deploy** button. When a survey is created, the **Management Groups** parameter defaults to **All Devices**. This means that clicking **Deploy** targets all the devices currently and subsequently connected to Tachyon.

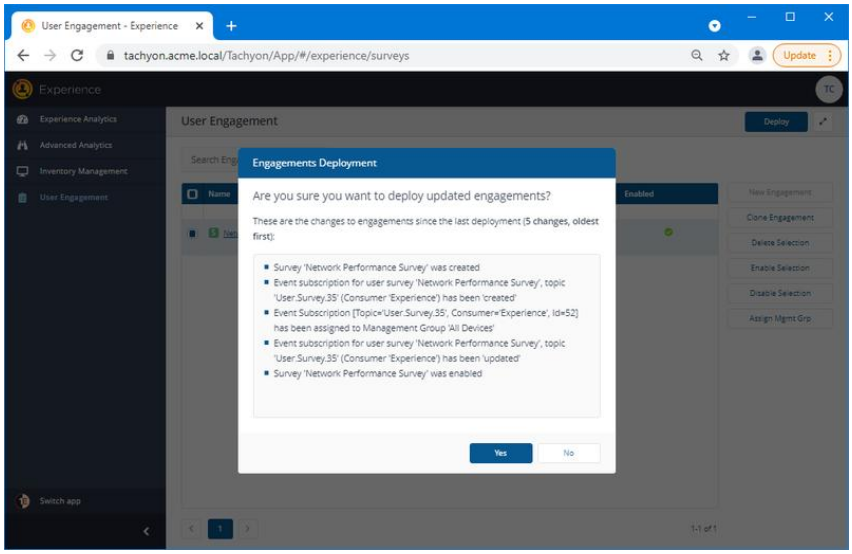
> **Note**
>
> The **Deploy** button sends out any changes to the states of the surveys - meaning you can also use it to set previously deployed surveys to not **Enabled**, thereby preventing further responses without completely deleting the survey, or you can delete surveys when they are no longer needed. You should be aware that the **Deploy** button will also send any other User Engagement administrator's changes.

It's good practice to test the survey on a few machines first before deploying to **All Devices**. This lets you see how the survey will appear to your end-users and gives you the opportunity to debug the text and selections before deploying to a wider audience. Doing this involves assigning a different Management Group to the survey that targets the selected devices. The **Assign Mgmt Grp** button can be used to limit the survey's targeted devices to a specific Management Group.

In our example, which only involves a few devices anyway, to keep things simple we can get away with deploying the survey without testing, so the EUC manager clicks the **Deploy** button.

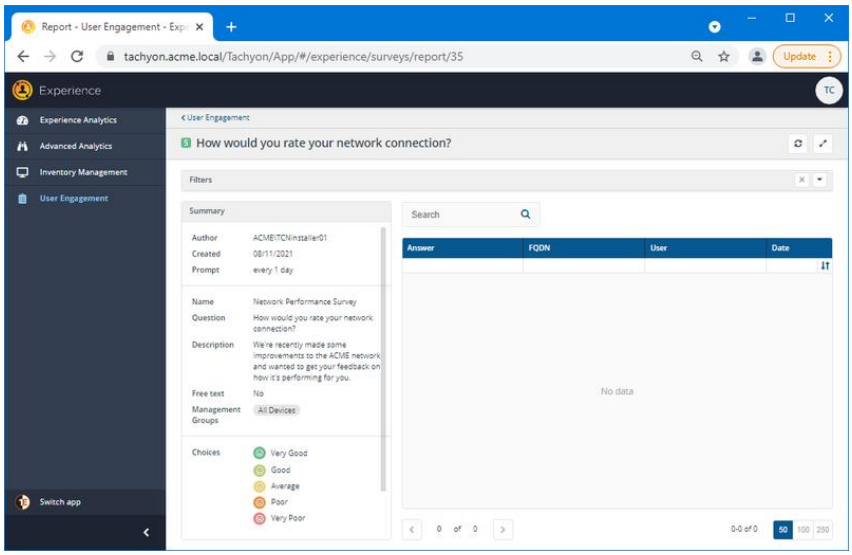


A **Policies Deployment** popup appears that shows the changes that will be deployed when the **Yes** button is clicked. The EUC manager reads the list carefully, sees that the only changes are the ones related to creating and enabling the **Network Performance Survey** and clicks **Yes**.



5.3.5.1.7 Monitoring surveys

Now the survey has been deployed, you will likely want to monitor its responses as they occur. In our scenario, the EUC manager clicks on the **Network Performance Survey** link in the **Name** column for the survey in the Engagements table, to display the responses page for that survey.



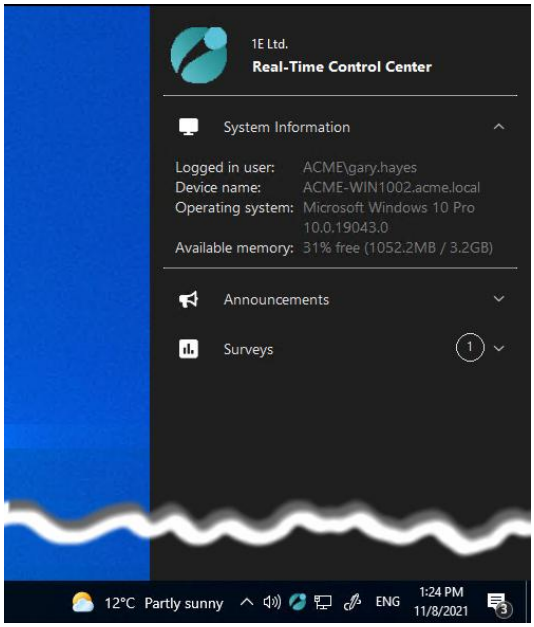
5.3.5.2 What the end-user sees

When the 1E Client is installed on a network device, by default it also adds an icon to the notification area that displays the Real-Time Control Center (RTCC). Initially this may be hidden, but can be dragged onto the taskbar to make it always visible. When an end-user clicks on the icon they will see an information bar with various section, as in the picture, that shows them:

Section	Description
Icon and title	Displays an icon, a company name and title for the Real-Time Control Center.
System Information	A collapsible section that provides information about the device and session where the RTCC is being displayed:

Information	Description
Logged-in user	The domain username for the session.
Device name	The FQDN for the device.
Operating system	The Operating System name and version number.

Section	Description
	Available memory The % free and the free and total values.
Announcements	A collapsible section that lists any current announcements targeted at the device.
Surveys	A collapsible section that lists any current surveys targeted at the device.



In our scenario the end-user **Gary Hayes** clicks on the notification icon to open the RTCC. They then expand the **Surveys** section to see survey question text for the newly deployed survey waiting to be answered, as shown in the picture.

Note

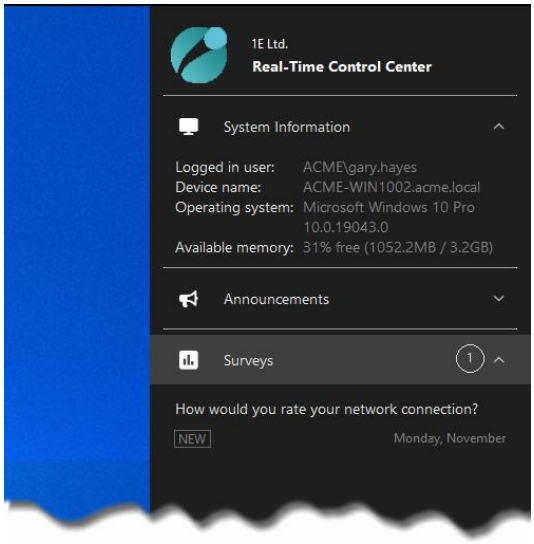
Surveys will also automatically popup to prompt the user without them having to manually select the item from the RTCC. This happens at what the 1E Client assesses to be the best moment according to the user's interaction with the device and whether they have chosen to allow the 1E Client to disturb them or not.

Note

The following 1E Client settings are used to configure the behavior of the Real-Time Control Center. If you click on a link, it will take you to the 1E Client documentation space.

Module.Interaction.Enabled | Module.Interaction.ActiveSessionThresholdSeconds | Module.Interaction.CompanyName | Module.Interaction.DoNotDisturb | Module.Interaction.IdleSessionThresholdMinutes | Module.Interaction.ITSM.ServiceNow.CreateIncidents | Module.Interaction.ITSM.ServiceNow.Enabled | Module.Interaction.ITSM.ServiceNow.GoBackDays |

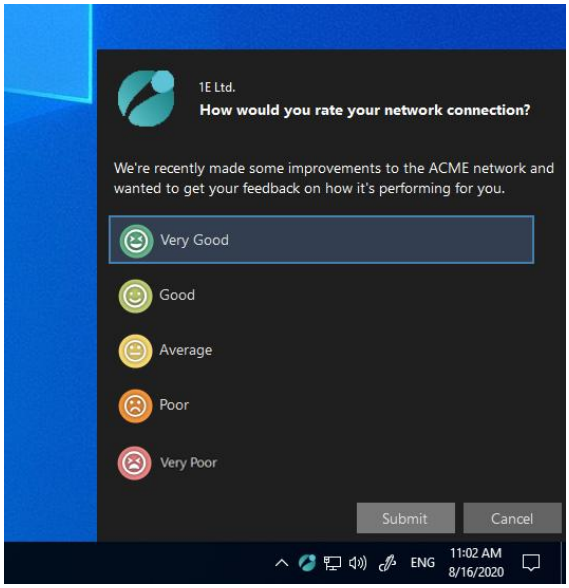
Module.Interaction.ITSM.ServiceNow.Url | Module.Interaction.LogSessionNotificationReadiness | Module.Interaction.MinimumMinutesAfterLogonBeforePrompt | Module.Interaction.MinimumMinutesAfterSessionActivationBeforePrompt | Module.Interaction.MinimumMinutesBetweenPrompts | Module.Interaction.NotificationIcon | Module.Interaction.PeriodsBeforeUiLaunch | Module.Interaction.PeriodsBeforeUiLaunchTimeout | Module.Interaction.Port | Module.Interaction.ResponseAuditsBeforeTidy | Module.Interaction.ResponseRetentionRows | Module.Interaction.SampleExclusionList | Module.Interaction.SampleUserInteraction | Module.Interaction.SnoozeTimeMinutes | Module.Interaction.Theme



5.3.5.2.1 Submitting a response to the survey

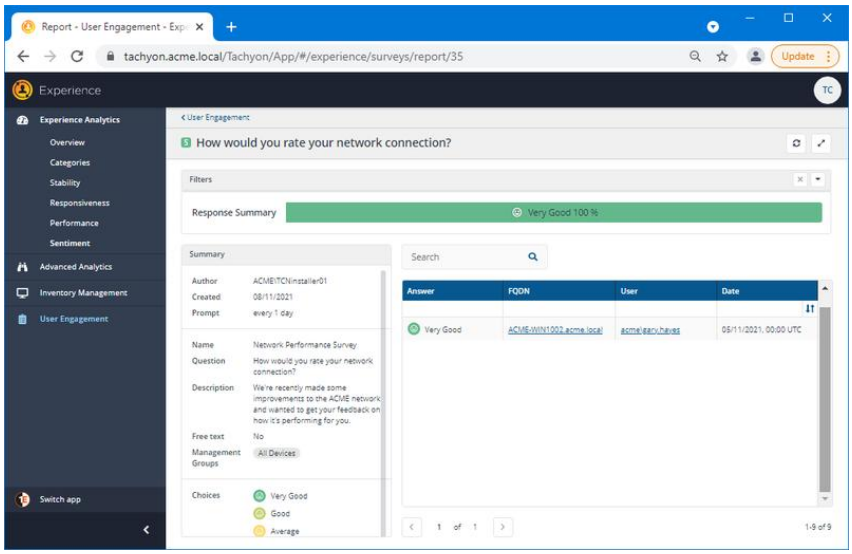
Clicking on the text of the survey question in the **Surveys** section displays the survey, showing the range of responses that can be made, as seen in the picture opposite.

Gary Hayes is happy with the way that the network is currently performing, so he clicks on the **Very Good** response and then clicks **Submit**.

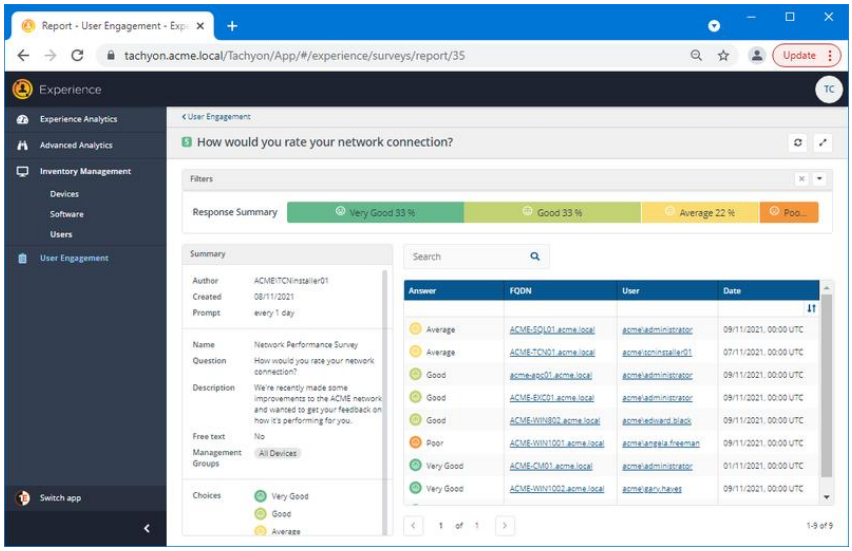


5.3.5.3 Viewing survey responses

Pretty soon after **Gary Hayes** has submitted his response, the EUC manager sees it appear in the Experience interface.

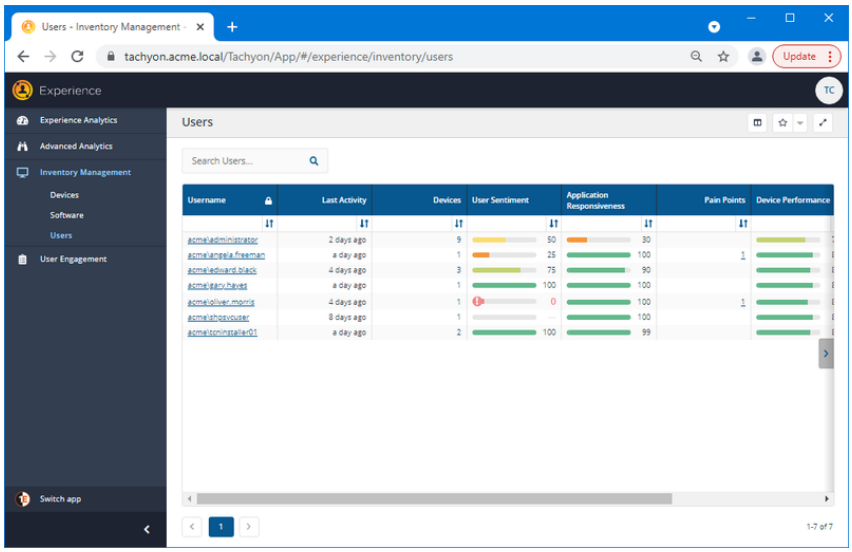


After a number of responses have been made, a clearer picture of the current user sentiment emerges. Here the EUC manager can see that overall the responses have been positive, with 33% being **Very Good** and another 33% being **Good**. There are a couple of outlying responses though that might merit some additional investigation.

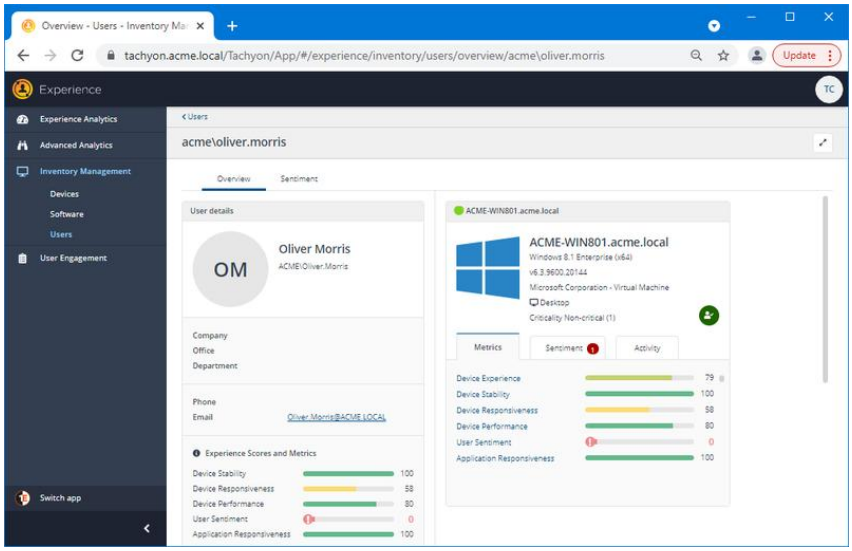


5.3.5.4 Viewing the Users page

Now the current set of responses are in, the EUC manager clicks on the **Experience→Users** page to view how Experience has rated their scores across a range of measurements. Here they notice that one of the users, **Oliver Morris**, has an exclamation mark showing in the **User Sentiment** column.



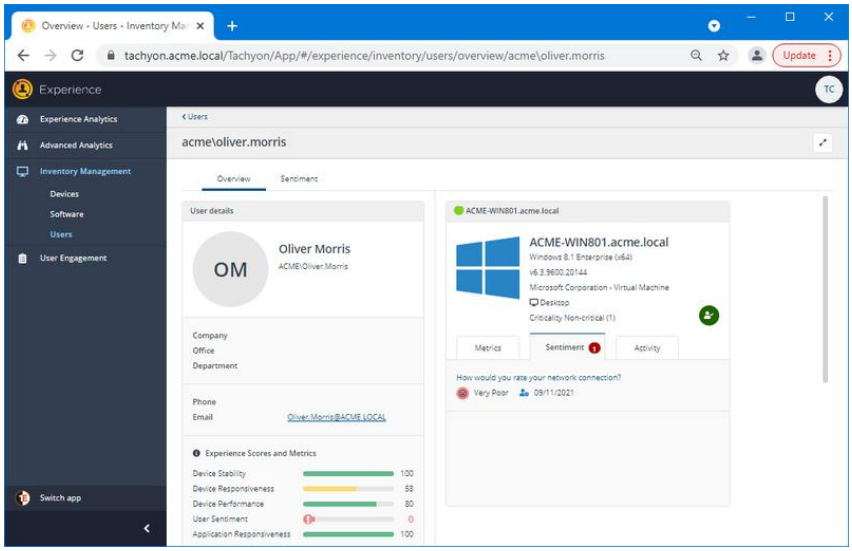
Clicking on the **Username** link for a user navigates to a page that displays information related solely to that user. Here the EUC manager has clicked on the link to view the page for **oliver.morris**. A number of details related to the user are displayed, the **Metrics** tab and the **User Sentiment** score are of interest here - particularly the exclamation mark displayed.



5.3.5.4.1 Viewing the user's Sentiment Survey responses

Clicking on the **Sentiment** tab displays the history of survey responses made by the user. For **Oliver.Morris** their response to the **How would you rate your network connection?** survey was to rate it as **Very Poor**. This is an interesting outlier for the survey responses and warrants further investigation, especially given that the other Experience scores for this user are coming back as good.

The EUC manager could click on the user's email and request some clarification directly. Perhaps there was some other cause for the **Very Poor** rating, such as an accidental response - or perhaps there were other environmental issues that haven't yet come to light. Nonetheless, the manager has been able to investigate the response and is empowered to do something to resolve the user's issue.



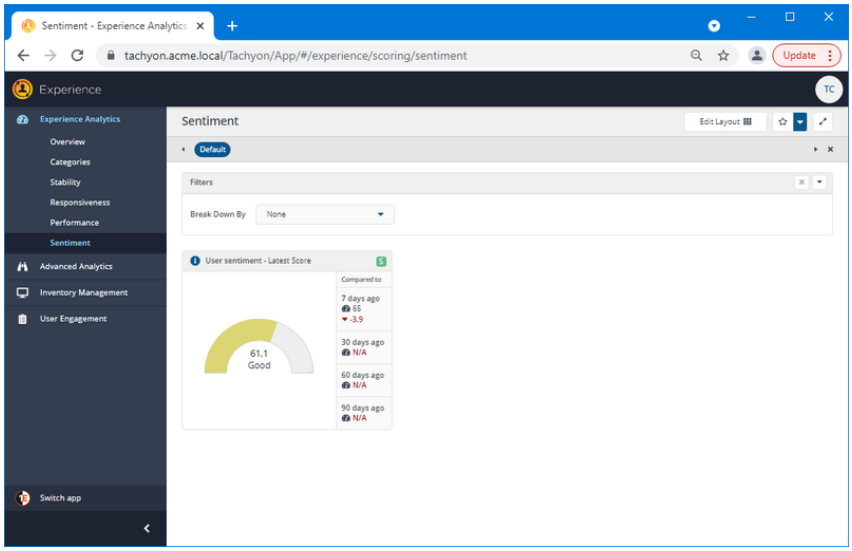
5.3.5.5 Adding the new survey to the Sentiment page

Now that the EUC manager has seen that the survey is returning the type of information that helps assess how the ACME network changes are affecting users, they would like to have those results

figure more prominently and be easier to access. To do this they can add a tile for the survey to the **Sentiment** page. By default, the Sentiment page just shows the **User sentiment - Latest Score** tile, so there's plenty of space available for you to add your own Sentiment Survey tiles.

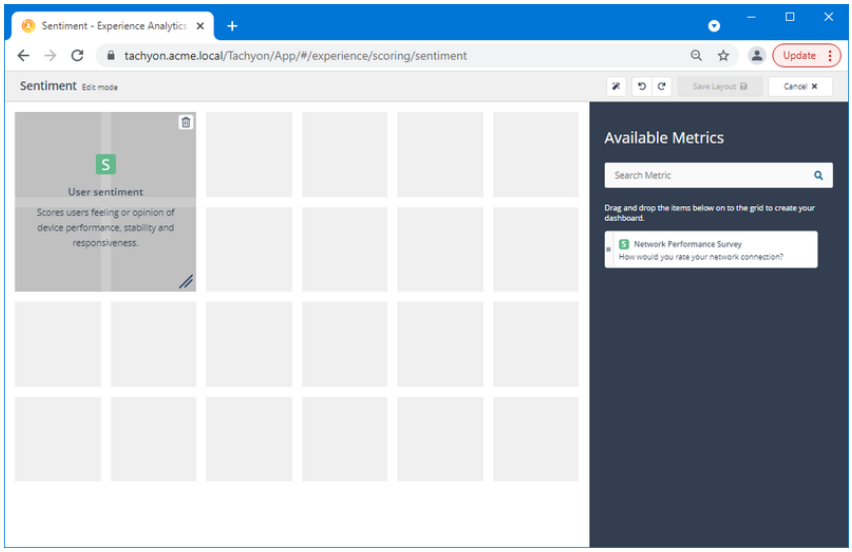
5.3.5.5.1 Editing the page layout to add the new Sentiment Survey

You can change the tiles that are displayed on the page by clicking on the **Edit Layout** button in the page header.



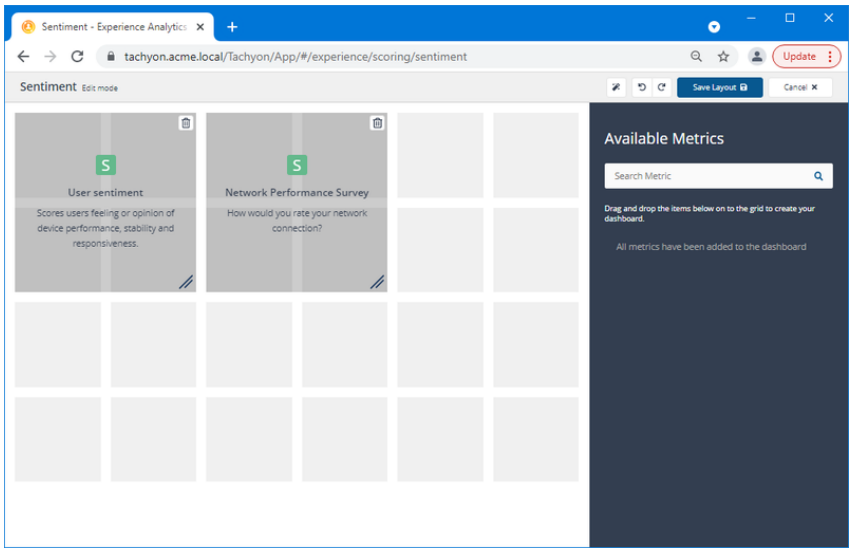
Clicking on **Edit Layout** opens up the **Sentiment Edit mode**. Here they can see the tiles that are already displayed on the page as well as the **Available Metrics**, that is the metrics that can be added to the page. As mentioned earlier the metric that gets added to the system for Sentiment Surveys is the same as the name set for the survey when it was created.

The EUC manager can see the **Sentiment** tile on the left-hand page layout pane, which is the default tile for the Sentiment page, and also the **Network Performance Survey** entry in the **Available Metrics** section. To add the new tile they click and drag it from the **Available Metrics** over on to the layout pane.



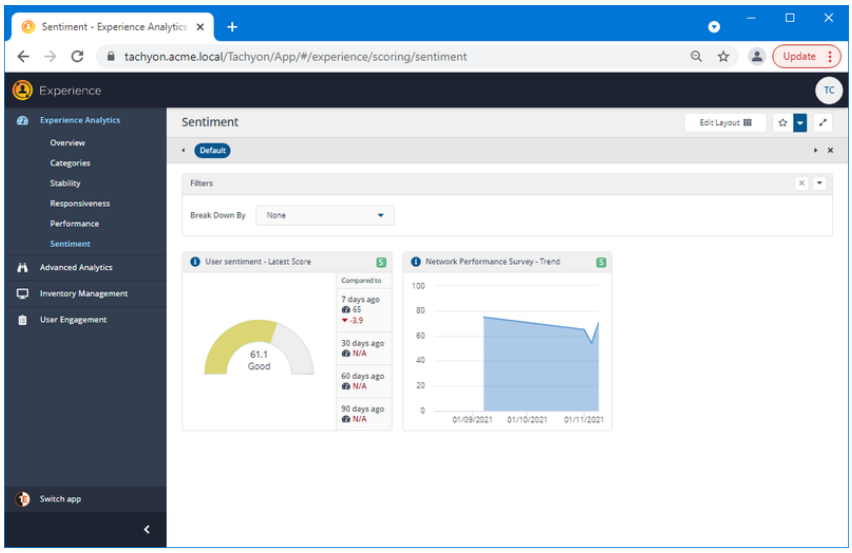
There are different options for the location of the tile and its dimensions, as described in Adding metrics to a dashboard, here the EUC manager just places the new tile next to the existing one and keeps it at the default size of four squares.

Clicking **Save Layout** applies the layout to the **Sentiment** page.

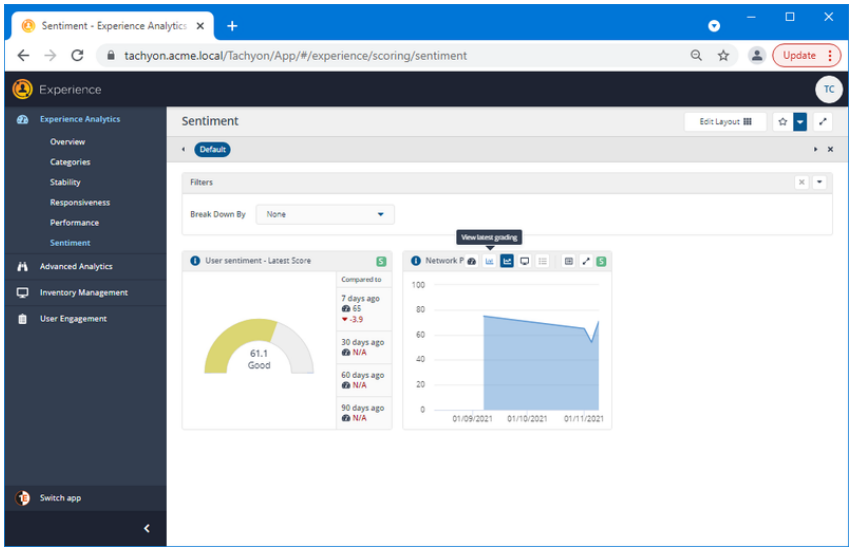


5.3.5.5.2 Changing the tile display

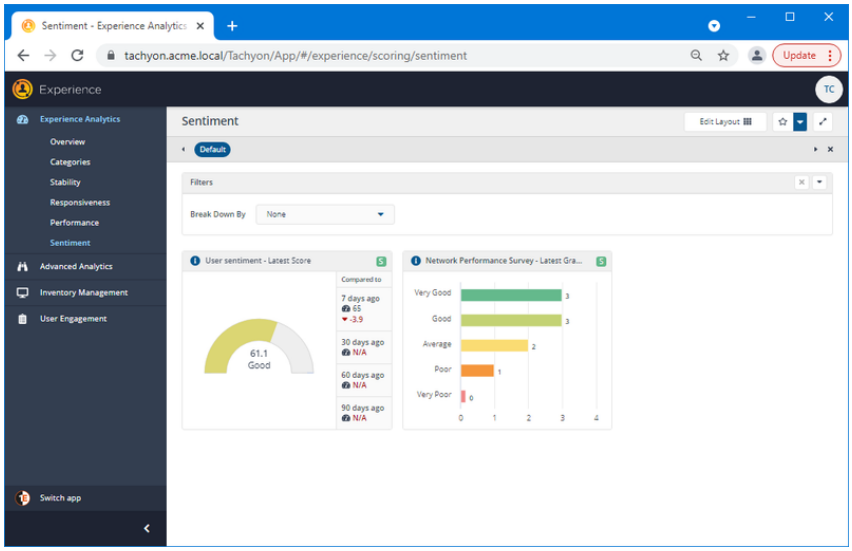
The EUC manager has added the **Network Performance Survey** tile to the **Sentiment** page, but it's still not quite displaying the information the way they want to see it. Instead of a line graph, they want to see the latest score for all the 5 possible responses.



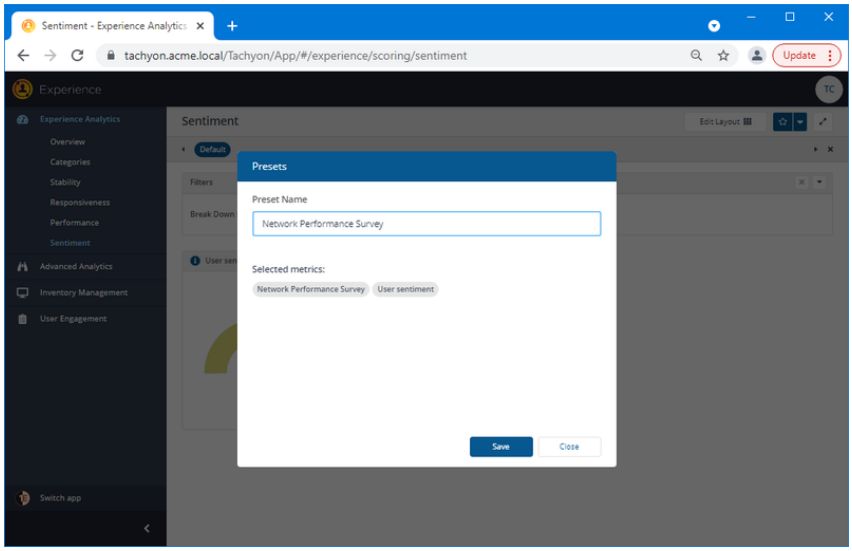
Clicking on the **View latest grading** button in the tile heading will provide the graphic needed.



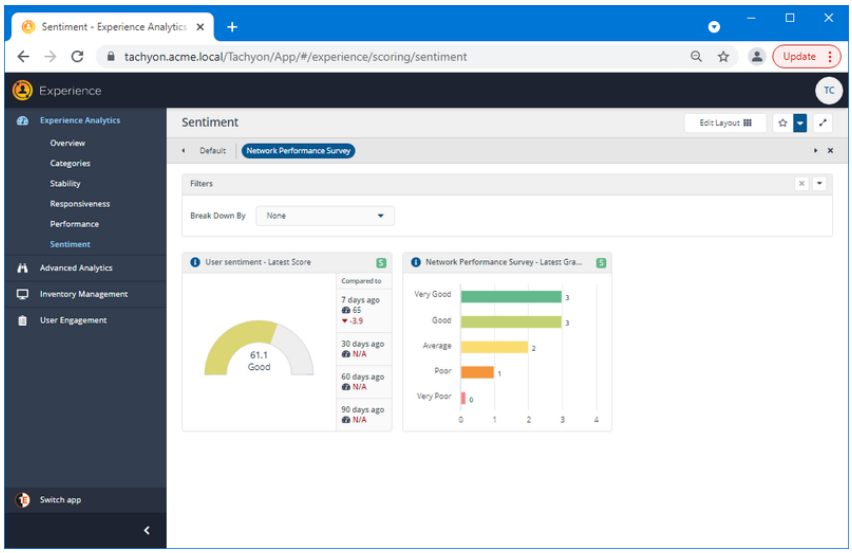
So this is the view the EUC manager wanted. Now they need to make it easily accessible after a page refresh or revisiting the site at a later date. To do that they need to save the layout as a Preset, which is done by clicking on the star button in the page header.



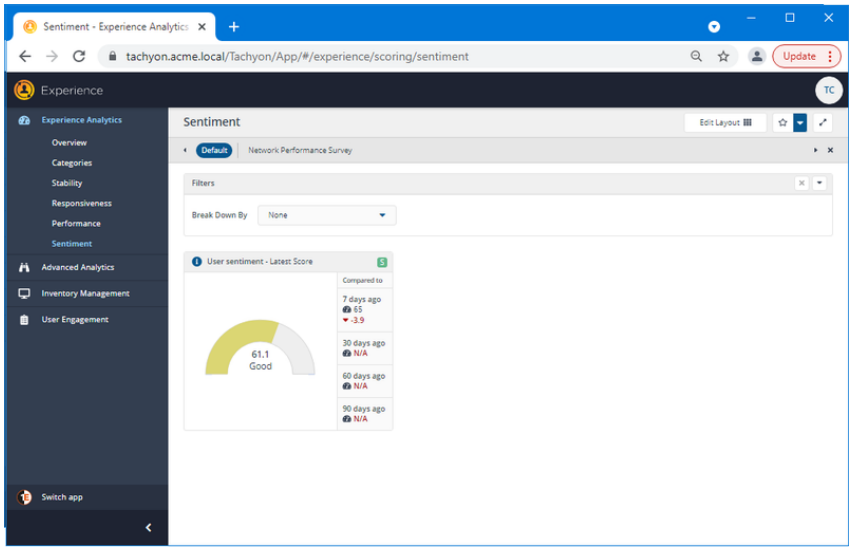
In the **Presets** popup they add a suitable name for the Preset and click **Save**.



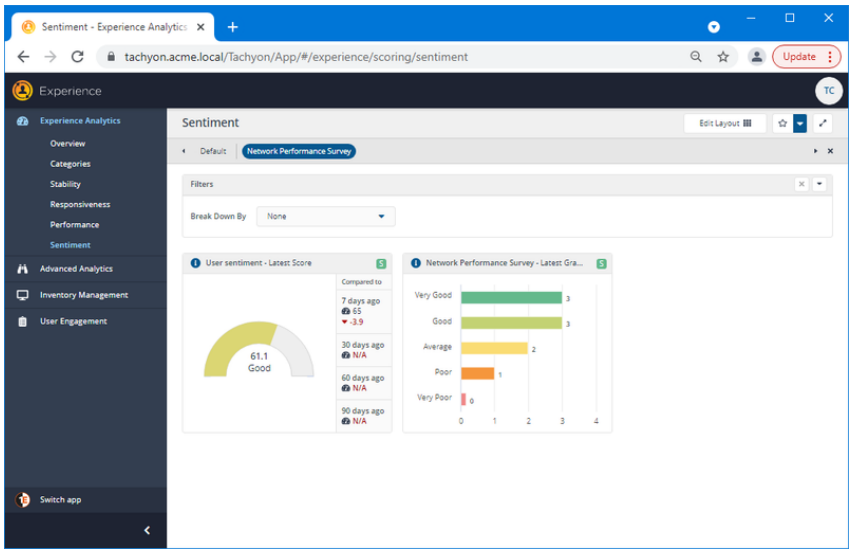
The new **Network Performance Survey** Preset is added to the page.



Now when they refresh the page it will revert to the default as normal, but they can easily get back to their tailored view by clicking on the **Network Performance Survey** Preset.



As they create new Sentiment Surveys, further tiles can be added to this view and stored in the same way, so the EUC manager can keep track of how their users are responding.



5.3.5.6 Next steps

Now that you've seen a possible way of using Sentiment Surveys for capturing ongoing feedback from end-users, you might want to take a look at Getting feedback via Info Surveys to see how one-off Surveys can be created, deployed and monitored in the Experience application.

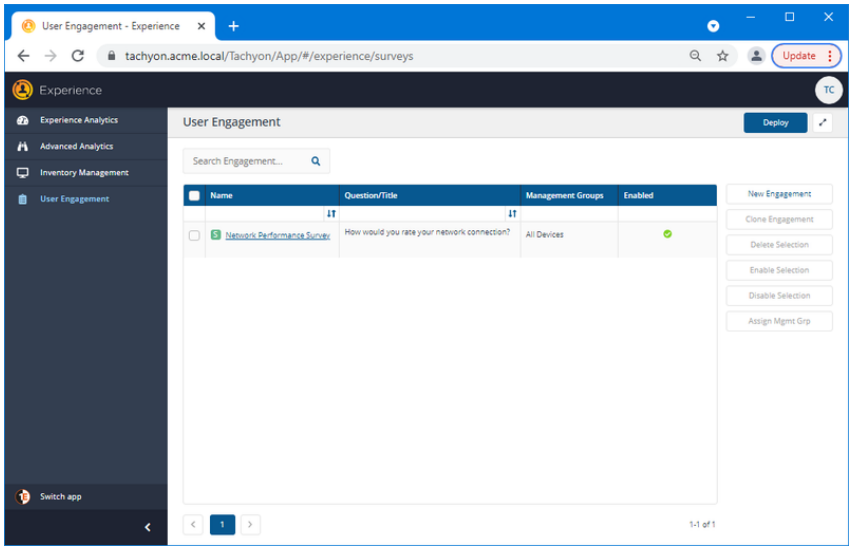
5.3.6 Getting feedback via Info Surveys

In this scenario the IT team want to make improvements to the way they provide their IT services, and they want to get some feedback from their users to see how they are currently resolving issues. The **end-user computing (EUC) manager** uses Experience to create and send a one-off survey to the users asking about how they currently resolve issues with IT. The users will have a week to choose to respond.

5.3.6.1 Creating a new Info Survey

The **Experience→User Engagement** page is where you manage all the Sentiment, Info Surveys and Announcements that have been created in Experience. You can easily see for each engagement the **Options** that it has been configured with, what **Management Groups** it has been assigned to and whether it's **Enabled** or not. In the picture, you can see the state following on from the Getting feedback via Sentiment Surveys scenario.

Click the **New Engagement** button to begin.

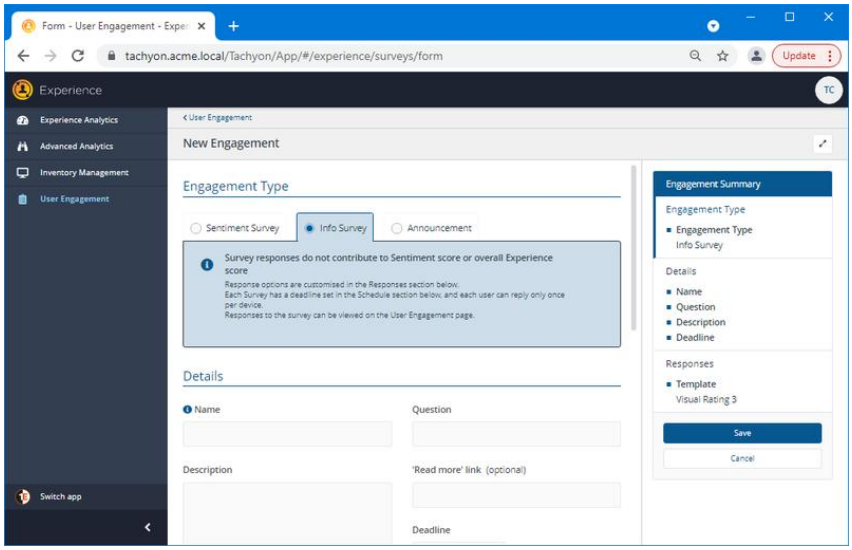


5.3.6.1.1 Info Surveys?

The first choice you face is what type of engagement you want to create.

Sentiment Surveys are more limited than Info Surveys in the range of possible responses you can select from, but this also means they can be consistently measured and reported on. However, in this scenario, the EUC manager doesn't want to create a survey that contributes towards the Sentiment score. Instead, they want to create a one-off survey to gather some user feedback on how end-users currently resolve their IT issues, they won't want to monitor the results as part of an ongoing assessment of user experience and so would choose an Info Survey.

The responses for Info Surveys can be modified to a larger extent than Sentiment Surveys, making them great for doing this type of arbitrary quick poll, but remember that they don't contribute to the Sentiment Score and therefore cannot be monitored over time.



5.3.6.1.2 Names, Questions, Descriptions and Deadlines

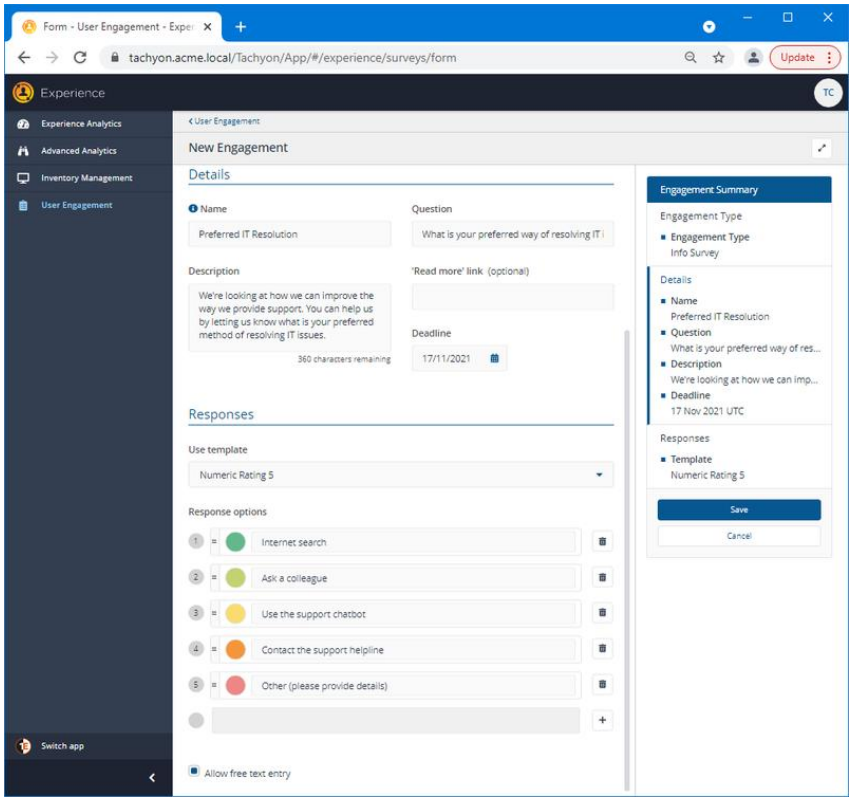
Having selected the **Info Survey** type the next steps are to set a **Name** for the survey, the **Question** and **Description** that will frame the purpose of the survey and the range of **Responses** that will be allowed.

The **Name** for an Info Survey is not stored as a metric that Experience can then report on. The **Name** must be unique amongst all the survey names that have been defined for Experience, but does not have to avoid other Metric names. For example, unlike Sentiment Surveys, **Network** on its own could be used as the **Name** for an Info Survey, even though this is already a metric that Experience reports on. It is best to choose a good name for the survey that reflects the type of question being asked, in this scenario the EUC manager names the survey: **Preferred IT Resolution**.

Just as in Sentiment Surveys, the **Question** frames the survey's meaning and purpose, if the question you choose has not been thought through carefully you will likely confuse your end-users and skew the results. For Info Surveys, the responses you set for the survey can be customized, so a wider variety of questions can be asked. In our scenario, the EUC manager sets the question to:
What is your preferred way of resolving IT issues?

Like Sentiment Surveys, the **Description** for Info Surveys is displayed to the end-user alongside the question and should provide additional context. Use it to capture their attention and provide some guidance as to how the question should be considered. Here, the EUC manager sets the **Description** to:
We're looking at how we can improve the way we provide support. You can help by letting us know what your preferred method of resolving IT issues is. This sets the scene for why the question is being asked and gives a small indication on how it could benefit the end-user and engages them in the process of improving IT. This aspect of the survey is subtler than determining the question but can still be important in terms of encouraging the maximum number of responses possible.

Unlike Sentiment Surveys, Info Surveys are only sent out once and end-users can only make a response once. You can, however, set a **Deadline** for receiving responses, this gives end-users a time range to interact with the survey and send their feedback. Before the deadline occurs, users that haven't yet responded will be prompted repeatedly at appropriate times to make a response. In this scenario, the EUC manager sets the **Deadline** to **17/11/2021**, giving their end-users 7 days to complete. After that time, the survey is closed and the prompts will no longer appear to users who haven't yet responded.



5.3.6.1.3 Defining the responses to the survey

The **Responses** must be closely linked with the **Question** text, and you will likely need to adjust both before you get a suitable fit that is obvious, simple and effective. Info Surveys let you choose a greater range, edit the responses text and select from a wider palette of colors and icons. But, because of that flexibility, they cannot be measured consistently and therefore cannot contribute towards the Sentiment score and have no bearing on the overall Experience score. Initially, the EUC manager selects Numeric Rating 5 for the response options. This gives them five options they can modify, choosing to add more responses (up to a maximum of 10) or remove some. The text of each response can also be edited. For this scenario, the EUC manager edits the text to allow the end-user to choose from the following options:

Internet search

Ask a colleague

Use the support chatbot

Contact the support helpline

Other (please provide details)

To support the last option the EUC manager also checks the **Allow free text entry** checkbox to give the end-users the opportunity to qualify the **Other** response by entering text that describes their other method of resolving IT issues.

5.3.6.1.4 Saving the new survey

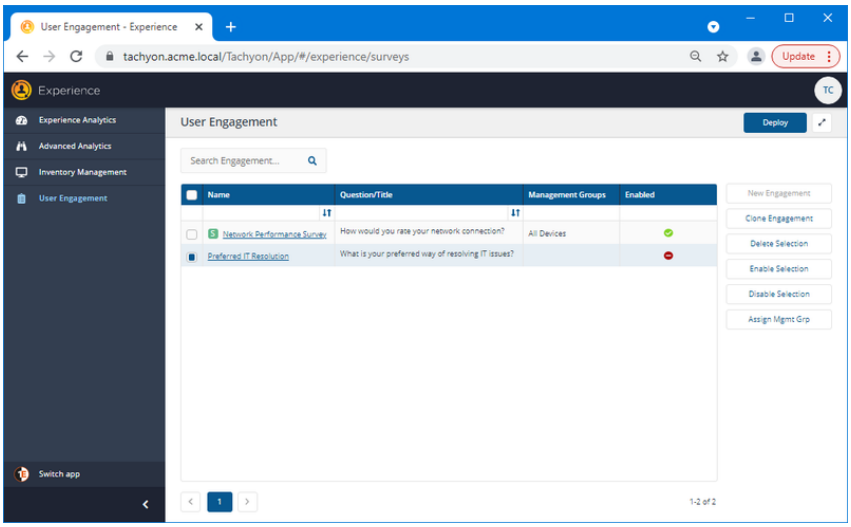
When you're happy with the settings you've made in the survey editor you can click **Save** to commit the changes and continue to the next step.

5.3.6.1.5 Setting the Management Groups for the new survey

Sentiment Surveys default to the **All Devices** Management Group, so they always have a target. Info Surveys don't have a default Management Group, so one must be assigned before the survey can be enabled and then deployed. For this survey the EUC manager wants to poll all of their end-users, so they will assign the **All Devices** Management Group.

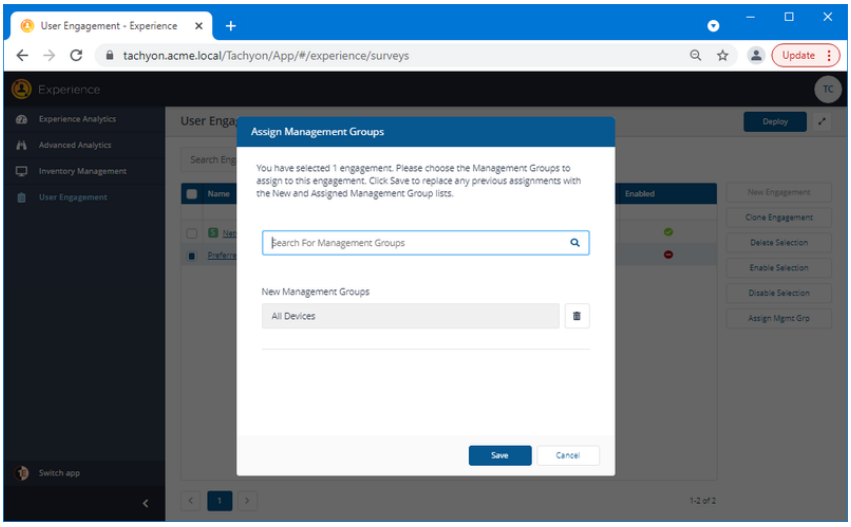
To do this:

They select the survey and then click the **Assign Mgmt Grp** button.



In the **Assign Management Groups** popup subsequently displayed, they type **All** into the search field and then select **All Devices** from the list of matching Management Groups. This gets added to the **New Management Groups** field.

They click **Save** to assign the Management Group.

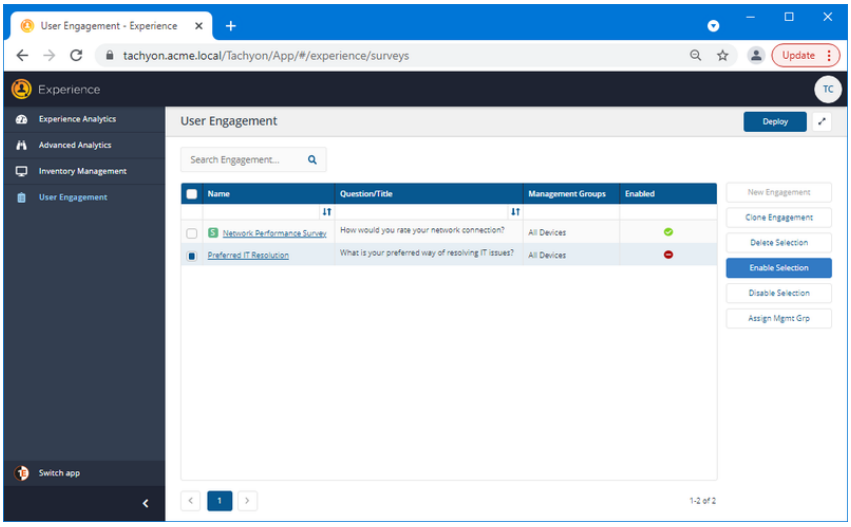


5.3.6.1.6 Enabling the new survey

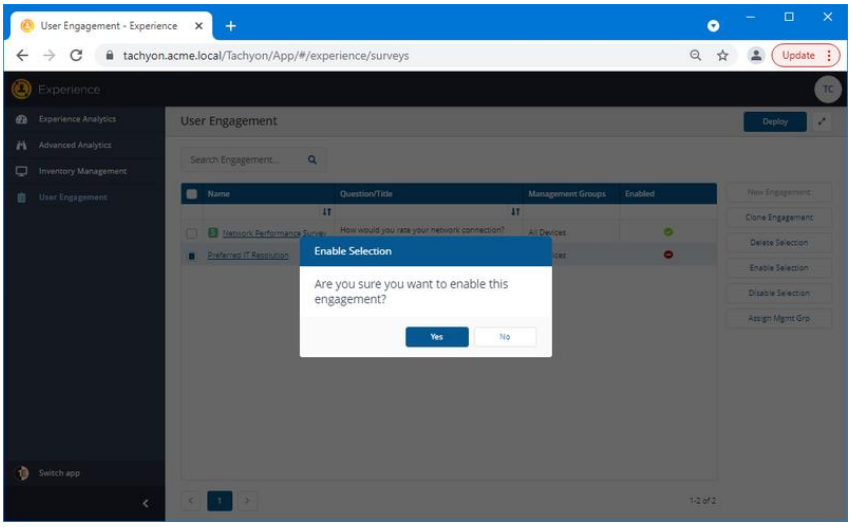
New surveys are not enabled by default. Before they can be deployed, they must be explicitly enabled, providing an additional gateway that prevents the survey being sent out too soon before it's ready.

To enable the new Info Survey the EUC manager:

Selects the checkbox at the left-hand end of each survey's entry in the Engagements table and then click the **Enable Selection** button.



Doing this displays an **Enable Selection** confirmation popup that you must acknowledge before the selected engagements are actually enabled. Click **Yes** to confirm the operation and **No** to cancel it.



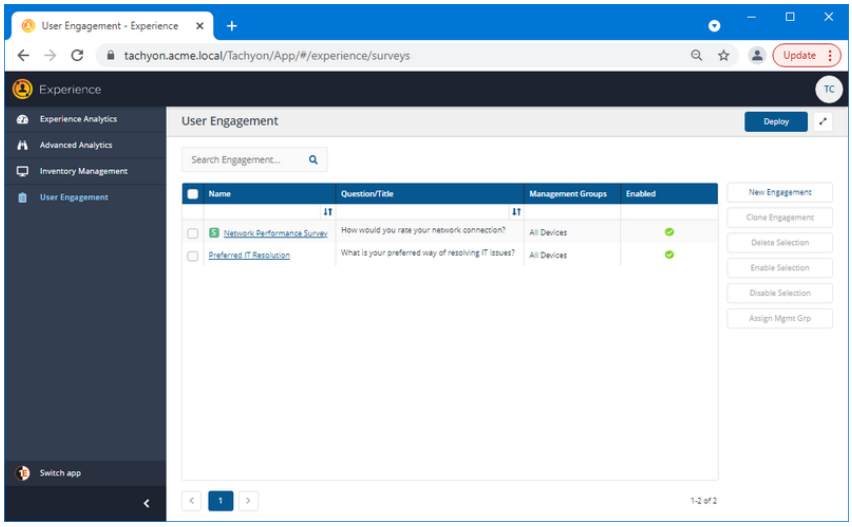
5.3.6.1.7 Deploying the new survey

So the new Info Survey has the **All Devices** Management Group assigned and has been enabled, it can now be sent to the end-users' devices by clicking the **Deploy** button, which will send the survey to all the devices currently and subsequently connected to Tachyon.

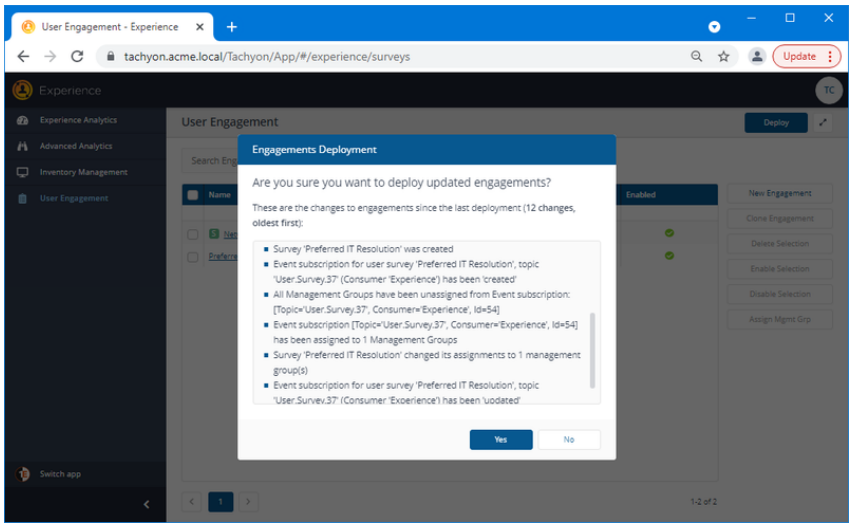
> **Note**
>
> The **Deploy** button will send out any changes to the states of the surveys - meaning you can also use it to set previously deployed surveys to not **Enabled**, thereby preventing further responses without completely deleting the survey, or you can delete surveys when they are no longer needed. You should be aware that the **Deploy** button will also send any other User Engagement administrator's changes.

It is good practice to test the survey on a few machines first before deploying to **All Devices**. This lets you see how the survey will appear to your end-users and gives you the opportunity to debug the text and selections before deploying to a wider audience. Doing this involves assigning a different Management Group to the survey that targets the selected devices.

In our example, which only involves a few devices anyway, to keep things simple we can get away with sending the Info Survey out without testing, so the EUC manager clicks the **Deploy** button.



An **Engagements Deployment** popup appears that shows the changes that will be deployed when the **Yes** button is clicked. The EUC manager reads the list carefully, sees that the only changes are the ones related to creating, assigning Management Groups and enabling the **Preferred IT Resolution** survey and clicks **Yes**. Subsequently, a notification will appear showing that the policy changes are being applied to the Tachyon Agents.



5.3.6.2 What the end-user sees

When the 1E Client is installed on a network device, by default it also adds an icon to the notification area that displays the Real-Time Control Center (RTCC). Initially the icon may be hidden, but may be dragged onto the taskbar to make it always visible. When an end-user clicks on the notification icon they will see the **Surveys** and **Announcements** that have been deployed to the device.

> **Note**
>
> Although Info Surveys are displayed in the list of available surveys, you cannot display them by clicking. Instead, for Info Surveys, the end-user must wait until they appear.

5.3.6.2.1 When does the survey appear?

To minimize the disruption to the end-user of having a survey popup when they're busy using the computer for other things, the 1E Client has a few heuristics that govern when the notifications appear. These measure and compare things like: whether the user is currently interacting with the device, how long it has been since they stopped interacting with the device, how long the notifications should wait before re-displaying if the user didn't respond to the last time it was displayed. These various options interact to essentially display the notification in the sweet spot between the user not actively doing something and the user having left their device.

Info Surveys also provide an option to **Dismiss**, which means that they don't want to answer the survey at all, or click **Later**, which means that they don't want to be bothered just at this moment but may respond when the notification is next displayed.

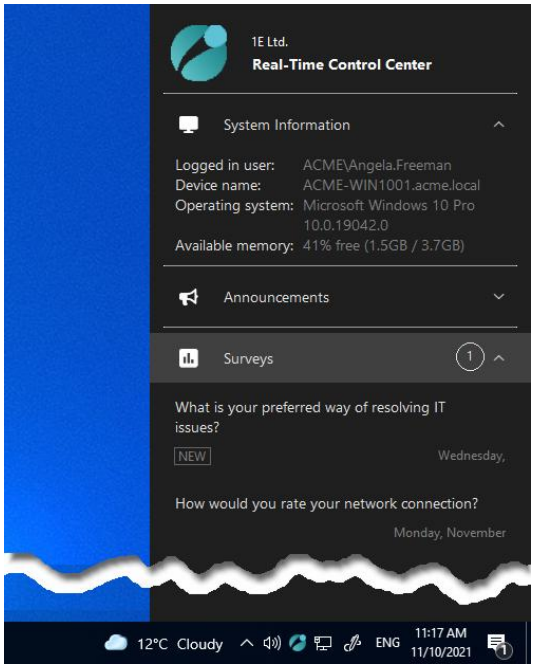
> **Note**
>
> Your end-users can also set the **Do not disturb** option, which prevents notifications from appearing for a configurable time period. Please refer to Do not disturb... for more details.

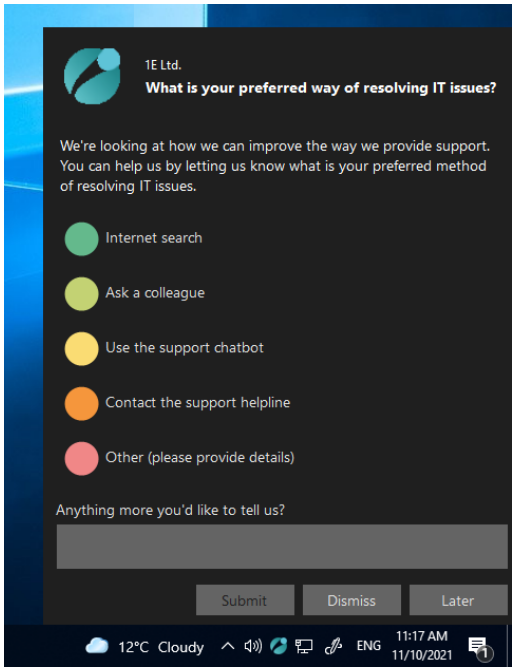
5.3.6.2.2 Responding to the survey

In our scenario, the deployed Info Survey pops up on an end-user's device. They can see both the question and the description text that was defined as part of the survey, along with the range of five customized options for responding and a free text edit box labelled **Anything more you'd like to tell us?**. Although the intention of the EUC manager is for this free text to be associated with the **Other (please provide details)** option, there's nothing to stop the end-user from adding extra information to help clarify any of their choices. There's also nothing to stop the end-user from selecting the **Other** option and not filling out the text box. This is why it is critical for the EUC manager to label the option correctly and at least provide a hint that more details should be added if that option is selected.

> **Note**
>
> The following 1E Client settings are used to configure the behavior of the Real-Time Control Center. If you click on a link, it will take you to the 1E Client documentation space.
>
> Module.Interaction.Enabled | Module.Interaction.ActiveSessionThresholdSeconds | Module.Interaction.CompanyName | Module.Interaction.DoNotDisturb | Module.Interaction.IdleSessionThresholdMinutes | Module.Interaction.ITSM.ServiceNow.CreateIncidents | Module.Interaction.ITSM.ServiceNow.Enabled | Module.Interaction.ITSM.ServiceNow.GoBackDays | Module.Interaction.ITSM.ServiceNow.Url | Module.Interaction.LogSessionNotificationReadiness | Module.Interaction.MinimumMinutesAfterLogonBeforePrompt | Module.Interaction.MinimumMinutesAfterSessionActivationBeforePrompt | Module.Interaction.MinimumMinutesBetweenPrompts | Module.Interaction.NotificationIcon | Module.Interaction.PeriodsBeforeUiLaunch | Module.Interaction.PeriodsBeforeUiLaunchTimeout | Module.Interaction.Port | Module.Interaction.ResponseAuditsBeforeTidy | Module.Interaction.ResponseRetentionRows | Module.Interaction.SampleExclusionList |

Module.Interaction.SampleUserInteraction | Module.Interaction.SnoozeTimeMinutes | Module.Interaction.Theme

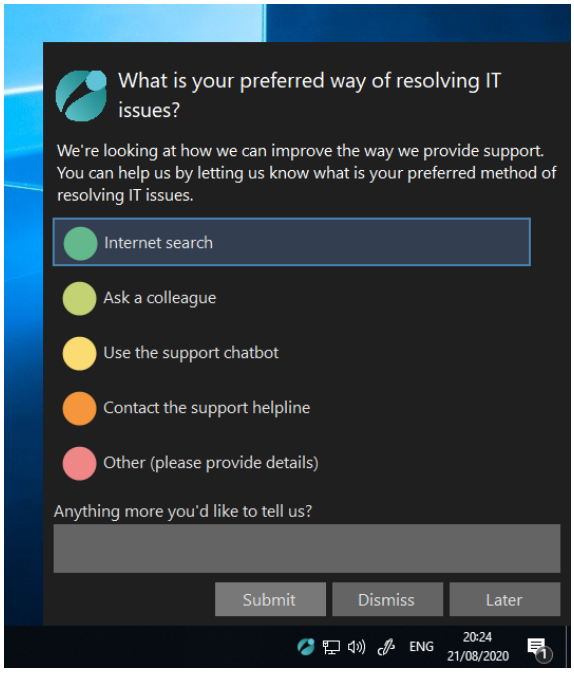




5.3.6.2.3 Submitting a response to the survey

The end-user will need to click on the response they want to make before the **Submit** button becomes enabled.

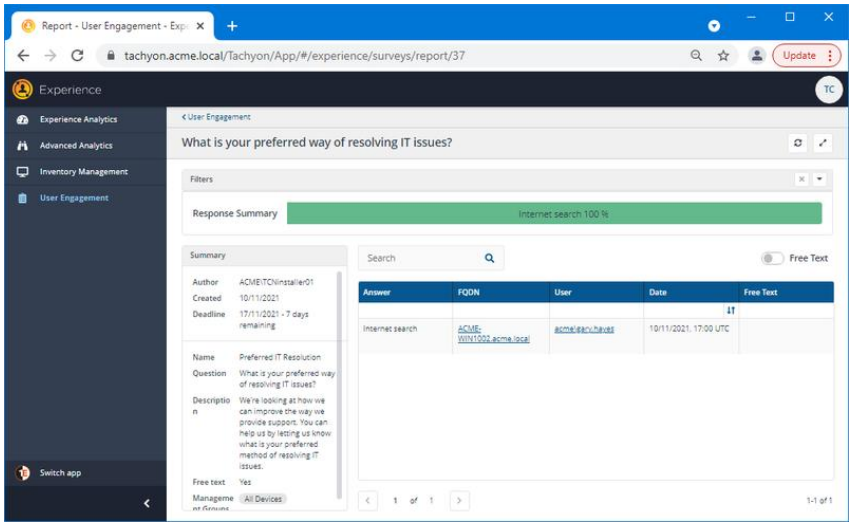
Our end-user is fairly tech-savvy and likes to sort their own problems as far as possible, so they click on the **Internet search** response and then on **Submit**.



5.3.6.3 Viewing survey responses

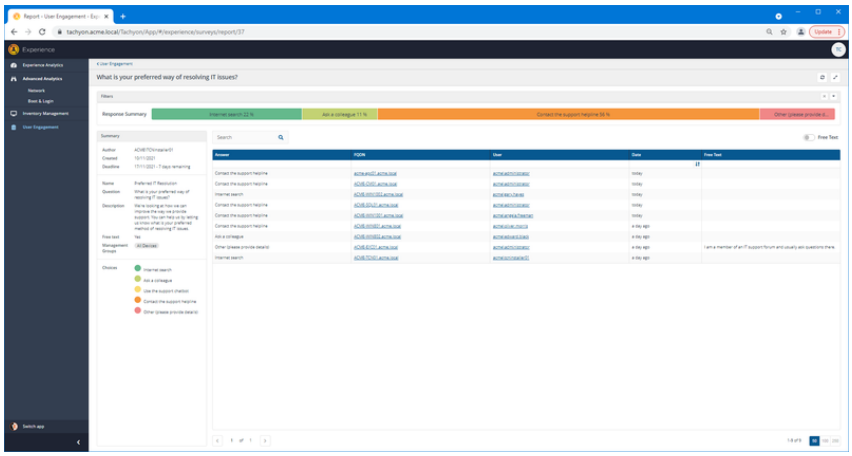
The **Preferred IT Resolution** survey has been deployed and end-users have begun to respond, the EUC manager wants to monitor those responses. For an Info Survey the only place the responses can be viewed is from its details page, you get to this by clicking on the link for the survey in the **Name** column of the Engagements table on the **User Engagement** page.

In the picture, the EUC manager has clicked on the **Preferred IT Resolution** link to display its details page. Here, they can see that a user has submitted a response.



After a number of responses have been made a clearer picture of the current user behavior appears. The majority of users **Contact the support helpline**. The next most popular option is to use **Internet search** and try to resolve their own issues. **Ask a colleague** is the next used option along with **Other**, the text that went with that response indicates that the user is a member of an IT support forum. A surprising aspect of the survey is that no one prefers the support chatbot, Perhaps that is because it is difficult to find, or that the users have had

a poor experience with it. Perhaps the EUC manager would want to follow up with another survey specifically aimed at getting feedback on the support chatbot. Clearly, the survey has performed its task and provided the EUC manager with information that will be useful to the IT department in terms of improving their IT service for end-users.

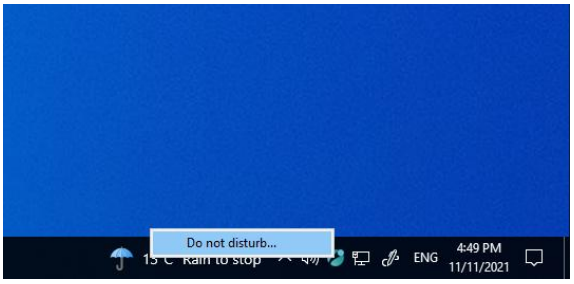


5.3.6.4 Do not disturb...

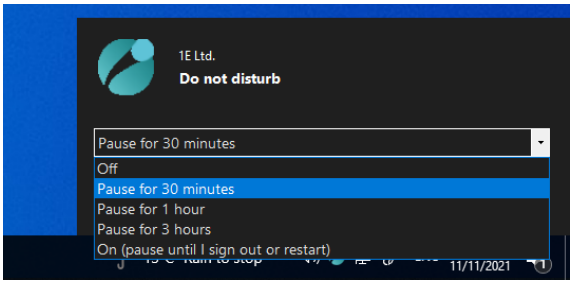
Sometimes your end-users want to be left undisturbed by survey notifications. They may be concentrating on a tricky piece of work or using their device to present to an audience and the last thing they want is a survey notification to popup unexpectedly. In these cases, the end-user can interact with the 1E Client notification icon to temporarily suspend notifications from appearing.

To do this, the end-user would:

Right-click on the 1E Client notification icon to display the **Do not disturb...** option.



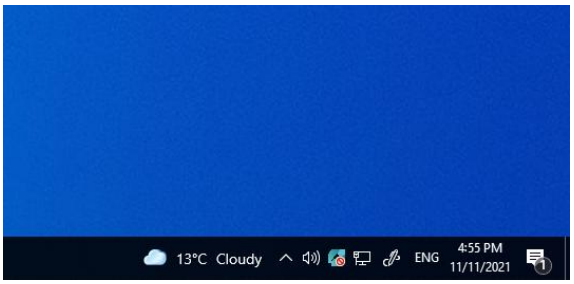
In the **Do not disturb** popup they would select the behavior they want to set.



The options are:

Option	Description
Off	Sets the **Do not disturb** feature to off. Notifications will appear as normal.
Pause for 30 minutes, 1 hour, 3 hours	Set the **Do not disturb** feature to on for the selected time period. Notifications will not appear during the selected period, 30 minutes, 1 hour or 3 hours. After that time notifications will appear as normal.
On (pause until I sign out or restart)	Set the **Do not disturb** feature to on until the end-user signs out or restarts their device.

After selecting one of the options that turns the **Do not disturb** feature to on, the notification icon will change to indicate that notifications will not appear.

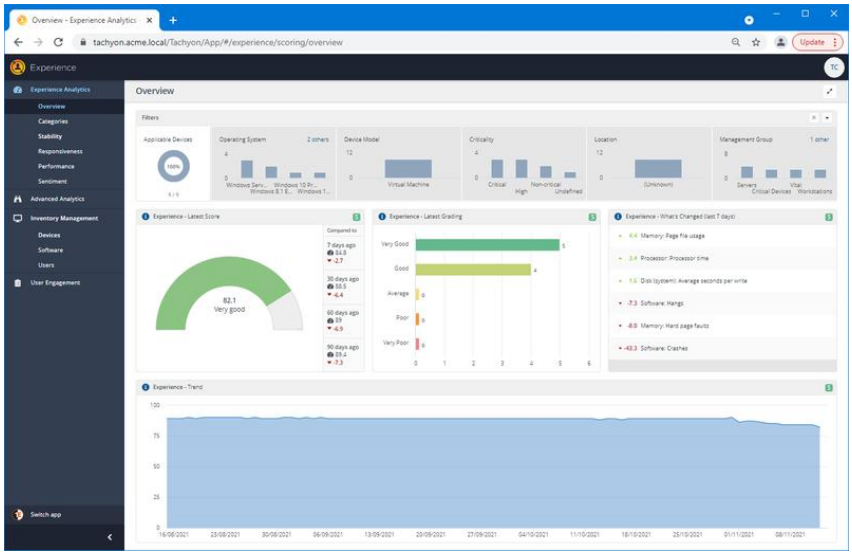


5.3.7 Investigating software crashes

In this scenario, the EUC manager uses Experience to track down the causes for a recent spate of software crashes. After finding some information, they then check whether the crashes have affected key devices currently involved in some urgent work for the company. Finally, they compare two devices, good and bad, to pinpoint the issue cause.

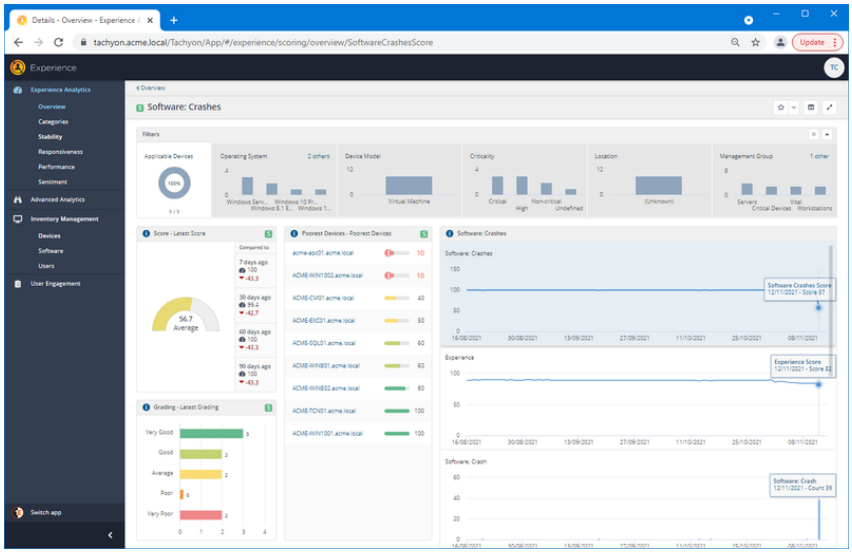
5.3.7.1 Checking the recent trends on the Overview page

The EUC manager checks the **Experience Analytics→Overview** page and notices on the **Experience - What's Changed (last 7 days)** tile that there has been a **-43.3** drop in **Software Crashes**. They click on the **Software Crashes** link in the tile to investigate this disturbing issue.



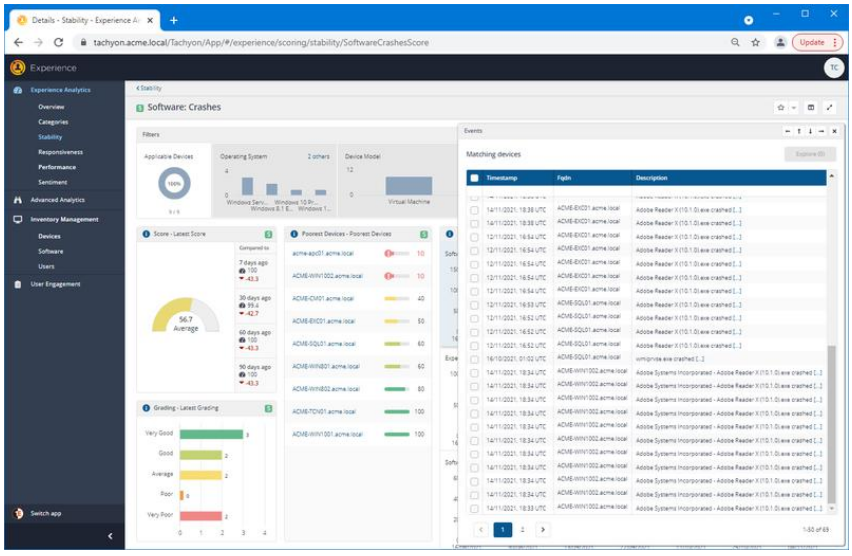
5.3.7.1.1 Checking the Software Crashes

On the Software Crashes page that there has been stability degradation across a number of devices, particularly for two devices, whose software crash score is now just 10 out of 100. Scanning through the graphs, they see that there is a sharp dip in the **Software Crashes Score** and that there have been **39** crashes counted for a single day.



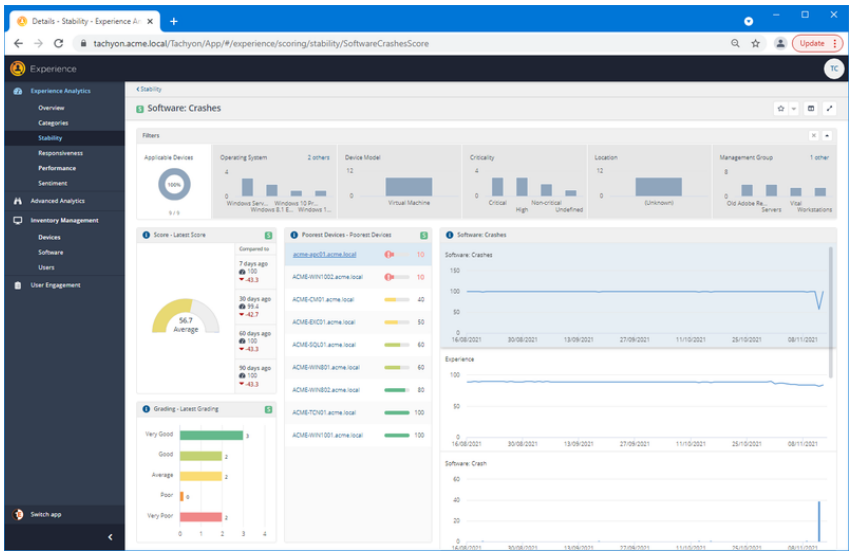
5.3.7.1.2 Viewing the recent crash events

Clicking on the bar for the Software Crash count displays a panel showing the related events. Here they can see that there have been numerous crashes for a particular version of Adobe Reader X (10.0.1).



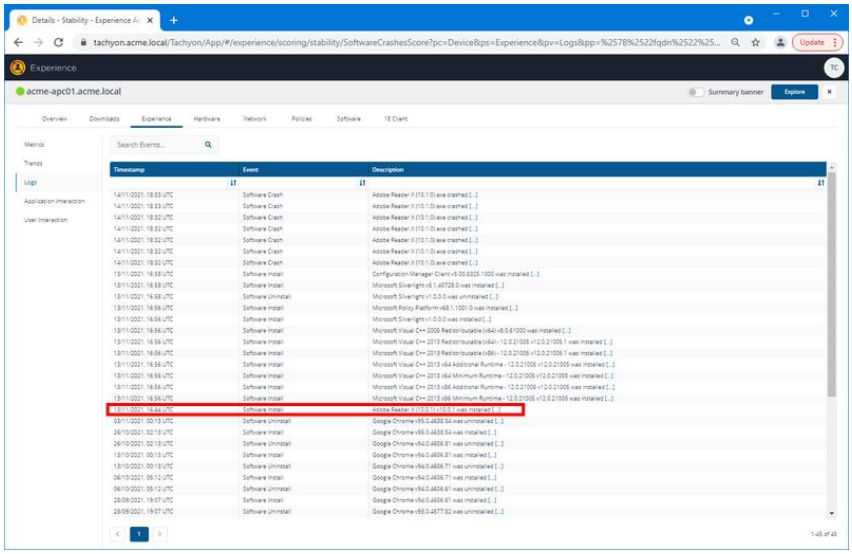
5.3.7.1.3 Investigating the most affected device

Closing the events panel, the EUC manager then clicks on the link for the topmost device in the Poorest Devices tile to open the Device Details panel for that device.



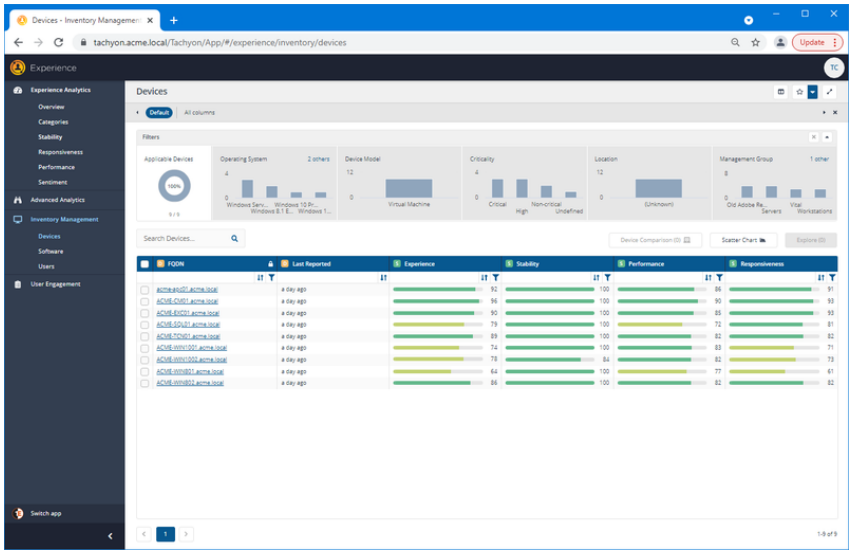
5.3.7.1.4 Checking the Logs for the device

From the Software Crashes page, the device links display the Device Details with the Logs panel open. Scanning down the log entries, they spot a significant entry that shows that Adobe Reader X (10.0.1) has recently been installed on the device.



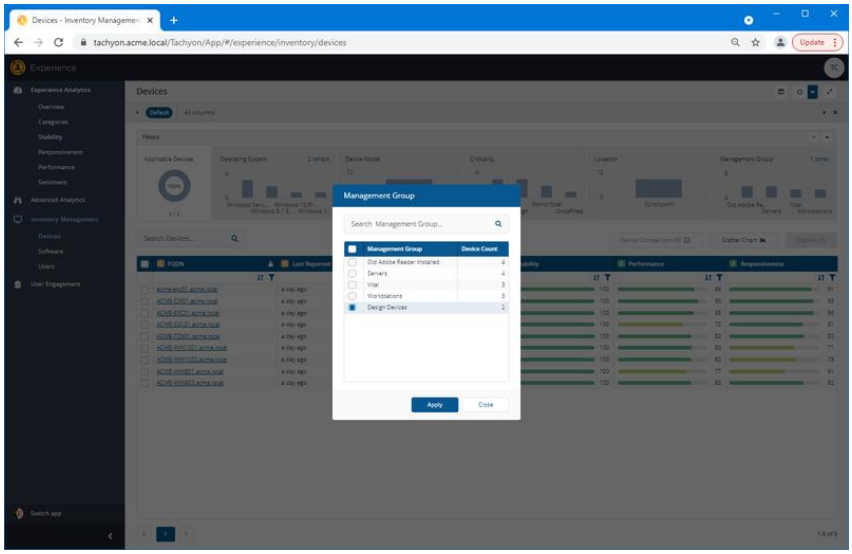
5.3.7.2 Focusing on specific devices using a Management Group filter

The EUC manager now wants to compare two devices, one affected by the crashes and the other not. They also want to check how a particular set of devices has been affected by the crashes. In our example, the EUC manager has an existing Management Group for the devices. They navigate to the **Inventory Management→Devices** page in order to use the Management Group filter to focus the view on the devices they are interested in.



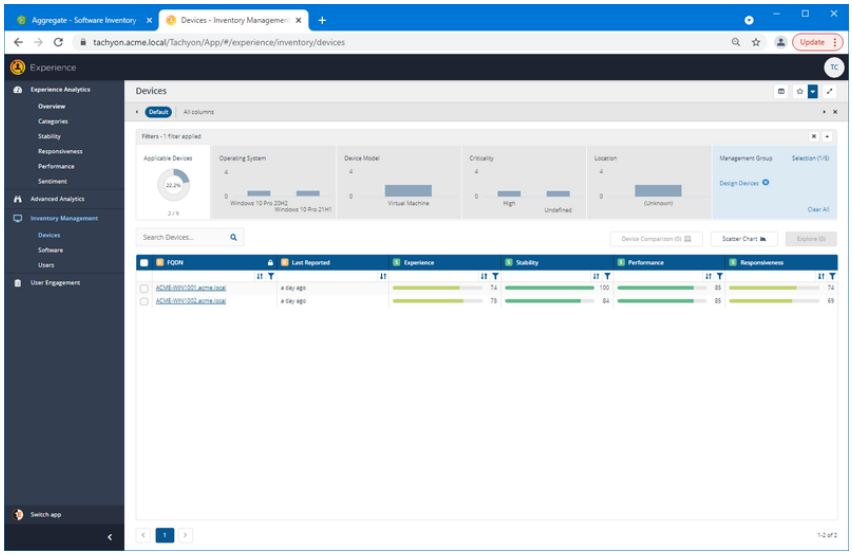
5.3.7.2.1 Selecting the Management Group filter

Clicking on the **1 other** link in the Management Group tile of the Filters bar displays the **Management Group** popup. Here they select the **Design Devices** Management Group that holds the devices they are interested in, and then click the **Apply** button.



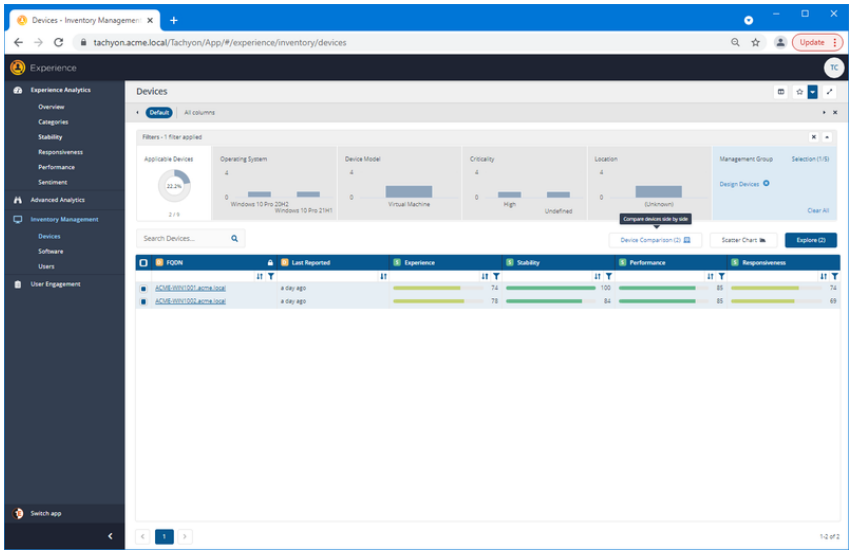
5.3.7.3 Comparing two devices

The Devices list is then filtered to contain just those devices. They can see from the Stability score that only one device has been affected by the crashes.



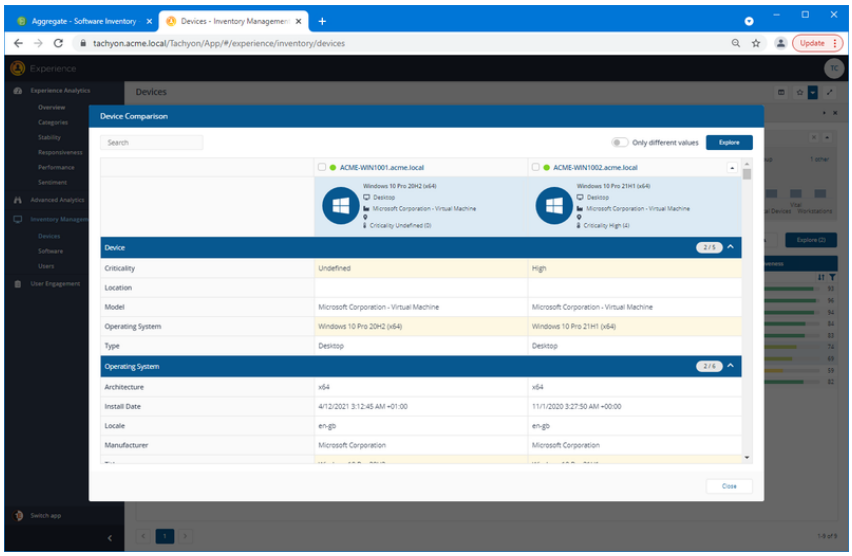
5.3.7.3.1 Using the Device Comparison tool

Selecting the two devices by clicking on the checkbox at the left-hand end of the header row enables the **Device Comparison** button. This button becomes enabled only when there are two items selected in the Devices list. Clicking on the Device Comparison button displays the **Device Comparison** popup and gathers the data from the two selected devices in real-time.



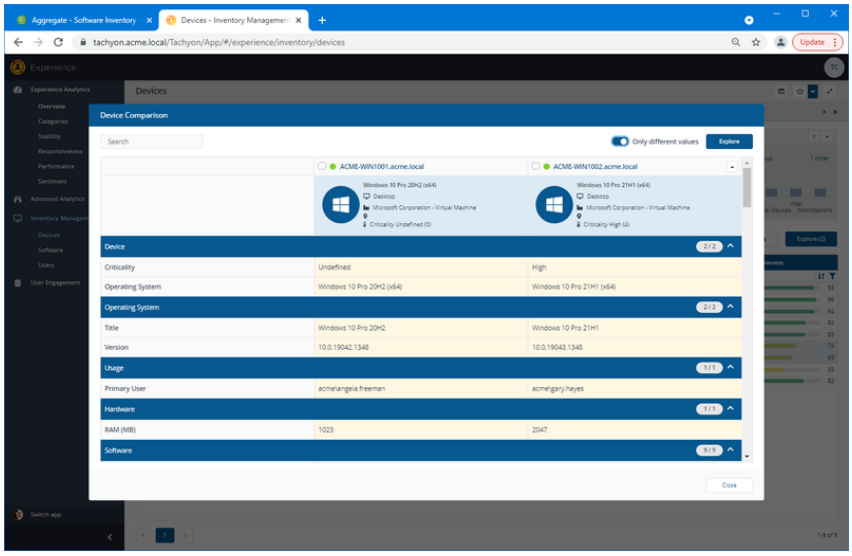
5.3.7.3.2 Comparing the settings for the devices

Initially, the **Device Comparison** popup shows all the parameters gathered from the devices, whether they are different or not. The differences are highlighted in yellow.



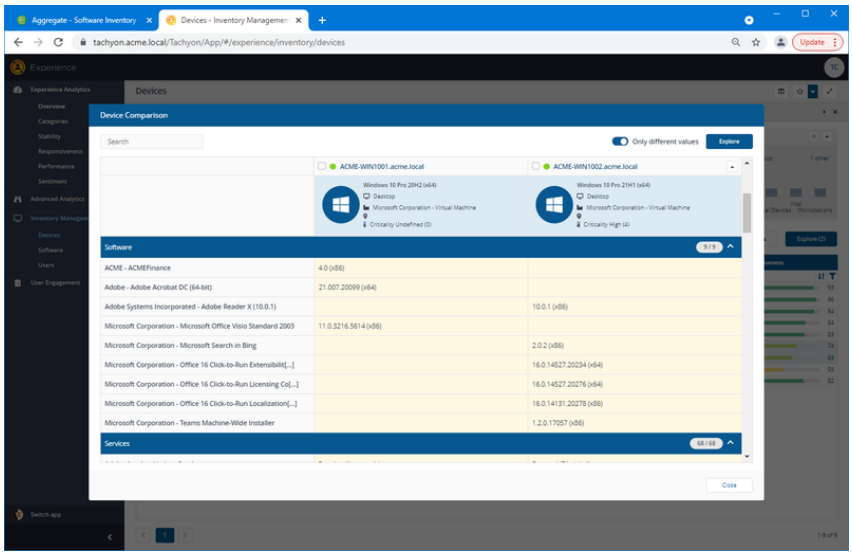
5.3.7.3.3 Focusing on the differences

You can focus on just the different value by flipping the **Only different values** toggle to on. The EUC manager notices some differences between the devices that may require some action - for example, the Operating System for the two devices is different and ideally for these devices they should be the same. However, they make a note of that for a future action and concentrate on tracking down the differences that may be significant to the Adobe Reader crashes.



5.3.7.3.4 Checking the differences in the installed software

Scrolling down the list of differences, they see in the **Software** section that two different versions of Adobe Acrobat\Reader are installed. The one on the device affected by the crashes is version **10.0.1 (x86)**, a very old version around 10 years out of date and with known vulnerabilities.

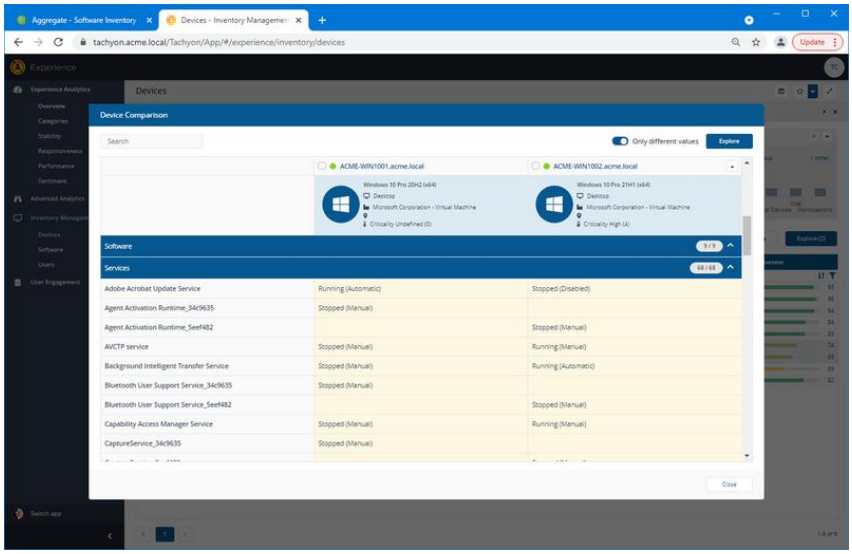


5.3.7.3.5 Checking the differences in the Services configuration

Checking the Services, they then see that the **Adobe Acrobat Update Service** is **Stopped (Disabled)** on the device affected by the crashes. So the device has an old version of the Adobe Reader installed, and the update service has been disabled. This strongly indicates the cause for the issue and suggests a possible resolution.

The EUC manager now needs to assign his team use Explorer to have the Adobe Acrobat Update Service to Started so that Adobe Reader will be updated on all devices where the old version is installed. Before doing this, there may be a need to send an announcement to all the affected devices to provide information about this

necessary change to the end-users on the devices, please refer to Broadcasting information via Announcements for more details.



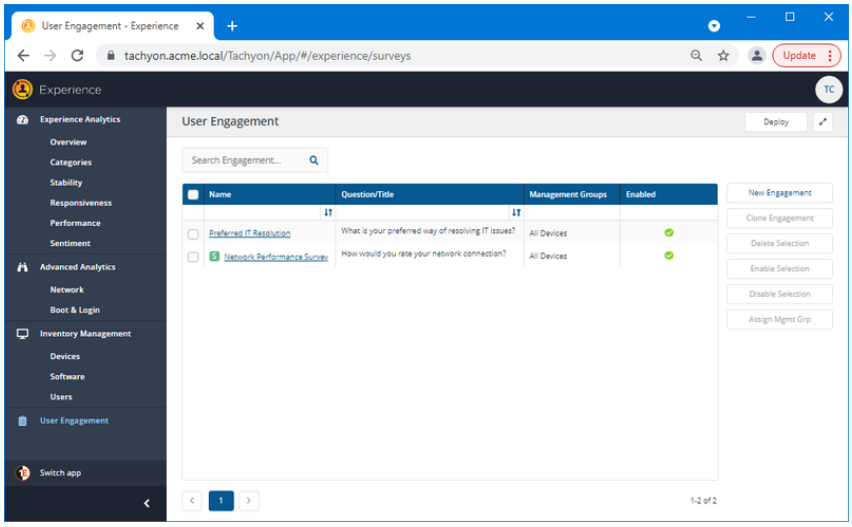
5.3.8 Broadcasting information via Announcements

In this scenario, the IT team want to notify users with certain older versions of Adobe Acrobat Reader that they are going to be upgraded to the latest version. The **end-user computing (EUC) manager** uses Experience to create and send an announcement that will be seen by the users on the devices in a specific Management Group.

5.3.8.1 Creating a new Announcement

The **Experience→User Engagement** page is where you manage all the Sentiment, Info Surveys and Announcements that have been created in Experience. You can easily see for each engagement the **Options** that it has been configured with, what **Management Groups** it has been assigned to and whether it's **Enabled** or not. In the picture, you can see the state following on from the Getting feedback via Info Surveys scenario.

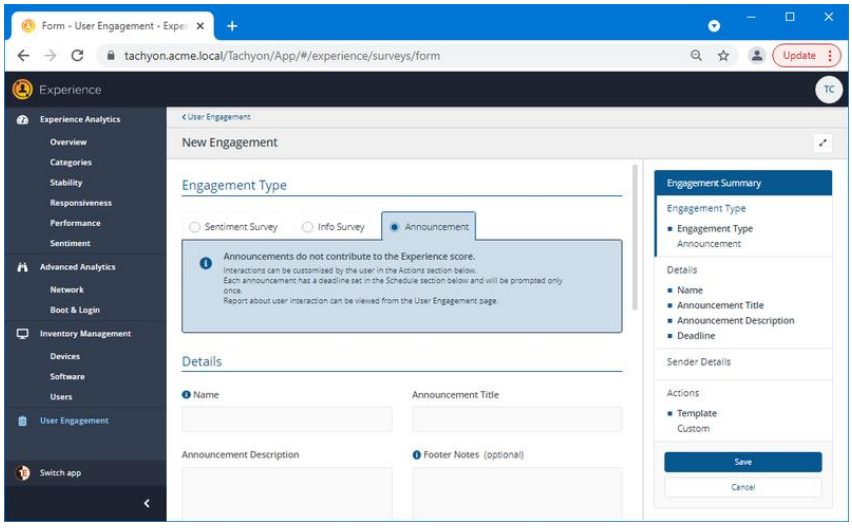
Click the **New Engagement** button to begin.



5.3.8.1.1 Announcements

In contrast to the survey types, Sentiment Survey and Info Survey, Announcement type engagements are used solely to broadcast information to end-users. You can still gather the results of sending the announcement, but this is only done to check that the information has been received. Announcements don't contribute to the Sentiment Score.

The picture shows the **Announcement** type selected.



5.3.8.1.2 Names, Announcement Titles and Descriptions, Footer Notes, Read more links, Deadlines and Priorities

Having selected the **Announcement** type, the next steps are to set a **Name** for the announcement, the **Announcement Title** and **Announcement Description** that will frame the purpose of the announcement. You can also optionally add **Footer Notes**, which can provide additional information in the announcement itself, and a **'Read more' link**, which can provide additional information for the announcement in the form of an externally available web page.

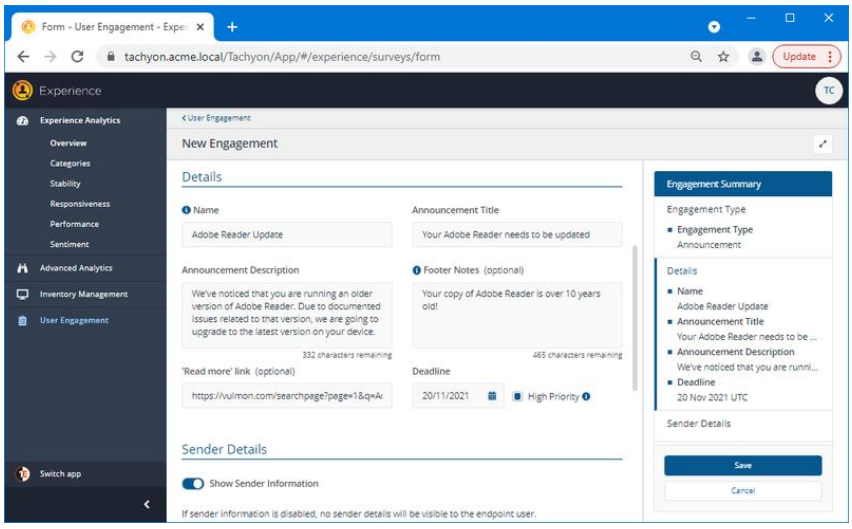
The **Name** for an Announcement is not stored as a metric that Experience can then report on. The **Name** must be unique amongst all the Engagement names that have been defined for Experience, but does not have to avoid other Metric names. For example, unlike Sentiment Surveys, **Network** on its own could be used as the **Name** for an announcement, even though this is already a metric that Experience reports on. It is best to choose a good name for the announcement that reflects the type of information being broadcast, so that it reminds you of its purpose if you encounter it on the **User Engagement** page at a later date, in this scenario the EUC manager names the survey: **Adobe Reader Update**.

The **Announcement Title** provides the headline for the information you are trying to get across to the end-user, if the headline has not been thought through carefully you will likely confuse your end-users and fail in your objective. In our scenario, the EUC manager sets the question to: **Your Adobe Reader needs to be updated**

The **Announcement Description** is displayed to the end-user just below the **Announcement Title** and should provide additional context. Use it to answer the likely questions that will arise from the announcement and provide some guidance as to what the user should expect. Here, the EUC manager sets the **Announcement Description** to:
We've noticed that you are running an older version of Adobe Reader. Due to documented issues related to th at version, we are going to upgrade to the latest version on your device. This sets the scene for why the action is being taken and gives a small indication on how it will increase the security on the end-user's device.

Footer Notes let you optionally provide additional bullet-points that emphasize your message. These are displayed in the announcement beneath the **Announcement Description**. In our example, the EUC manager adds **Your copy of Adobe Reader is over 10 years old!** as a footer note. This highlights just how out-of-date the installed version is and brings the message home that it needs to be replaced.

Optionally, the **'Read more' link** field can be set, which adds the text **Click here to find out more** to the announcement. The user can click on this link to find out related supplementary information. In our scenario, the EUC manager has found a page on a vulnerabilities listing site that deals with the particular version of Adobe Reader. That way the end-user can click on the **Click here to find out more** link in the announcement and check for themselves the vulnerabilities that are present on their device - because that version of the software is installed - again reinforcing the idea that an upgrade is required.



Announcements are only sent out once, and end-users can only make a response once. You can, however, set a deadline for receiving responses, this gives end-users a time range to acknowledge that they have seen and processed the information. Before the deadline occurs, users that haven't yet responded will be prompted repeatedly at appropriate times to respond. In this scenario, the EUC manager sets the **Deadline** to **20/11/2021**, giving their end-users a seven-day window to view the information. After that time, the announcement is closed and the prompts will no longer appear to targeted users who haven't yet responded.

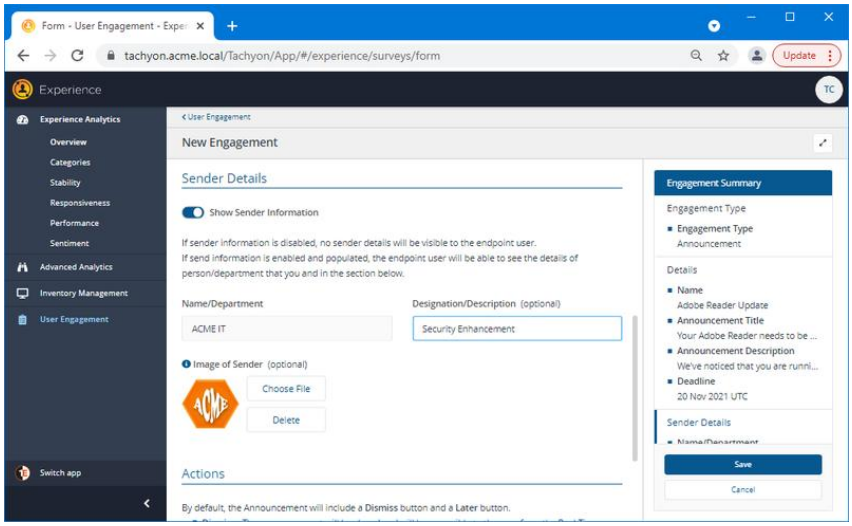
The final parameter in the **Details** section lets you determine how insistent the announcement will be. Setting the **High Priority** option ensures that the announcement will be delivered, even if the end-user has chosen to restrict notifications. You should use this option with care, as you don't want to be disturbing your end-users for every notification you want to send. If every notification is set to high priority, then none of them are.

In our scenario, the EUC manager is justified in setting this announcement to **High Priority**, as the action they intend to take will have an impact on the targeted end-users and will enhance the security and reliability of their device.

5.3.8.1.3 Setting the Sender Details

Announcements are a direct communication to your end-users, you will likely want that communication to be as well-received as possible. Part of that process is to provide information about exactly who wants the communication to be made. In this example it will be the ACME IT department who will take the action, but in another scenario, the announcement could just as well have been sent on behalf of the CEO for the company. You can imagine how this would affect the processing of the information by the end-user when they receive the announcement.

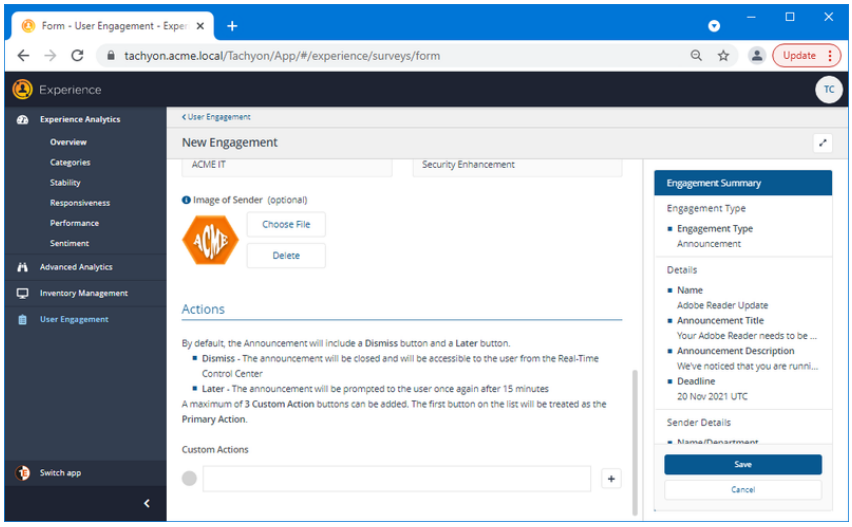
The EUC manager enables the **Show Sender Information** toggle, sets the **Name/Department** field to **ACME IT** and the optional **Designation/Description** to **Security Enhancement**, because that's the name of the project they are taking this action under. They also badge the announcement with the ACME logo to make it official and give it the company seal of approval.



The **Actions** section comes last in the Announcement Engagement editor. Here you can provide additional URLs tied to buttons, that can be triggered by clicking on each button - or in the case of the **Primary Action** button (the first one on the list), by hitting the <enter> key. For example, you may have set up a registration page on your company intranet that can be triggered by a URL. In this case you could create a **Please register** announcement, add a **Custom Actions** button called **Register** and set that to the URL. When an end-user subsequently receives the announcement asking them to register, they click on the **Register** button and it takes them to the registration page via the provided URL.

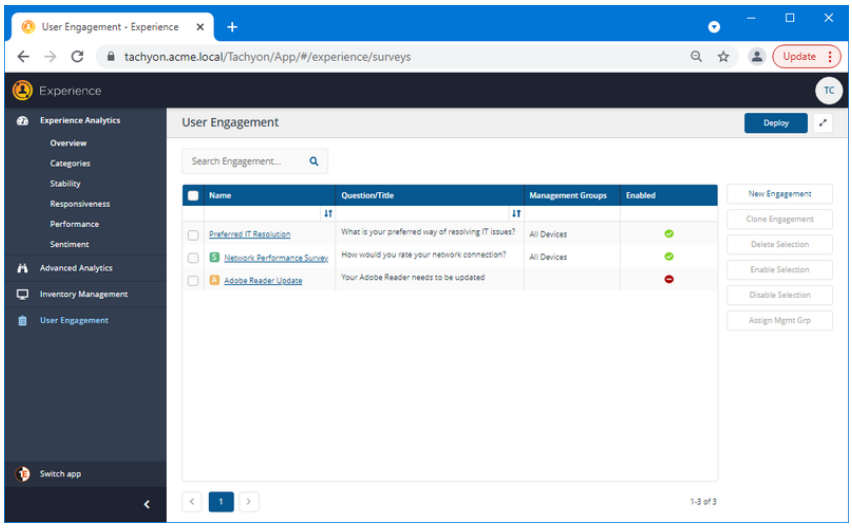
A second option, if your organisation allows is to provide a link to an App Store or Service Catalog, to allow users to update the software themselves.

In our scenario, the EUC manager doesn't have any **Custom Actions** they want to add to the announcement so they leave this section blank.



5.3.8.1.4 Saving the new announcement

When you're happy with the settings you've made in the survey editor you can click **Save** to commit the changes and continue to the next step. The picture shows the new announcement added with no Management Groups set and not yet enabled.

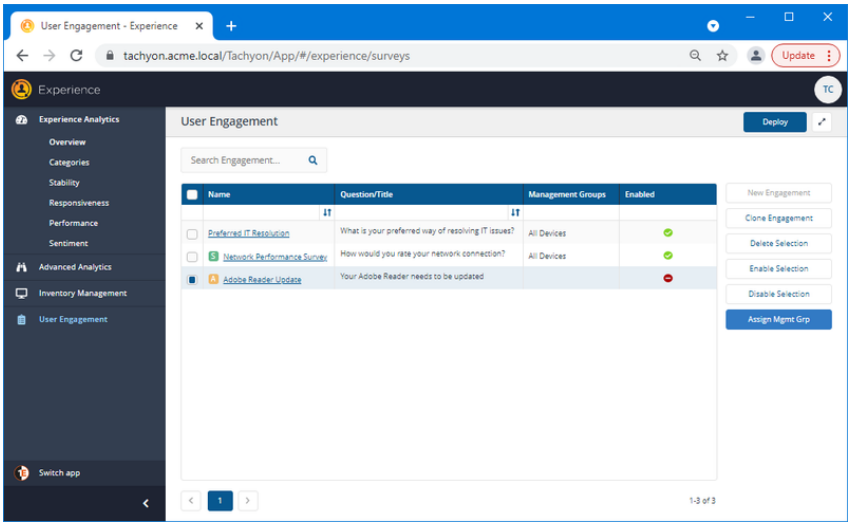


5.3.8.1.5 Setting the Management Groups for the new announcement

Announcements don't have a default Management Group, so one must be assigned before the survey can be enabled and then deployed. For this announcement, the EUC manager already has an **Old Adobe Reader Installed** Management Group defined that targets the devices they have identified where the old version is installed. They now need to set that as the Management Group for the announcement.

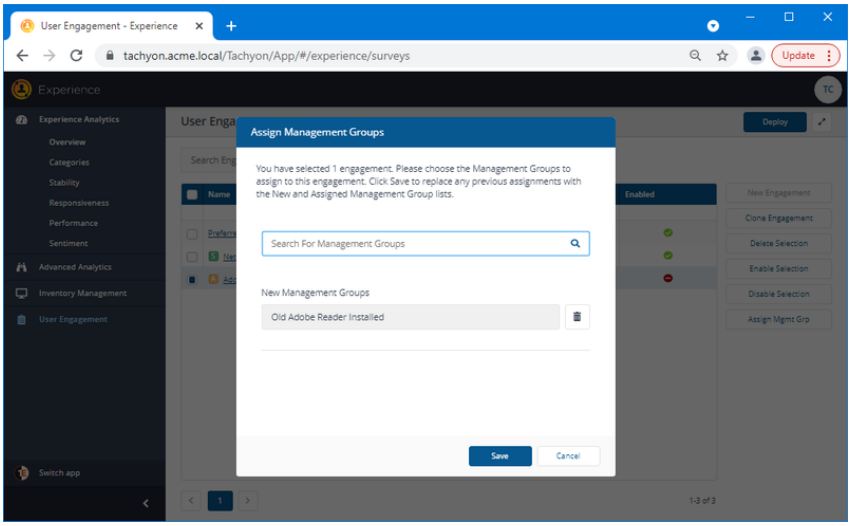
To do this:

They select the survey and then click the **Assign Mgmt Grp** button.



In the **Assign Management Groups** popup subsequently displayed, they type **Adobe** into the search field and then select **Old Adobe Reader Installed** from the list of matching Management Groups. This gets added to the **New Management Groups** field.

They click **Save** to assign the Management Group.

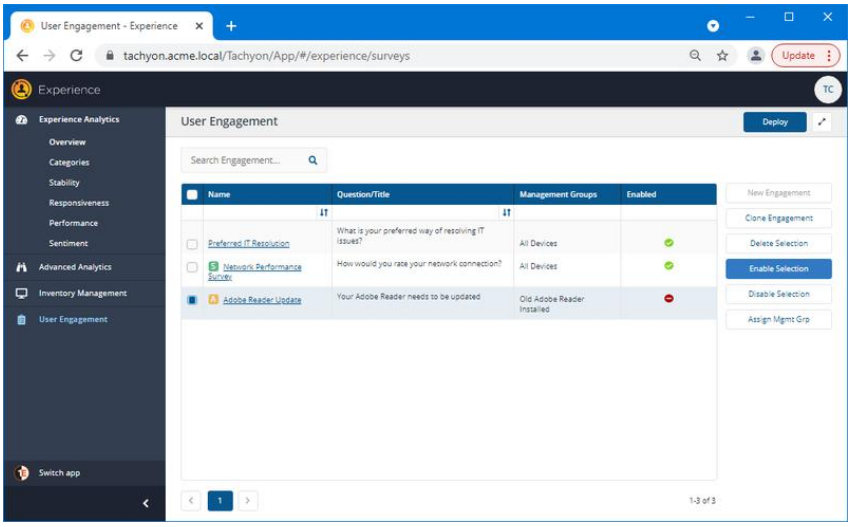


5.3.8.1.6 Enabling the new announcement

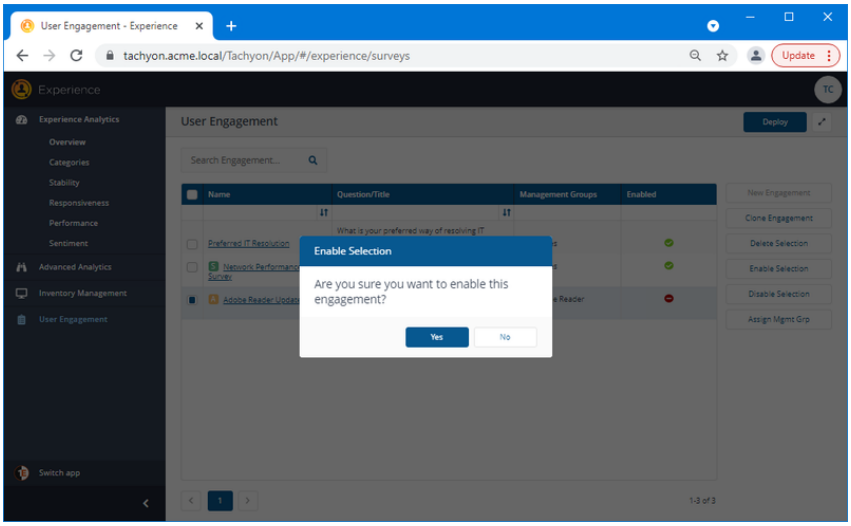
New engagements are not enabled by default. Before they can be deployed, they must be explicitly enabled, providing an additional gateway that prevents the engagement being sent out too soon before it's ready.

To enable the new announcement the EUC manager:

Selects the checkbox at the left-hand end of the announcement's entry in the Engagements table and then clicks the **Enable Selection** button.



Doing this displays an **Enable Selection** confirmation popup that you must acknowledge before the selected engagements are actually enabled. Click **Yes** to confirm the operation and **No** to cancel it.



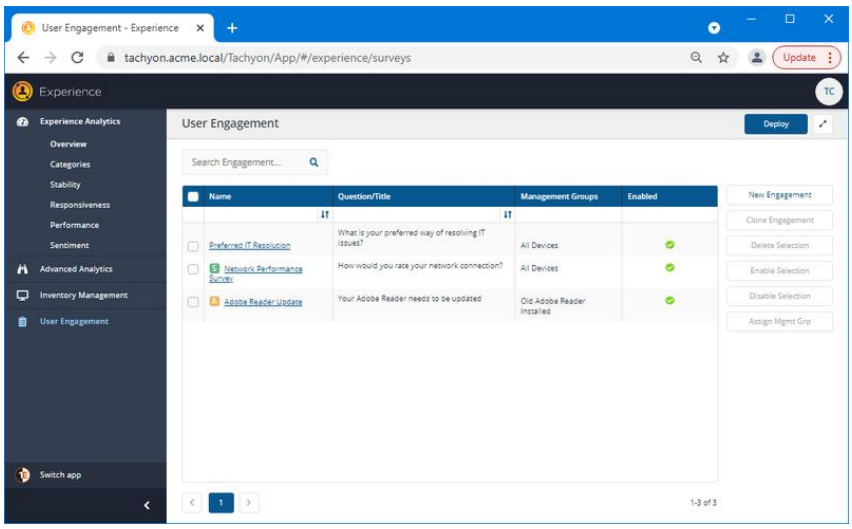
5.3.8.1.7 Deploying the new announcement

So the new announcement has the **Old Adobe Reader Installed** Management Group assigned and has also been enabled, it can now be sent to the end-users' devices by clicking the **Deploy** button, which will send the announcement to all the devices in the selected Management Group, that are currently or subsequently connected to Tachyon.

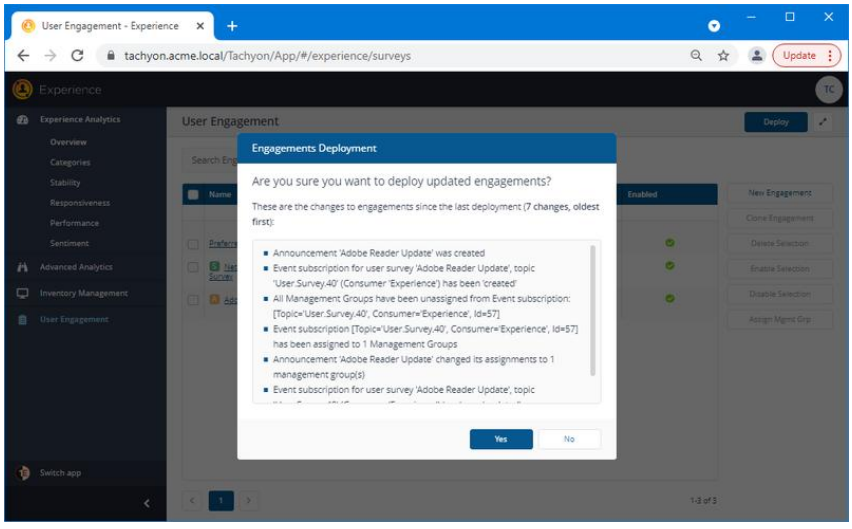
> **Note**
>
> The **Deploy** button will send out any changes to the states of the engagements - meaning you can also use it to set previously deployed engagements to not **Enabled**, thereby preventing further responses without completely deleting the engagement, or you can delete engagements when they are no longer needed. You should be aware that the **Deploy** button will also send any other User Engagement administrator's changes.

It is usually good practice to test the engagement on a few machines first before deploying to **All Devices**. This lets you see how the engagement will appear to your end-users and gives you the opportunity to debug the text and options before deploying to a wider audience. Doing this involves assigning a different Management Group to the survey that targets the selected test devices.

In our example, which only involves a few devices anyway, to keep things simple we can get away with sending the announcement out without testing, so the EUC manager clicks the **Deploy** button.



An **Engagements Deployment** popup appears that shows the changes that will be deployed when the **Yes** button is clicked. The EUC manager reads the list carefully, sees that the only changes are the ones related to creating, assigning Management Groups and enabling the **Adobe Reader Update** announcement and clicks **Yes**. Subsequently, a notification will appear showing that the policy changes are being applied to the Tachyon Agents.



5.3.8.2 What the end-user sees

When the 1E Client is installed on a network device, by default it also adds an icon to the notification area that displays the Real-Time Control Center (RTCC). Initially the icon may be

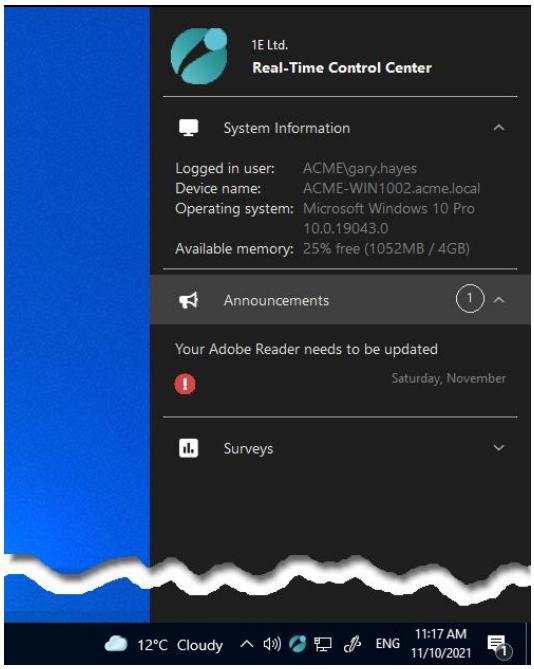
hidden, but may be dragged onto the taskbar to make it always visible. When an end-user clicks on the notification icon they will see the **Announcements** and **Surveys** that have been deployed to the device.

5.3.8.2.1 When does the announcement appear?

To minimize the disruption to the end-user of having an announcement pop up when they're busy using the computer for other things, the 1E Client has a few heuristics that govern when the notifications appear. These measure and compare things like: whether the user is currently interacting with the device, how long it has been since they stopped interacting with the device, how long the notifications should wait before re-displaying if the user didn't respond to the last time it was displayed. These various options interact to essentially display the notification in the sweet spot between the user not actively doing something and the user having left their device.

> **Note**
>
> Your end-users can also set the **Do not disturb** option, which usually prevents notifications from appearing for a configurable time period. However, the Experience Engagement Administrator can also override this option by setting an announcement to High Priority, so that the announcement will appear regardless of the user's selection in the **Do not disturb** option - as is the case in our scenario.

Announcements are also accessible from the **Real-Time Control Center**, which allows the end-user to access them directly at any time.

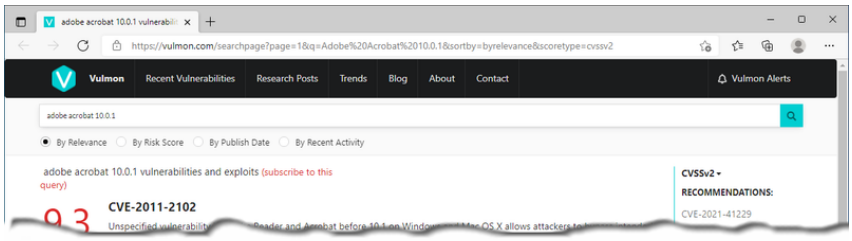


5.3.8.2.2 Interacting with the announcement

In our scenario, the deployed announcement pops up on an end-user's device. They can see from the announcement title that their Adobe Reader needs to be updated, and from the description

text, why this is necessary and what is going to happen. A footnote on the announcement highlights the fact that the installed version is over 10 years old.

The announcement has been configured with a URL that links to a page with more information. Clicking on the**Click here to find out more**link opens the linked page in their default browser. Here, they can read more about the vulnerabilities associated with the installed version of adobe reader and along with the description and footnote in the announcement feel re-assured that upgrading is the right choice.

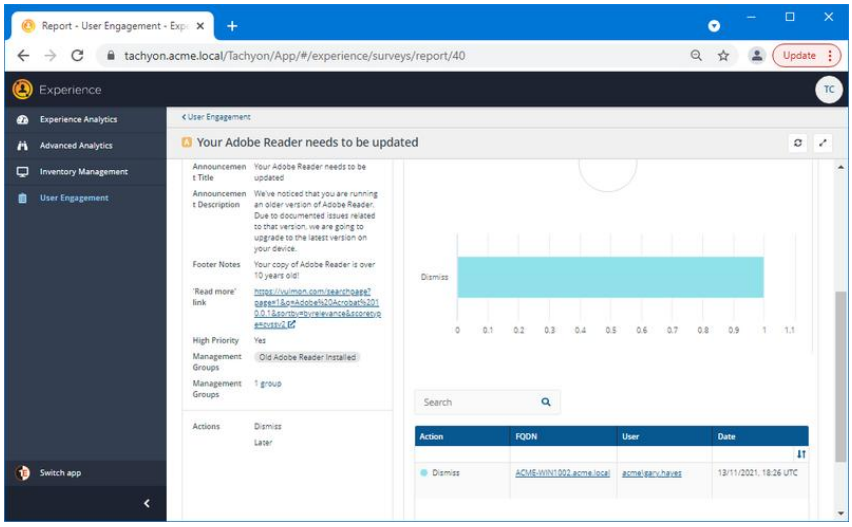


Announcements provide two default buttons, **Dismiss** and **Later**, Clicking **Dismiss** indicates that the end-user has read and processed the announcement. Clicking **Later**, means that they don't want to be bothered just at this moment but may respond when the notification is next displayed.

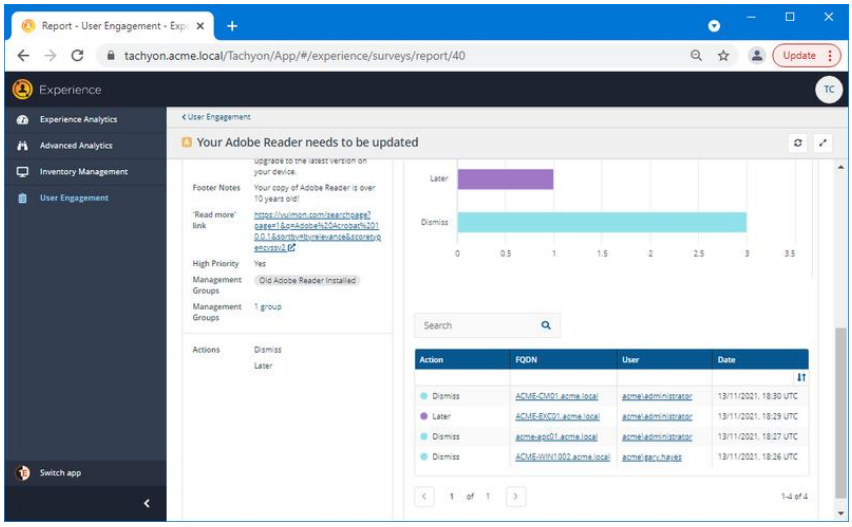
5.3.8.3 Viewing the announcement responses

The **Adobe Reader Update** announcement has been deployed and end-users have begun to respond, the EUC manager wants to monitor those to see who has read the announcement. For an announcement the only place the responses can be viewed is from its details page, you get to this by clicking on the link for the announcement in the **Name** column of the Engagements table on the **User Engagement** page.

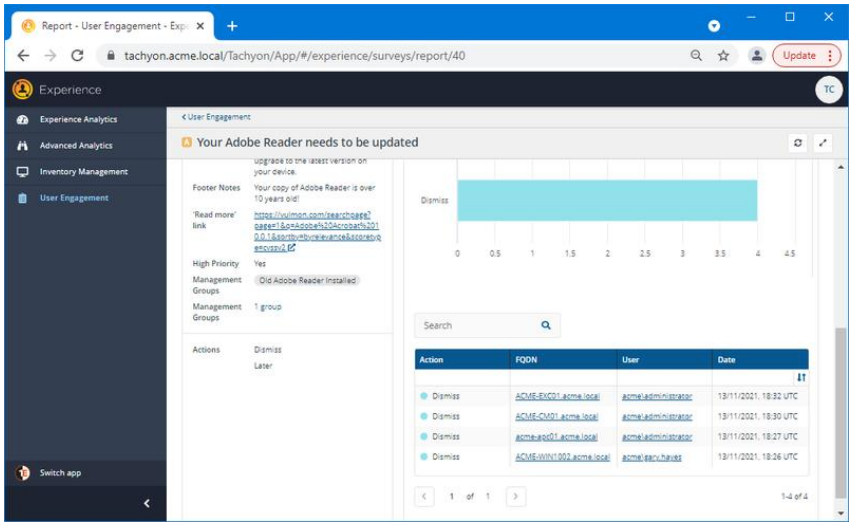
In the picture, the EUC manager has clicked on the **Adobe Reader Update** link to display its details page. Here, they can see that a user has submitted a response. **Dismiss** in this case is likely a good response to the announcement, indicating that the end-user has at least looked at the announcement and clicked the **Dismiss** button.



After a number of responses have been made, a clearer picture of the current user behavior appears. Most of them have clicked the **Dismiss** button, and just one has clicked **Later** to receive the announcement at a later time.



Finally, the EUC manager checks the results again and sees that all the targeted end-users have responded. They can now go ahead and remediate the Adobe Reader issue knowing that the affected users have been notified.



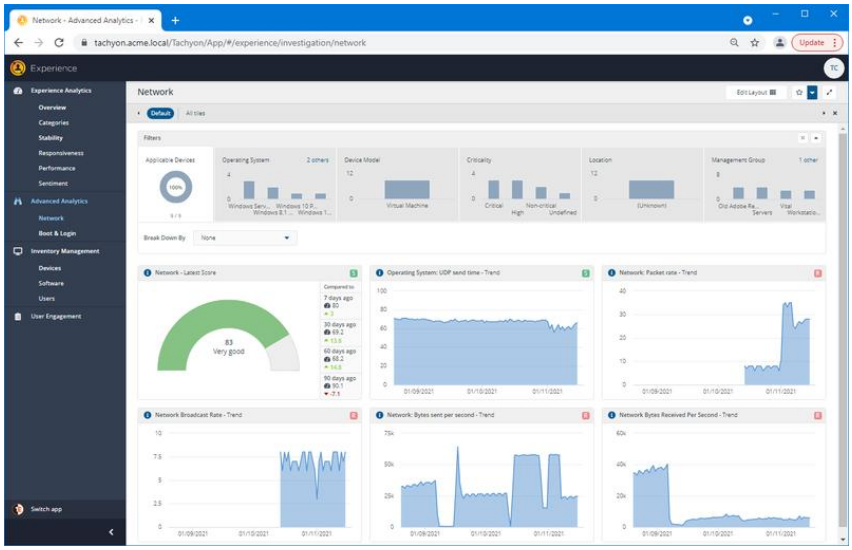
5.3.9 Investigating Network Performance

In this scenario, the EUC manager uses the **Advanced Analytics→Network** page of Experience to monitor and examine experience related to the network performance for devices.

5.3.9.1 Taking a look at the Network page

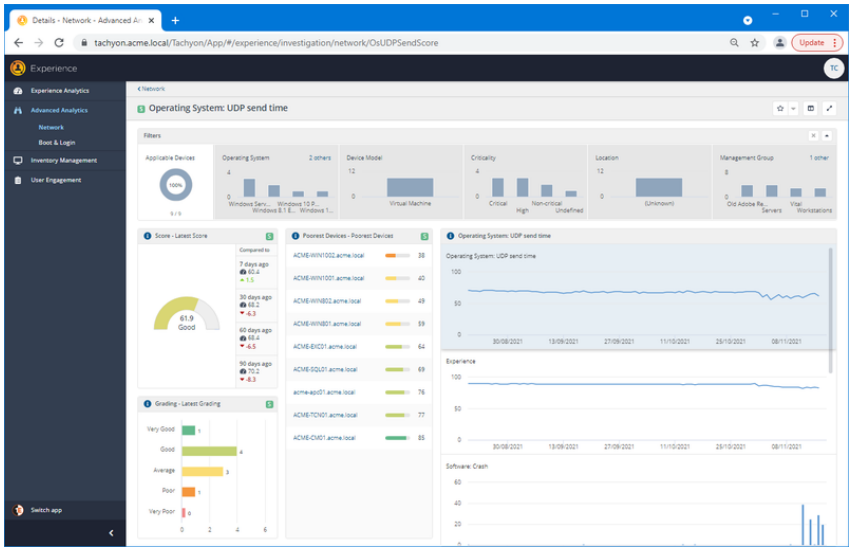
The **Advanced Analytics→Network** page provides a dashboard where network performance data can be examined. By default, there are two score related tiles: **Network - Latest Score** and **Operating System: UDP send time - Trend**. The rest of the tiles show averages of the raw, unprocessed data being measured across all the devices.

The EUC manager navigates to the **Advanced Analytics→Network** page, sees that the general overall score is **83 Very good**, but also sees that there's been a bit of fluctuation for the measurements on the other tiles showing the averaged raw data.



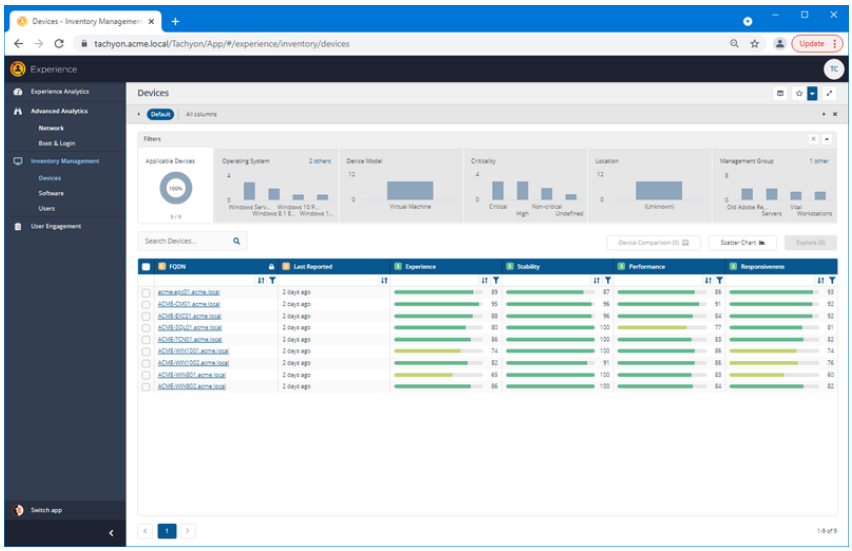
5.3.9.1.1 Focusing on the UDP send time

Looking at the trend on the **Operating System: UDP send time - Trend** tile, they notice that there has recently been a dip in the score. Clicking on one of the data points in the chart navigates to the **Operating System: UDP send time** page. Here they can see in the **Poorest Devices** tile that a few devices aren't performing particularly well in that area. There is also a recent downward trend for the Experience score that matches the fluctuations in the UDP send time.



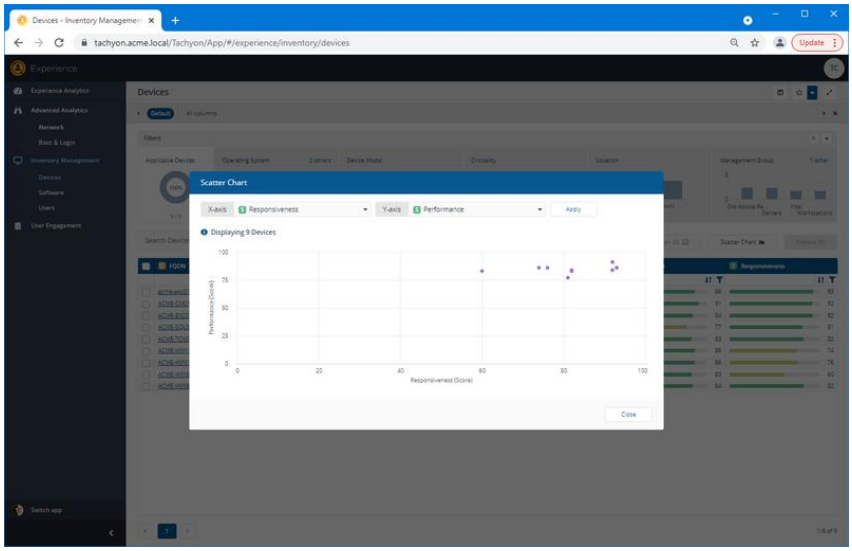
5.3.9.2 The Devices page

Navigating to the **Inventory Management→Devices** page enables the EUC manager to investigate the devices using the Scatter Chart popup. To display this, click on the **Scatter Chart** button just above the devices table.



5.3.9.2.1 The Scatter Chart

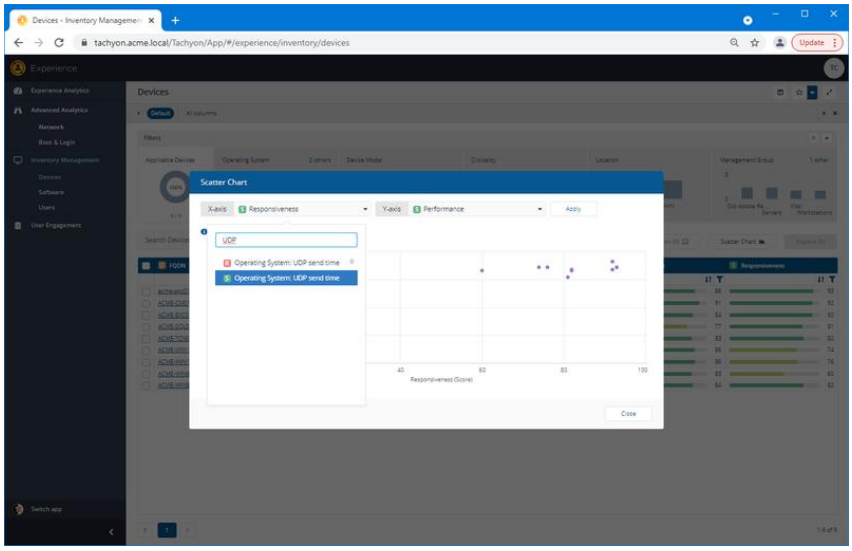
The Scatter Chart plots the devices in the current view on a chart with two selectable axes. Initially, this shows the **Responsiveness** score on the **X-axis** and the **Performance** score on the **Y-axis**. In our example, the devices are all situated in the ideal top-right quadrant for these two scores.



5.3.9.2.2 Selecting the UDP sent time score for the X-axis

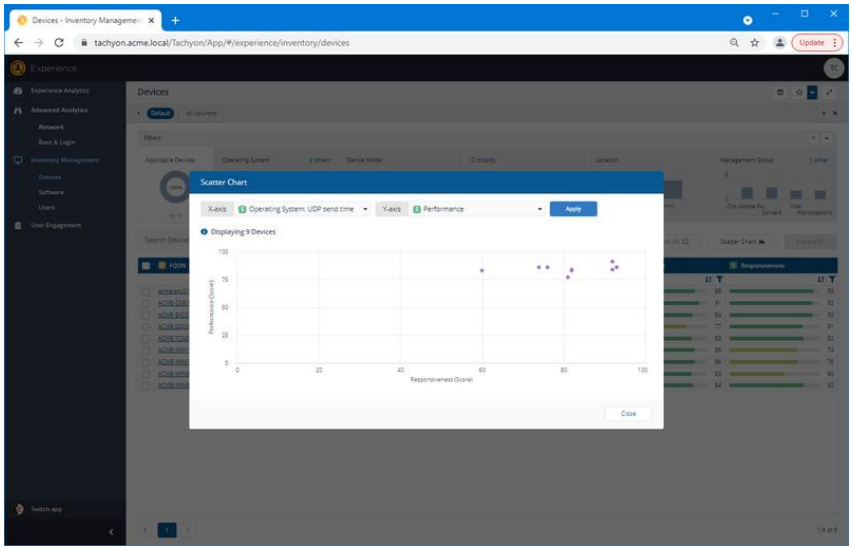
The EUC manager wants to plot the devices according to the UDP send time, in order to determine both the poorest and best scoring devices. Clicking on the drop-down menu next to the X-axis field, displays the list of available parameters. You can choose from a selection of score or raw values. Typing into the search field filters the available parameters to those that match.

In our example, the EUC manager types **UDP** into the search field and then selects the **Operating System: UDP send time** score from the list of matching parameters.



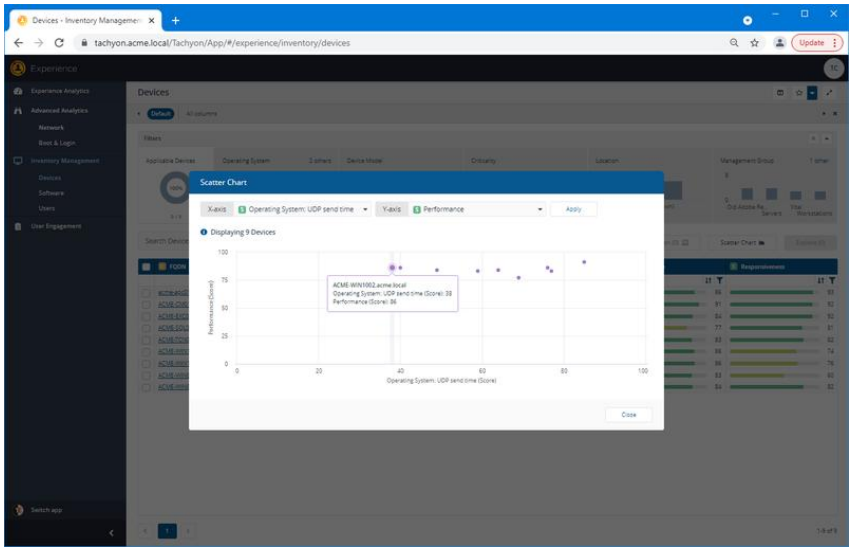
5.3.9.2.3 Applying the selected change to the X-axis

When you make a change to either axis parameter, you then need to click **Apply** to change the plot of the Scatter Chart. The picture shows the **Apply** button highlighted.



5.3.9.2.4 The device with the lowest UDP send time score

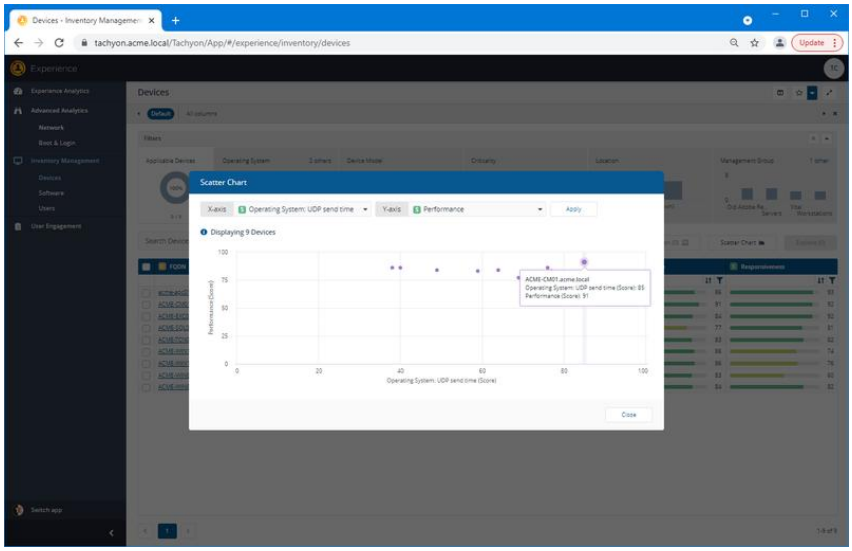
When the devices are plotted using the **Operating System: UDP send time** along the X-axis, the poorest score is displayed on the left. Hovering over a point, shows the FQDN and X and Y values for that device. Here, the EUC manager can see that the device with the poorest UDP send time score is **ACME-WIN1002.acme.local**.



5.3.9.2.5 The device with the highest UDP send time score

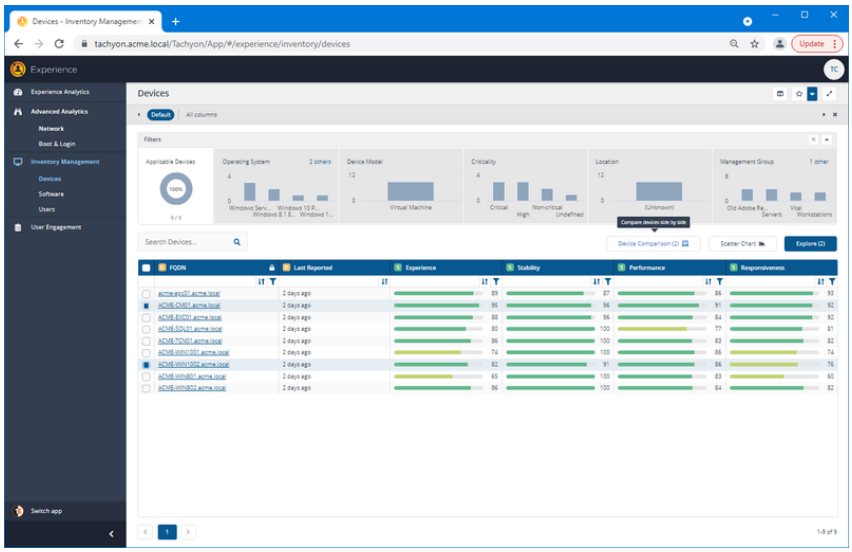
Correspondingly, hovering over the point furthest to the right displays the details for the device with the highest UDP send time score. In our example, this is **ACME-CM01.acme.local**. Having

made a note of the devices with the lowest and highest UDP send time scores, the EUC manager clicks the Close button on the **Scatter Chart** popup.



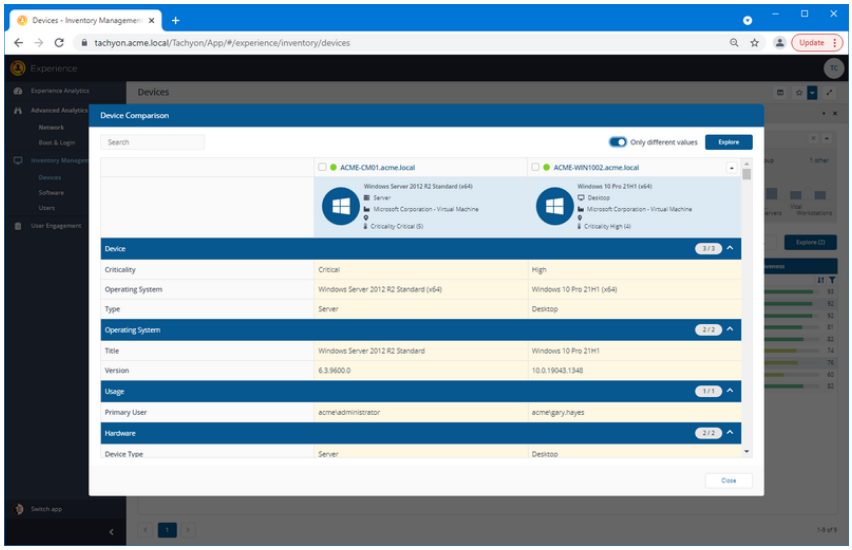
5.3.9.2.6 Selecting the devices with the lowest and highest UDP send times

On the **Devices** page, the EUC Manager selects the two devices they made a note of earlier, and then clicks the **Device Comparison** button.



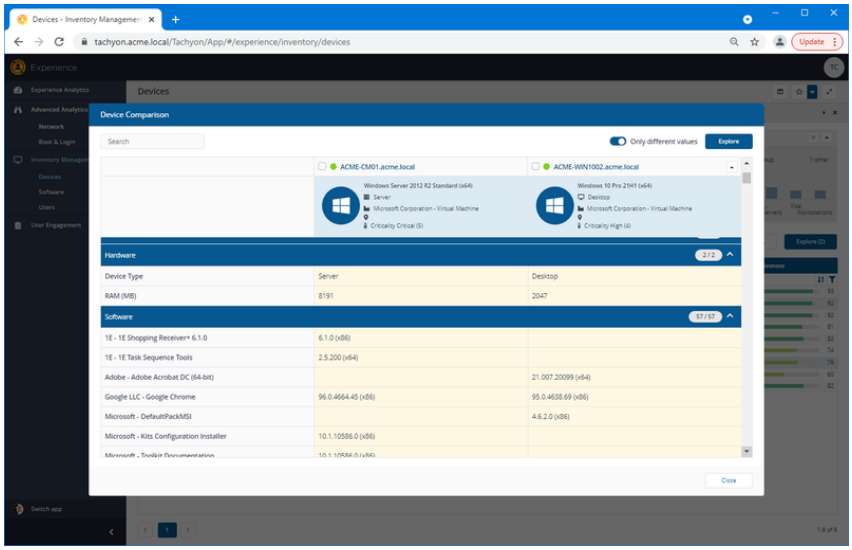
5.3.9.2.7 The Device Comparison popup set to display only different values

When the **Device Comparison** popup is displayed, the EUC manager first turns on the **Only different values** toggle - to concentrate on the differences. They can see that the two devices have different Operating Systems, which may or may not be significant.



5.3.9.2.8 A possibly significant difference

Further down in the **Hardware** section, another, more significant difference is shown. Here, the EUC manager can see that the device with the best performing UDP send time score has 4 times as much **RAM (MB)** as the poorest one. As they know that these are both virtual devices, they conclude that this may be a contributing factor to the differences in throughput performances. The next step would be to test assigning more RAM to the device with the poorest UDP send time and see if this resolves the issue.



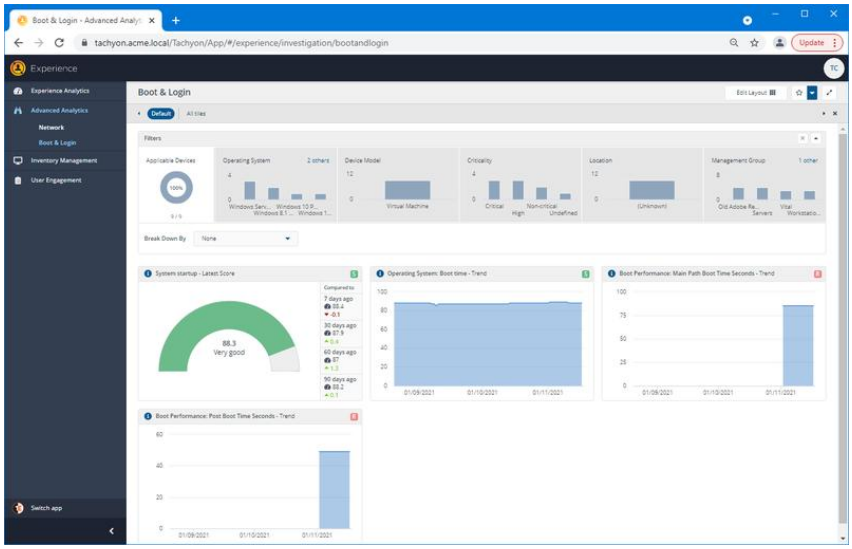
5.3.10 Investigating Boot and Login Performance

In this scenario, the EUC manager uses the **Advanced Analytics→Boot & Login** page of Experience to monitor and examine experience related to the boot and login performance for devices.

5.3.10.1 Taking a look at the Boot & Login page

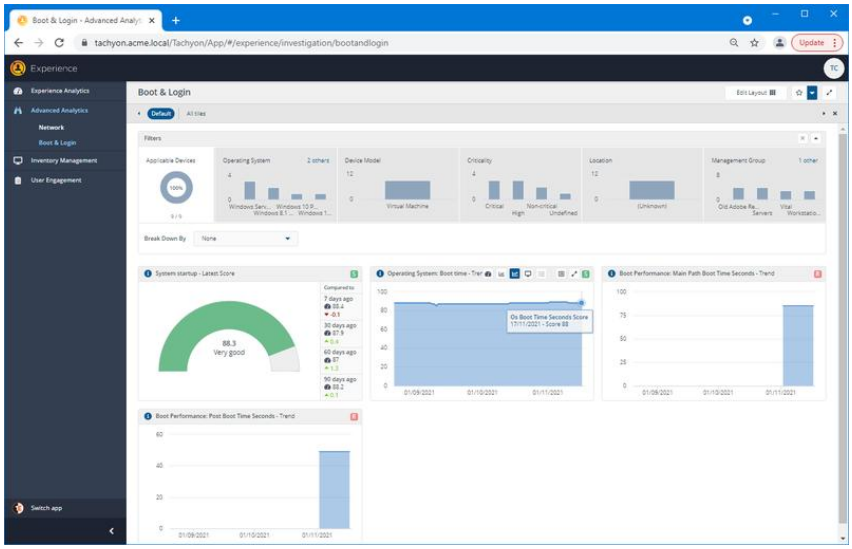
The **Advanced Analytics→Boot & Login** page provides a dashboard where boot and login performance data can be examined. By default, there are two score related tiles: **System startup - Latest Score** and **Operating System: Boot time - Trend**. The rest of the tiles show averages of the raw, unprocessed data being measured across all the devices.

The EUC manager navigates to the **Advanced Analytics→Boot & Login** page, sees that the **System startup - Latest Score** is **88.3 Very good**, but also sees that there's been a very slight downward trend for both the System startup score over the past 7 days and for the **Operating System: Boot time**.



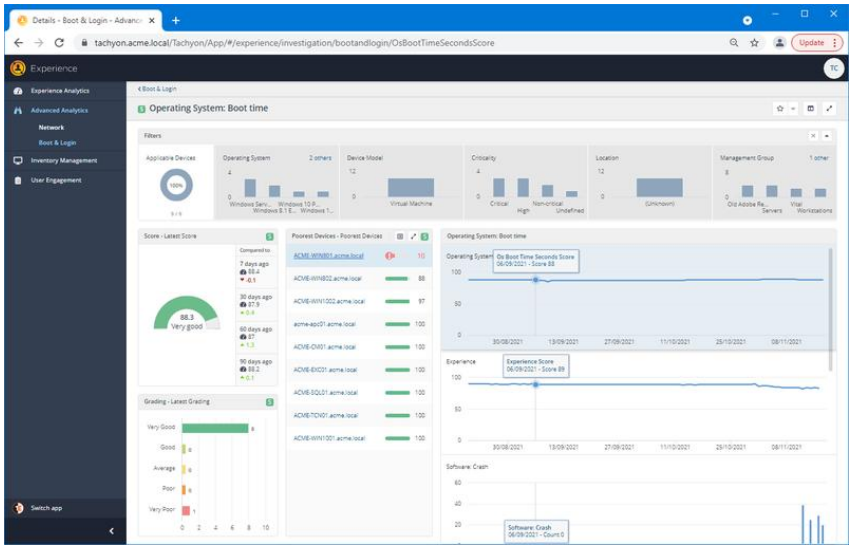
5.3.10.1.1 Focusing on the Boot time

Looking at the trend on the **Operating System: Boot time - Trend** tile, they click on one of the data points in the chart, which navigates to the **Operating System: Boot time** page.



5.3.10.2 The Operating System: Boot time page

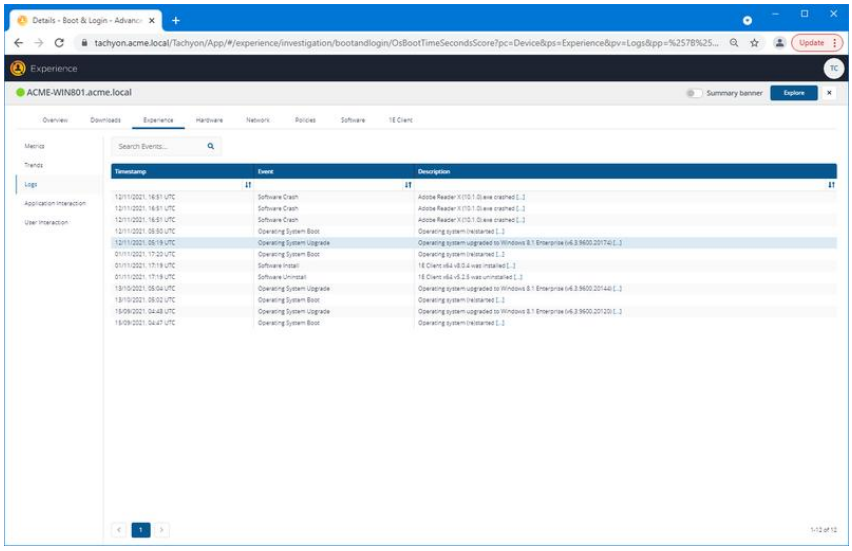
Here, the EUC manager can see in the **Poorest Devices** tile that one device isn't performing particularly well on its boot time score. Selecting the device FQDN link displays its device details.



5.3.10.2.1 A possibly significant sequence of events

From this link, the device details opens on the **Experience** tab with the **Logs** panel displayed, which shows the system events for the device. Here, the EUC manager sees that the most recent **Operating System Boot** event for this device has occured just after an **Operating System Upgrade**.

They conclude that this may be a contributing factor to the poor startup time and that they can safely overlook the issue for the time being. However, they make a note of the device name just in case there is actually an ongoing issue that stems from another cause.



5.3.11 Creating your own dashboard

Experience allows you to customize and save your own dashboards for viewing later, the saved dashboards are called Presets. This tutorial shows you how to create and use them.

The ability to customize dashboard views is common to the following Experience pages.

Experience page	Pages with customizable dashboard views
Experience Analytics	Stability
	Responsiveness
	Performance
	Sentiment
Advanced Analytics	Network
	Boot & Login
Inventory Management	Devices
	Software
	Users.

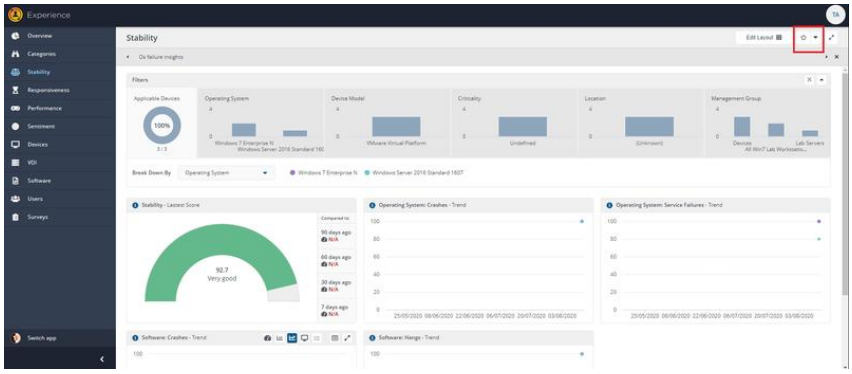
At the top of pages where you can customize the dashboard you'll see the controls highlighted in the picture.

> **Note**
>
> Before saving the dashboard you may want to choose which metrics to show in your custom Preset view. The way you choose metrics differs depending on the page you're customizing:

Stability, Responsiveness, Performance, Sentiment, Network and Boot & Login pages use **Edit Layout**

Devices, Software, and Users pages use **Select Metrics**.

> For a detailed walkthrough of how to choose and save the metrics for your new Preset, please refer to Adding metrics to a dashboard.

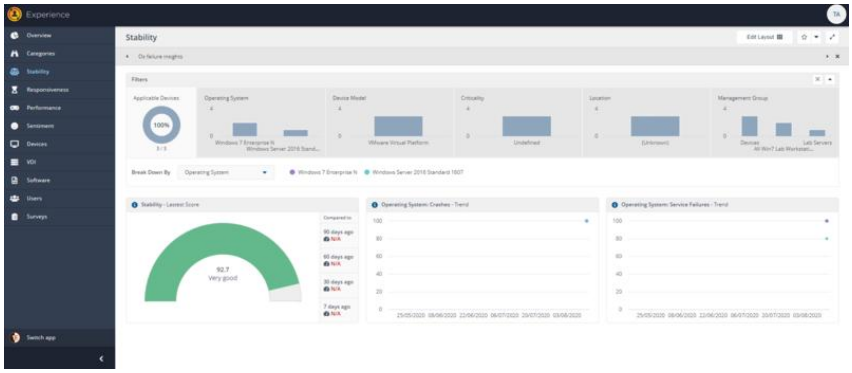


Our example shows the**Stability**page where the tiles displayed have been edited to focus on the following metrics:

Stability - Latest Score

Operating System: Crashes - Trend

Operating System: Service Failures - Trend.



To save the preset we click the star button on the top right of the page, called **Save the configuration as preset**. This opens the **Presets** popup where we can set the **Preset Name** and save the Preset view for our selected metrics:

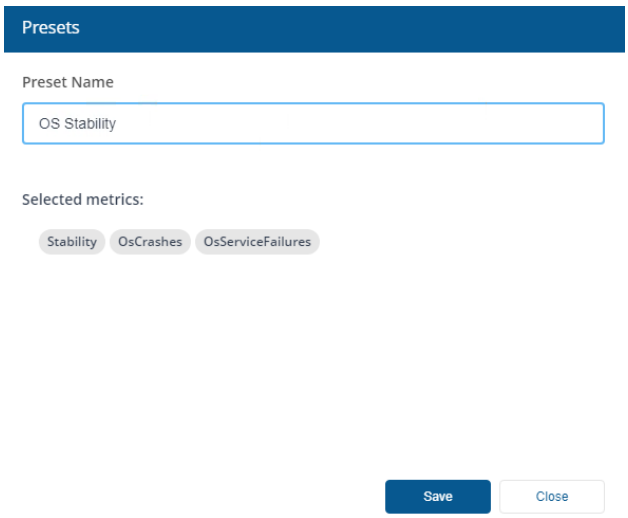
Stability

OsCrashes

OsServiceFailures.

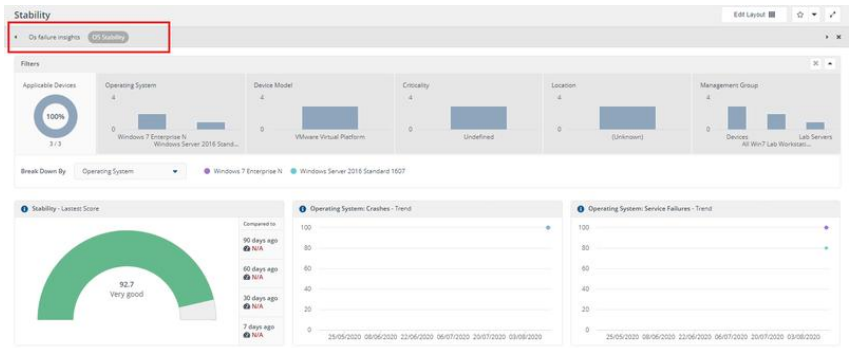
Your selected metrics and filters will show on this screen.

We'll set the **Preset Name** as **OS Stability** and click **Save** to return to the Stability dashboard page.

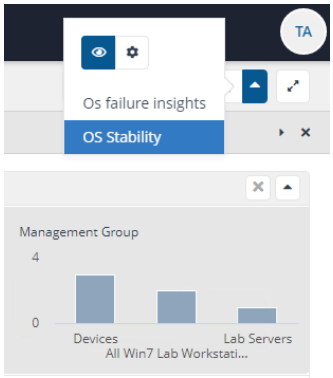


Now, on the **Stability** page our Presets are shown at the top of the page on the preset view bar. When you have multiple Presets on the presets bar, you can view that preset dashboard by selecting one of them.

> **Note**
>
> The preset bar can be closed using the **X** icon on the right side of the bar. You can reopen the preset bar by using the down arrow next to the star icon and selecting the eye icon.
>
> The preset bar is also reopened when current page is manually reloaded, or when you navigate to another page the preset bar will be open when you return.



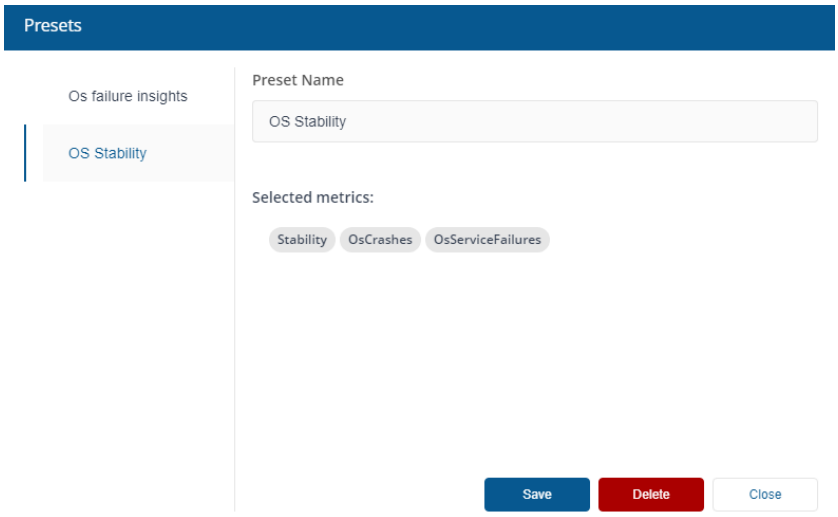
To view (eye icon) or manage (gear icon) a Preset, click the down arrow next to the star button.



When you click the gear icon you can do either of the following:

Changethe name used for the selected Preset by editing the **Preset Name** field then clicking **Save**.

Delete the selected Preset by clicking the **Delete** button.



5.3.12 Adding metrics to a dashboard

It is possible to change the displayed metrics for a dashboard in order to view different data in Experience.

Experience allows you to create custom dashboards and choose which metrics are displayed on them. The saved dashboards are called Presets. This tutorial shows you how to choose the metrics for these custom preset dashboards.

The ability to customize dashboard views and choose which metrics are shown on them is common to the following Experience pages:

Stability

Responsiveness

Performance

Sentiment

Devices

Software

Users.

At the top of each page where you can customize the dashboard, depending on the page you're viewing you'll see either an **Edit Layout** or a **Select Metrics** control:

Edit Layout- used on the Stability, Responsiveness, Performance and Sentiment pages

Select Metrics- used on the Devices, Software, and Users pages.

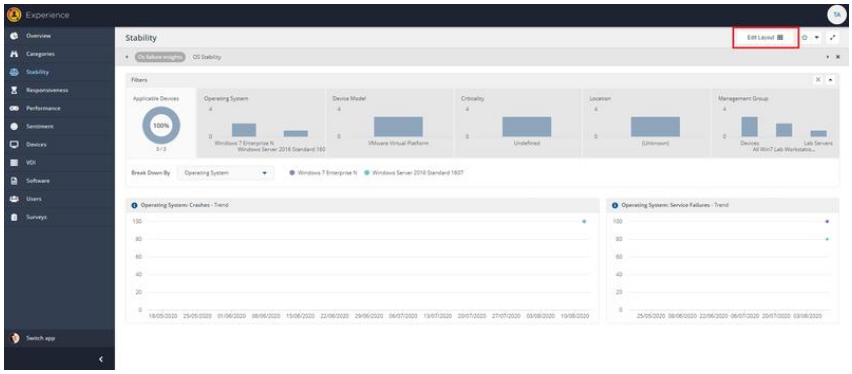
Note

For a detailed walkthrough of how to create custom dashboards for your chosen metrics, please refer to Creating your own dashboard.

5.3.12.1 Edit Layout

The **Edit Layout** control only applies to the Stability, Responsiveness, Performance and Sentiment pages.

To choose the metrics to display on your dashboard, click the **Edit Layout** control as highlighted in the picture.



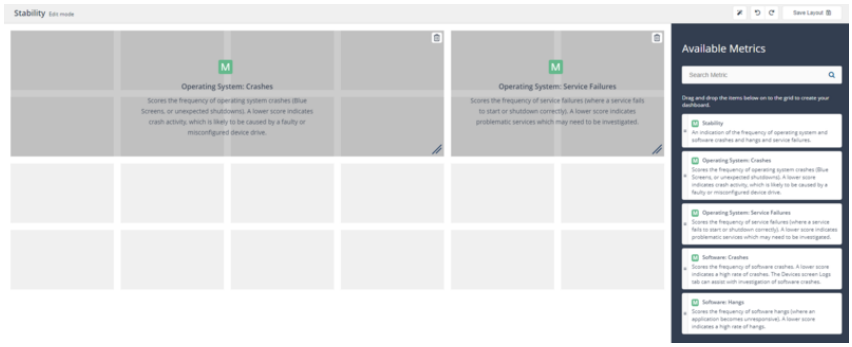
When you're in **Edit mode** you can choose which metrics are displayed on your dashboard. You can:

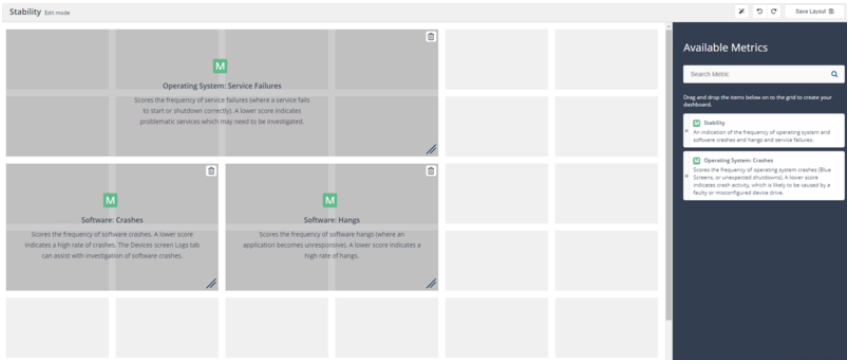
Add metrics from **Available Metrics** by using drag and drop on to the grid to create your dashboard

Remove metrics from your dashboard by clicking the trash can icon on metric panels in the left-hand pane

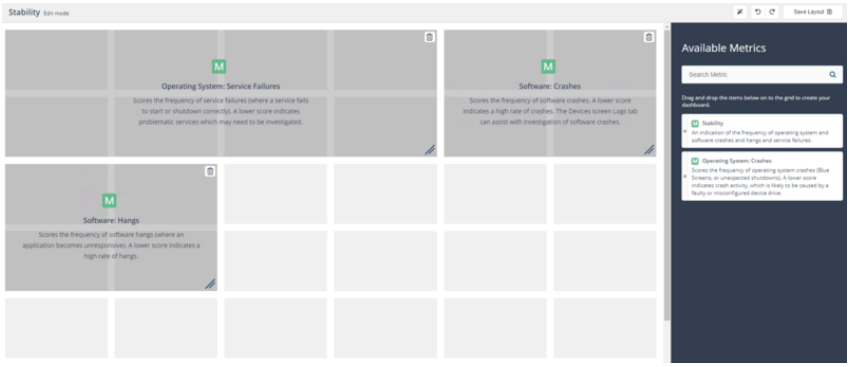
Resize how much of the dashboard an individual metric uses by dragging the bottom right-hand corner of a panel using the squared background as a guide.

In our example we chose to add **Software: Crashes** and **Software: Hangs** and remove **Operating System: Service Failures**. We also want the**Operating System: Service Failures**to have more visibility on the dashboard, so we have expanded this view.





You can also use the **optimise space** icon (magic wand) on the top right-hand corner of the page, which automatically adjusts the view to remove any potential gaps on the dashboard. In our example clicking the **optimise space** icon gives us the result in the picture.



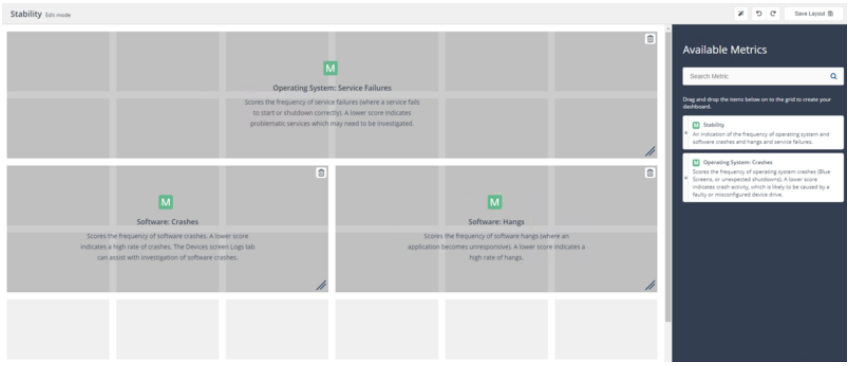
In our example we preferred to manually adjust the view so that **Operating System: Service Failures** covers the top of the dashboard with **Software: Crashes** and **Software: Hangs** underneath.

Using the **undo** icon on the top right-hand corner of the screen we undid the **optimise space** action and then manually expanded **Operating System: Service Failures**, **Software: Crashes** and **Software: Hangs** to fill the space.

We then clicked **Save Layout** on top right-hand corner of the screen, to save this layout and return to the dashboard view.

Note

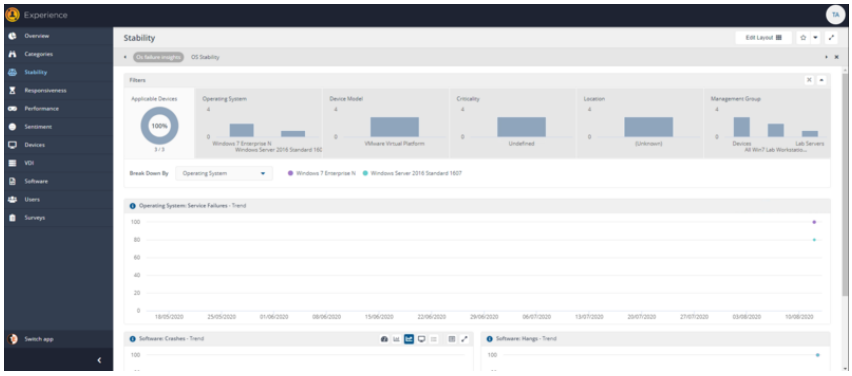
To reverse your changes in edit mode, either use the undo button on the top right-hand corner of the screen. You can also reload the page to return to the selected dashboard without saving your changes or use the back button on your browser.



Now we have chosen the metrics to display on our dashboard we can add it to the list of Preset dashboards.

Clicking the star icon in the top right-hand corner of the screen will give you the option to save this view as a Preset dashboard you can return to a later date.

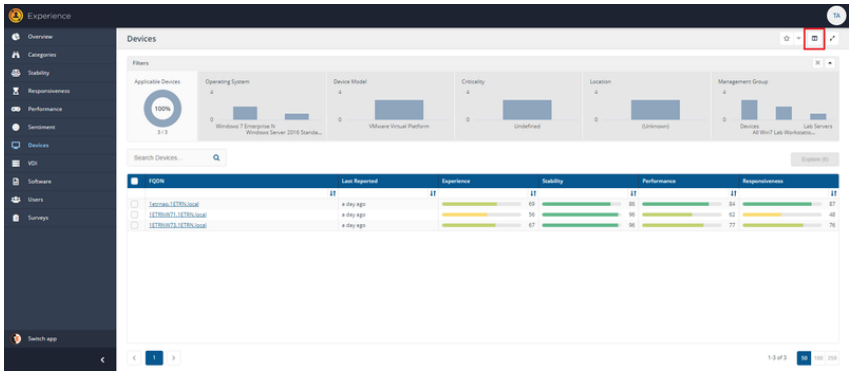
> **Note**
>
> For a detailed walkthrough of how to save Preset dashboards for your chosen metrics, please refer to Creating your own dashboard.



5.3.12.2 Select Metrics

The **Select Metrics** control only applies to the Devices, Software, and Users pages.

To choose the metrics to display on your dashboard, click the **Select Metrics** control as highlighted in the picture.



The **Select Metrics** control allows you to add different metrics or remove metrics that are visible on the currently displayed dashboard.

In our example, we'll remove the **Experience** metric to focus on **Stability**, **Performance** and **Responsiveness**. We can do this by selecting the **Experience** metric and clicking the double arrow icon to remove it from the list of **Visible Metrics** and add it to the list of **Available Metrics**.

In addition, you can:

Drag and drop columns to change the order they are displayed.

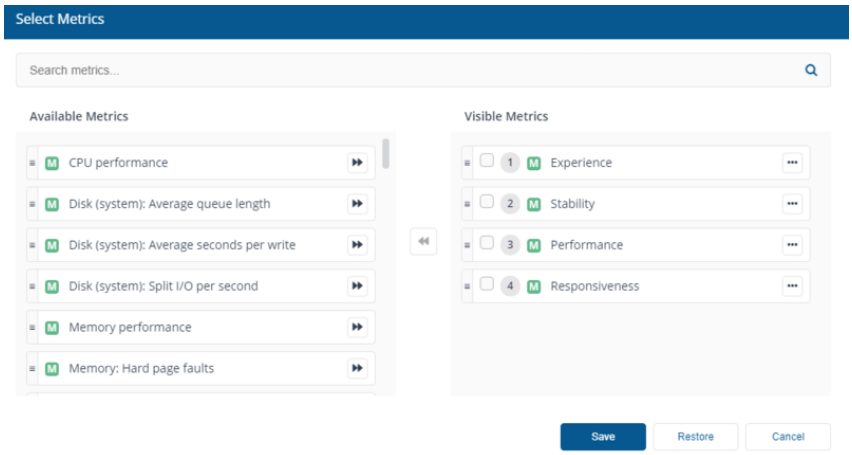
Also use the arrow controls to move up or move down, exclude or include any column - clicking on the ellipsis displays on each metric displays these additional controls.

To apply the view to the current dashboard and return to the dashboard view, click**Save**.

Note

If you've made a number of changes and you want to revert to the original metrics settings you can click on the **Restore** button in the **Select Metrics** popup to revert to the original settings.

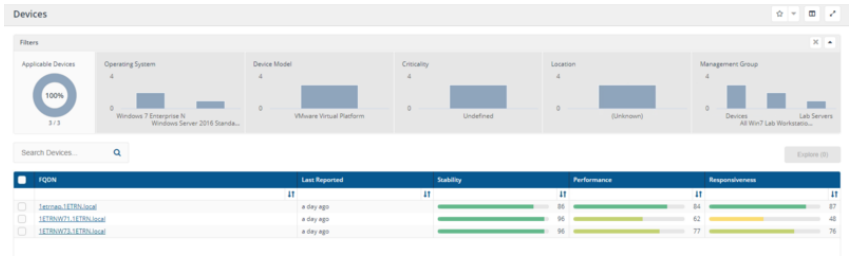
Clicking **Cancel** will also cancel your changes and exit the **Select Metrics** control.



When you have saved your changes and returned to the dashboard view, clicking the star icon in the top right-hand corner of the screen will allow you to save this view as a Preset dashboard you can return to a later date.

Note

For a detailed walkthrough of how to save Presets for your chosen metrics, please refer toCreating your own dashboard.



5.4 Troubleshooting

A general methodology for investigating issues with ExperienceExperience, as well as identifying key issues and their resolutions.

For known issues relating to specific components, please refer to the respective troubleshooting pages:

Clients	Platform	Applications	Integration
1E Client	1E	Endpoint Automation	1E Core for ServiceNow
1E Client Deployment Assistant		Experience Analytics	1E ITSM Connect for ServiceNow

PXE Everywhere	Endpoint Troubleshooting Writing 1E Instructions (1E SDK)	1E Service Catalog Connect for ServiceNow 1E Virtual Assistant

5.4.1 1E Support contact details

5.4.1.1 Support Web portal

Maintenance support customers can log onto the 1E Support Web Portal at https://support.1e.com/ using the login details provided with their maintenance contract. This provides issue tracking, product hotfixes, and knowledge base articles related to each product.

5.4.1.2 Telephone support

Maintenance support customers can contact the technical support department at 1E through the following support numbers. Just phone the relevant number for your area, so your call can be routed quickly and efficiently to the correct support group:

US/Canada:	1-866-349-4032 (Toll-Free) 1-917-339-2360 (Standard)
UK/Europe:	+44 (0)208 326 3499
India:	+91 120 402 4002
Australia:	+61 739 111 118

5.4.1.3 Email support

Maintenance customers can use the following email for additional support. Evaluation customers can also use this email with the temporary access code that is provided through customercare@1e.com as part of their evaluation.

support@1e.com

5.4.2 The technical support process

Read through the Troubleshooting pages to see if there are known issues, or quick resolutions to any problems you may have encountered.

Maintenance support customers can use the 1E Support Web Portal to review knowledge base articles and download hotfixes.

If still encountering problems, create a technical report (log files and details) and then contact the 1E technical support team.

5.4.2.1 Creating a technical report

If possible, please obtain the following details and log files before contacting 1E, to include in your technical report.

5.4.2.1.1 Version details

The OS, version number, and patch level for:

Tachyon Servers

1E Client

Configuration Manager - if used

Other 1E Server software, for example, Shopping, Nightwatchman, and WakeUp.

For Nomad and Shopping, please provide OS, version number, and patch level for:

Configuration Manager DPs

Nomad extensions used on Configuration Manager Consoles

ActiveEfficiency Server.

5.4.2.1.2 Environmental details

If there were any recent changes made to your configuration

The name of the machines, Configuration Manager Application and/or Package IDs for when the issue occurred

5.4.2.1.3 Problem details

When did the issue occur, ensure log files cover this period

The scope of the issue – did it affect a particular geographical location, group of users, or client machines

Details of any self-help troubleshooting steps you carried out

In the event of a service crash or if you are experiencing high CPU or memory usage, provide us with the dump file, event viewer logs, and traces. We will provide you with FTP details to upload these files.

5.4.2.2 Log files

5.4.2.2.1 Tachyon Server log files

For any issue, please provide a zip containing log files from the following locations:

%ALLUSERSPROFILE%\1E\Catalog*.log

%ALLUSERSPROFILE%\1E\ContentDistribution*.log

%ALLUSERSPROFILE%\1E\Platform Consumers*.log

%ALLUSERSPROFILE%\1E\SLA Platform*.log

%ALLUSERSPROFILE%\1E\Tachyon*.log

If you are having licensing issues, please include:

%ALLUSERSPROFILE%\1E\Licensing*

Please refer to the Tachyon Platform 8.1 - Log files page for more details.

5.4.2.2.2 1E Client logs on Windows

%ALLUSERSPROFILE%\1E\Client\1E.Client.log (used by 1E Client and Tachyon features, and Shopping client)

%ALLUSERSPROFILE%\1E\Client\NomadBranchUninstall-YYYY_MM_HHTMM_HH_SS_000Z.log

5.4.3 Configuration issues

Configuration issues that may prevent data getting into Tachyon Experience.

5.4.3.1 No data in Tachyon Experience

Component	Things to Check	Notes

Tachyon Coordinator	Log file (%programdata%\1E\Tachyon\Tachyon.Coordinator.log)	Check for log entries like the following to ensure that the Coordinator is successfully initiating data processing:
		`INFO AggregateSoftwarePerformance - Starting full aggregation of software performance (or Starting incremental aggregation of software performance)`
		`INFO AggregateSoftwarePerformance - Software performance aggregation results`
		Ensure no errors are reported in the Coordinator log.
		Additional logging of the data processing can be found in the SQL table TachyonExperience.dbo.ProcessLog, such as tasks performed, time taken and row counts. The same data is logged into the coordinator log file.
		Note

Component	Things to Check	Notes
		The following value in %programfiles%\1E\Tachyon\Coordinator\Tachyon.Server.Coordinator.exe.config controls the frequency with which the Coordinator initiates cube processing. `<add key="ExperienceSync" value="0 2 * * * ExperienceSynchronization" /> (2am is the default)` It is not recommended that this value be changed.

1E Licensing	License file (%programdata%\1E\Licensing\Tachyon.lic	Ensure the Tachyon Server is licensed for Tachyon Experience:
		`<Feature name="TachyonPlatform">`
		`<Consumer name="Platform" enable="on"> </Consumer>`
		`<Consumer name="Experience" enable="on"> </Consumer>`

Aggregated Software Data	Ensure software aggregated data has been populated	Check the **LastProcessed** setting in the **TachyonExperience.dbo.GlobalSettings** table for the last processed time. To check the sizes of aggregation tables, run a DB report **Disk usage by table** and verify that **dbo.SoftwarePerformance_xx tables** have non zero records.

Component	Things to Check	Notes

Table Name	# Records	Reserved (KB)
cache.vSoftwarePerformance__1404025993	228	840
dbo.AnnouncementActionEvent	0	0
dbo.ApplicationServer	0	0
dbo.ApplicationServerResourceDemand	0	0
dbo.AppliedChanges2	70	144
dbo.Architecture	2	144
dbo.Attribute	32	144
dbo.Device	500,010	503,368
dbo.DeviceDeduplication	0	0
dbo.DeviceInteractionMetric	22	144
dbo.DevicePerformance	67,238,981	33,585,768
dbo.DevicePerformanceMetric	66,856,329	30,858,048
dbo.DeviceResourceAllocation	0	0
dbo.DeviceResourceDemand	0	0
dbo.DeviceResourceDemandQuarterHour	0	0
dbo.Event	50,063	16,416
dbo.Executable	176	144
dbo.GlobalSetting	16	72
dbo.InvestigationCategory	3	144
dbo.InvestigationCategoryAttributeMapping	0	0
dbo.InvestigationCategoryMetricMapping	46	72
dbo.LatestDevicePerformance	500,010	223,208
dbo.LatestDevicePerformanceMetric	500,010	239,376
dbo.LatestUserSurveyPerformanceMetric	2	72
dbo.ManagementGroup	78	72
dbo.ManagementGroupMember	3,717,874	216,984
dbo.Metric	110	208
dbo.MetricChildren	59	72
dbo.ProcessLog	19	72
dbo.Product	20	144
dbo.SoftwarePerformance	2,066,804,330	523,466,560
dbo.SoftwarePerformance_07	18,350,396	242,600
dbo.SoftwarePerformance_07_Staging	0	0
dbo.SoftwarePerformance_30	29,666,267	744,392
dbo.SoftwarePerformance_30_Staging	0	0
dbo.SoftwarePerformance_60	35,955,228	772,416
dbo.SoftwarePerformance_60_Staging	0	0
dbo.SoftwarePerformance_90	40,873,375	665,928
dbo.SoftwarePerformance_90_Staging	0	0
dbo.SurveyAnswerEvent	0	0
dbo.TimestampLookup	1,097	72
dbo.Topic	14	144
dbo.User	2	144
dbo.UserSurveyPerformanceMetric	1	288
dbo.Version	182	144

5.4.4 Known issues

Lists of the current known issues with implementing, configuring, and using Tachyon Experience.

If you cannot find an issue and its workaround on this page, please

Refer to 1E platform - Known issues for the Platform and other applications.

Try searching the 1E Support Portal https://support.1e.com/ for issues that have hotfixes.

If you need further help, please refer to the Troubleshooting page for how to contact 1E Support and the technical support process.

Issue	Description	Workaround
Experience - Software > Duplicate row for a product is displayed on Software screen when architecture column is added from column picker following an upgrade from 8.0.	The architecture column did not exist in pre-v8.0 SoftwarePerformance table. When upgraded to v8.0 or later, architecture column has been introduced as nullable column to accommodate pre-upgrade data. It will be set as null for all existing data from before the upgrade. Gradually as new experience performance data comes in post upgrade architecture will now be included. This means that for 90 days after the upgrade aggregations within the Software screen of experience can have two entries, one with an unknown architecture and one with a valid architecture.	The existing data will correct itself 90 days after the upgrade. If you need to fix this issue in the meantime, a maintenance Stored Procedure for the Experience database can be obtained from 1E. The SP will update the null architecture for pre-upgrade software performance rows by using post-upgrade rows to identify and correct old software architectures.
Experience Analytics - Tiles have an additional text "score" added to them when view between saved preset is changed.	When user changes the view between Default and user saved presets; an additional text "Score" gets added to the tile title, e.g: StabilityScore, ResponsivenessScore.	Refreshing the browser removes the additional text "Score".
A survey that has been dismissed by the user will reappear if it is disabled then re-enabled.	If a user engagement (survey or announcement) is disabled then re-enabled then it appears to the 1E Client as a completely new	Do not disable an engagement then re-enable it! In effect this creates a new instance, at least in terms of data sent to the 1E Client.

Issue	Description	Workaround
	engagement and the previous state (dismissed, in this case) is lost.	
Application Interaction table can contain processes reported as *.tmp files where the Product and Version columns are blank.	The Application Interaction view is reached by launching the Experience > Devices and viewing the Device hyperlink. When viewing the Experience > Application Interaction tab, the *.tmp records are also displayed which do not have associated Product or Version details. These should be filtered out.	None
The Survey response page displays responses from a device that do not match the score seen when viewing the Device details due to duplicate survey names	When a survey is deleted, the old responses do not get removed and current behavior causes issues when a new survey is created with the same name. The calculations for sentiment score includes responses from the old survey where the names match.	Where this occurs, recreate the survey using a unique name that has not been previously used. If you are affected by this, please contact 1E Support for additional help.
When doing a search on Survey page, the page size resets back to the default (50)	On the Experience > Survey page, the page size can be increased to to display 100 or 250 rows. However, when a search is performed on the page, the page size jumps back to the default 50.	None
Survey reports always shows Applicable devices as 100%	Even when a general purpose survey has been assigned to a Management Group, the filter for survey reports always shows 100% for Applicable devices and not consistent with the devices assigned to the selected Management Group	None

5.5 Reference

This section includes references for the tiles included in Experience as well as how the scores are calculated.

5.5.1 Page reference

A reference for the fields and tables on the pages in the Tachyon Experience application.

5.5.1.1 Experience Analytics menu

The Experience Analytics menu contains a number of pages. We recommend the Overview page as the starting place for any Tachyon Experience journey where you can get immediate answers to how your enterprise is performing from an end-user perspective, and you can drill down to get details on specific problem areas and find routes to immediate resolutions.

5.5.1.1.1 Overview page

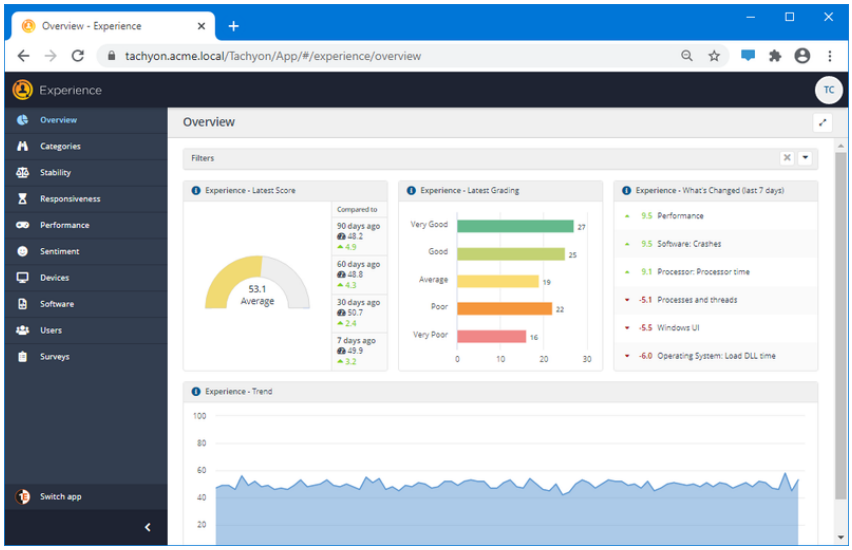
The **Overview** page is the starting place for any Tachyon Experience journey. Here you can get immediate answers to how your enterprise is performing from an end-user perspective and you can drill-down to get details on specific problem areas and find routes to immediate resolutions.

Your key indicator is the **Experience - Latest Score** chart, which gives your enterprise a score out of 100 based on a combination of measured events and user surveys. The closer you are to 100 the better the IT experience your end-users are having.

The **Experience - Latest Grading** chart provides a breakdown of the experience score showing how many devices and users fall into each of the five experience grades - ranging from **Very Good** to **Very Poor**. This helps interpret the experience score and see how it maps onto end-user experiences.

The **Experience - What's Changed (last 7 days)** chart provides an overview of the significant changes, good or bad, that have occurred during the past week.

Finally you can use the **Experience - Trend** chart to check how well your enterprise is performing over time in terms of how your end-users see it. You could use this chart to help gauge progress on any improvement programs you might have put in place or act as an advanced warning that there are underlying issues that are affecting your end-users and need resolving.



Without filters, the dashboard shows the status of all devices in the environment and all of their subsequent scores. When filters are added, the dashboard is recalculated according to the applied filter. For an explanation of filters, please refer to Filters and Breakdown bar.

Hovering over the icon in the upper left corner of any tile shows the name of that tile or the metric that tile is displaying.

5.5.1.1.1.1 Dashboard charts

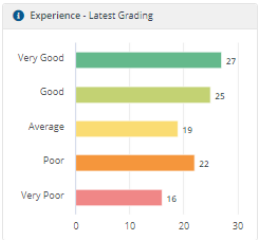
5.5.1.1.1.1.1 Experience - Latest Score

This tile shows the overall score with a sidebar showing the score over the last week, month, 60 day, and 90 day periods. It will show the difference in the score over that time period. Clicking into the colored portion of the chart will take you to additional details.

For details on the calculation of the Experience Score please refer to The Scores: Experience Score.

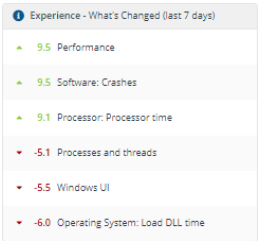
5.5.1.1.1.2 Experience - Latest Grading

The Grading tile allows you to see the numbers of devices for each score. You can drill into each of the ratings - Very Good, Good, Average, and Poor to see the devices that have that score. This allows identification of the poorly performing devices very quickly.



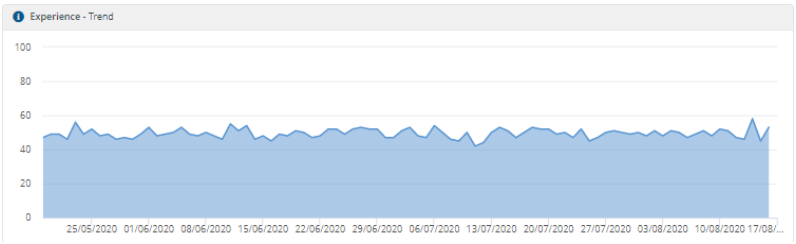
5.5.1.1.1.1.3 Experience - What's Changed (last 7 days)

This tile shows you the score over a period of days and the amount of change in the score. A negative number is reflected in Red and shows the performance has worsened. A positive number is reflected in Green and shows that the performance has improved.

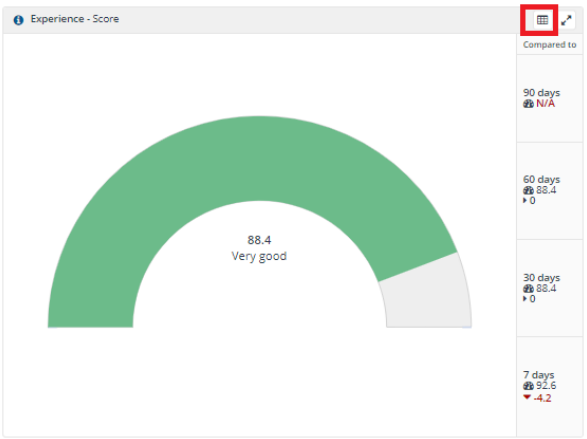


5.5.1.1.1.1.4 Experience - Trend

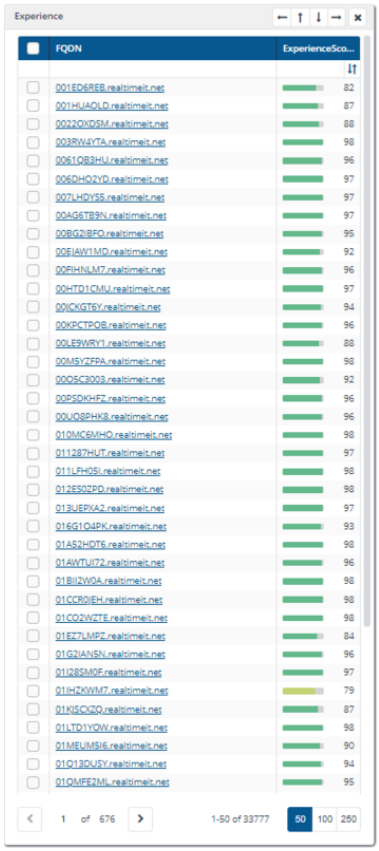
The trend tile shows the score over a succession of days. Any area on the line can be highlighted and the date and the score for that day viewed.



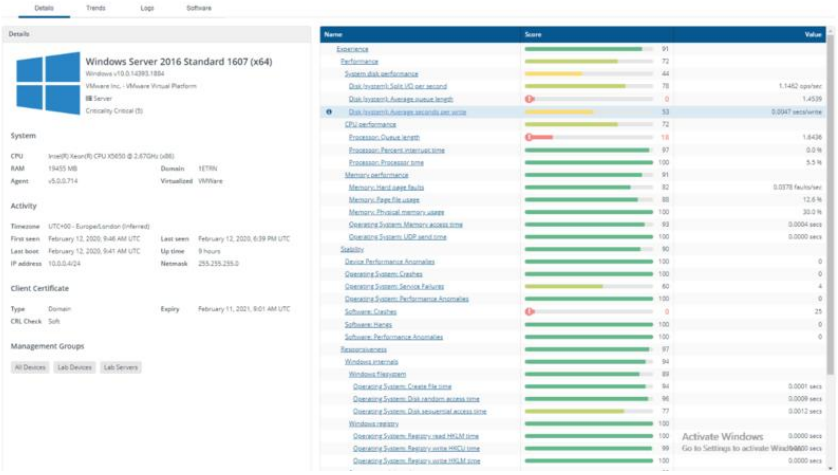
Clicking on the View Detailed data button at the top of any tile brings up the Raw data



This presents a box of the raw data for the selection. Clicking on any of the devices opens the details page for the device.



The details page shows all the metrics that are being collected. The colored bars represent the grading numbers. Any that are very poor will be red with an exclamation point.



5.5.1.1.2 Categories page

The Categories page shows a dashboard of the scores from each of the four categories:

Stability

Responsiveness

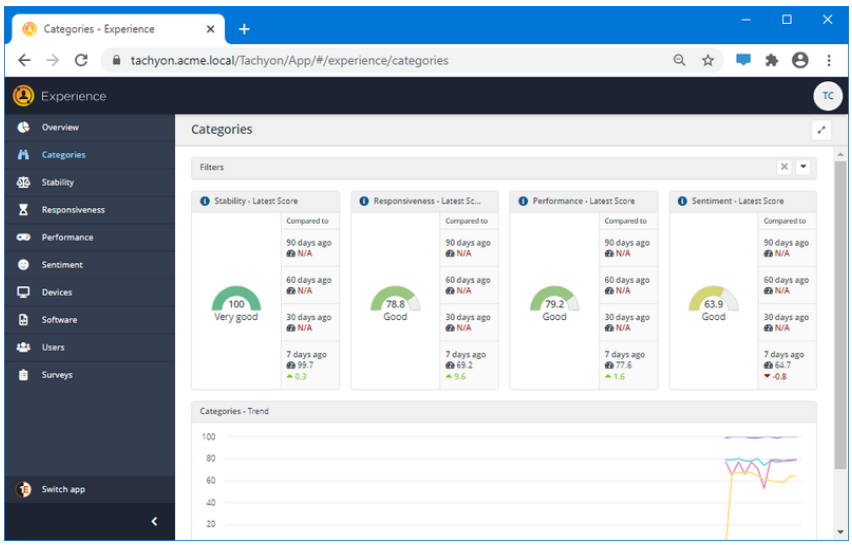
Performance

Sentiment

The first row of tiles shows the Latest Score view from each of the categories. Clicking on one of these tiles opens the related page in Experience.

The tiles either display information on the entire estate, if no filtering has been selected, or just the devices that are covered by the filtering query. For example, if the selected filter is **High Criticality** - the tiles will only contain devices that were configured as **High** for **Criticality**.

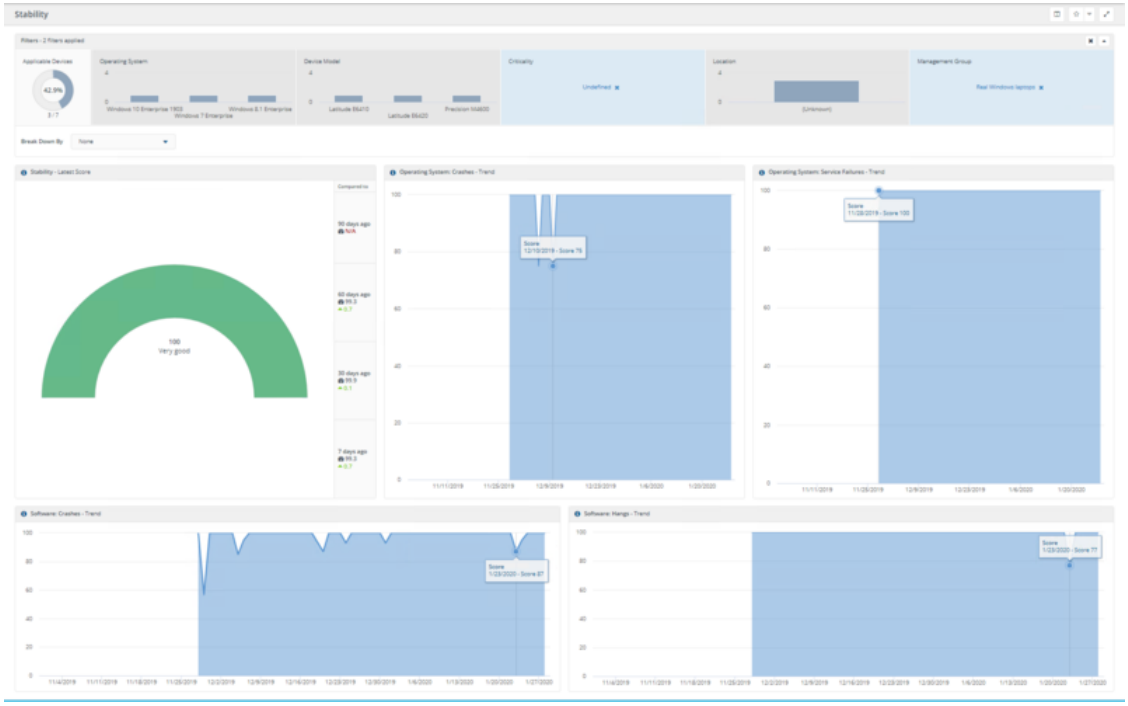
The tile on the bottom row shows the trend for all the categories over time.



5.5.1.1.3 Stability page

The stability score is derived by measuring the "crashiness" of applications and the operating system of a device. The different types of crashes have a differing impact on the score, based on the amount of impact on the end-user.

An application crash is annoying but the crash of the entire operating system could cause data loss so has more weight on the score. The page allows you to drill into the tiles to see the different metrics that are collected. For information on the makeup of the score see Stability Score



5.5.1.1.3.1 Stability - Latest Score Tile

The Latest Score tile can be selected for additional details. This is the view when selecting the Latest Score Tile with the Filters bar collapsed.

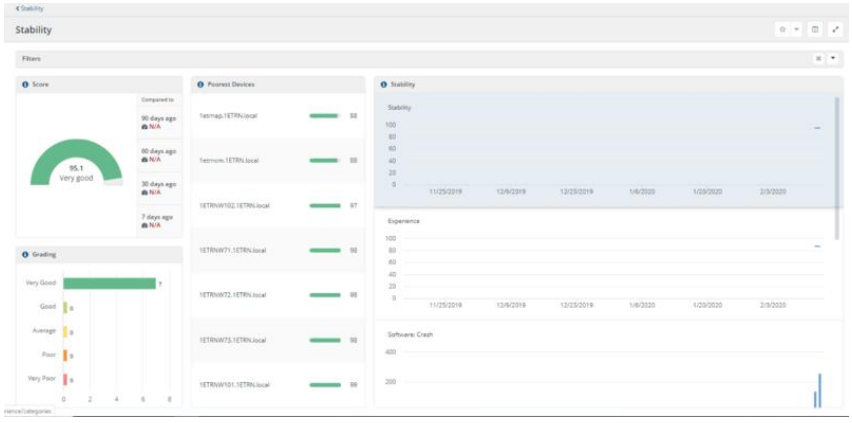
This view has the following tiles:

Score - with comparison history on the side

Poorest Devices in the Environment

Timeline of the Scores for Stability and Experience

Environment Stability Grading Bar Chart

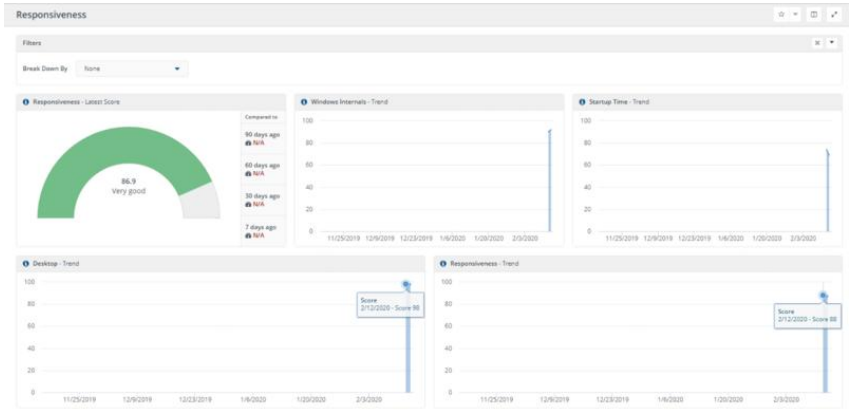


5.5.1.1.4 Responsiveness page

The responsiveness score is derived by measuring how well Windows application perform during our "Synthetic micro-transactions". The successful and timely operation of Windows and Windows applications is key to a positive user experience on that device.

The page allows you to drill into the Latest Score tile to see the different metrics that are collected. For information on the makeup of the score see Responsiveness Score

5.5.1.1.4.1 The Responsiveness Page



5.5.1.1.4.2 Responsiveness - Latest Score Tile

The Latest Score tile can be selected for additional details. This is the view when selecting the Latest Score Tile with the Filters bar collapsed.

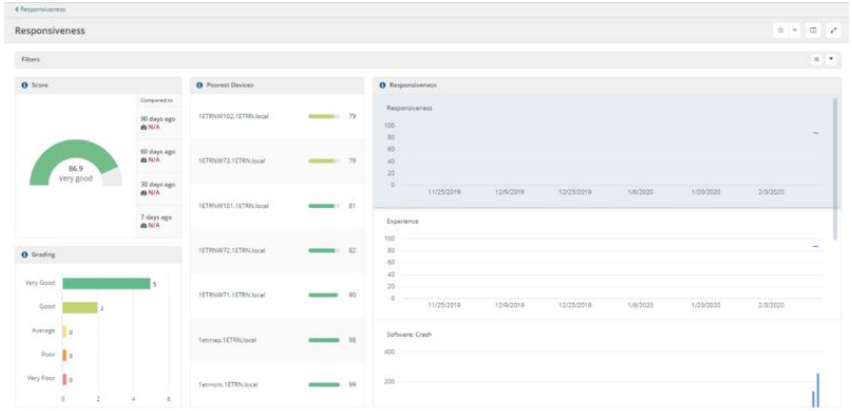
This view has the following tiles:

Score - with comparison history on the side

Poorest Devices in the Environment

Timeline of the Scores for Responsiveness and Experience

Environment Stability Grading Bar Chart



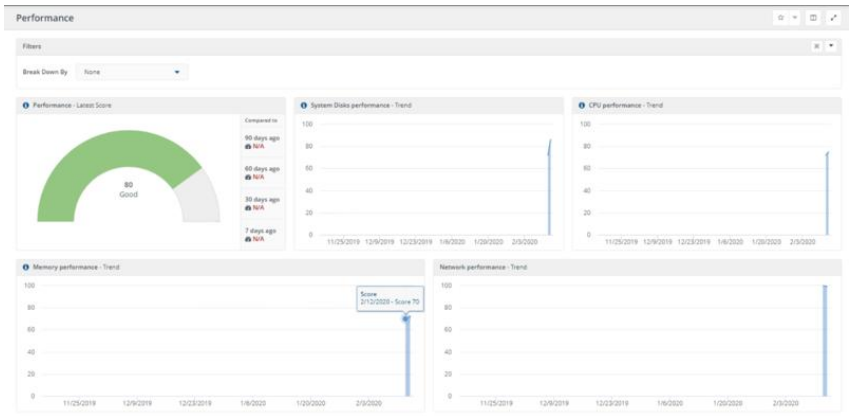
5.5.1.1.5 Performance page

The performance score is derived by measuring the performance of the device using the Windows Performance Counters. These counters measure many data points on the device including CPU usage, disk usage, memory usage, and processes.

The page allows you to drill into the Latest Score tile to see the different metrics that are collected. For information on the makeup of the score see Performance Score

More information on the Windows Performance Counters can be found here: https://docs.microsoft.com/en-us/windows/win32/perfctrs/performance-counters-portal.

5.5.1.1.5.1 The Performance Page



5.5.1.1.5.2 Performance - Latest Score Tile

The Latest Score tile can be selected for additional details. This is the view when selecting the Latest Score Tile with the Filters bar collapsed.

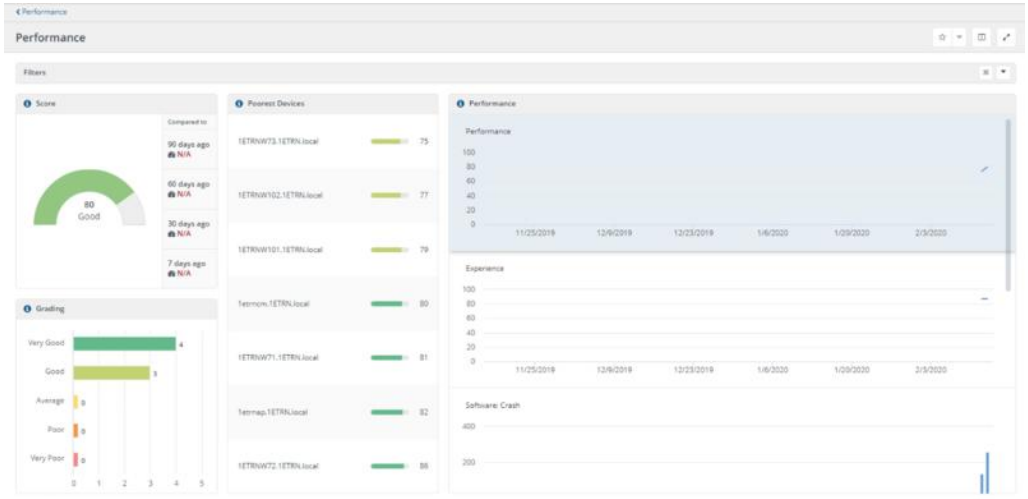
This view has the following tiles:

Score - with comparison history on the side

Poorest Devices in the Environment

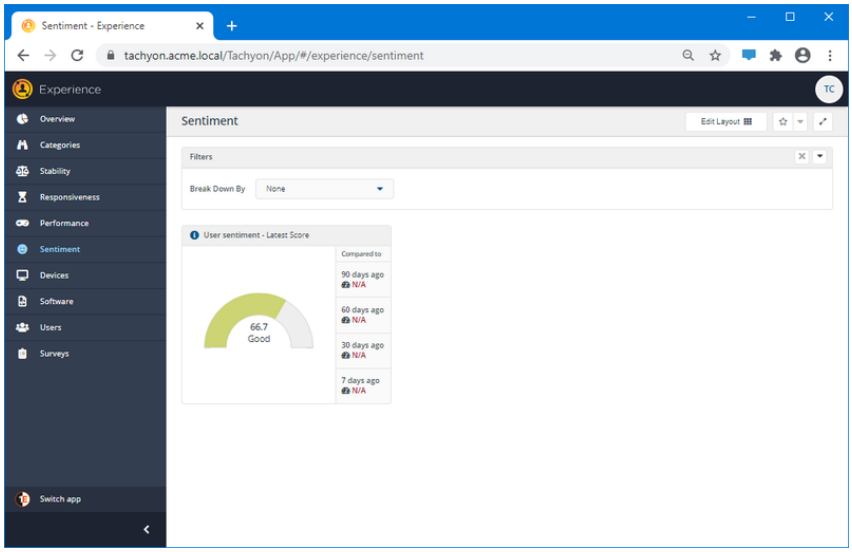
Timeline of the Scores for Performance and Experience

Environment Stability Grading Bar Chart



5.5.1.1.6 Sentiment page

The **Sentiment** page provides charts that focus on the Sentiment scores in Experience. You can also change the layout to add tiles for any User Sentiment Surveys you have created.



5.5.1.1.6.1 The Sentiment page

This page is the dashboard for monitoring your network's User Sentiment score and any User Sentiment Surveys you have created.

5.5.1.1.6.2 Editing and storing the Sentiment page layout

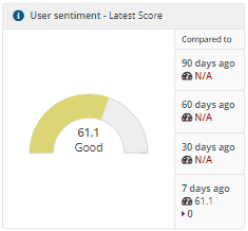
To display your own User Sentiment Surveys on the Sentiment page you click on the **Edit Layout** button to add the new metrics that are related to the Surveys. Once you have configured

5.5.1.1.6.3 Filters

You can apply filters and different breakdowns for the data displayed on the Sentiment page.

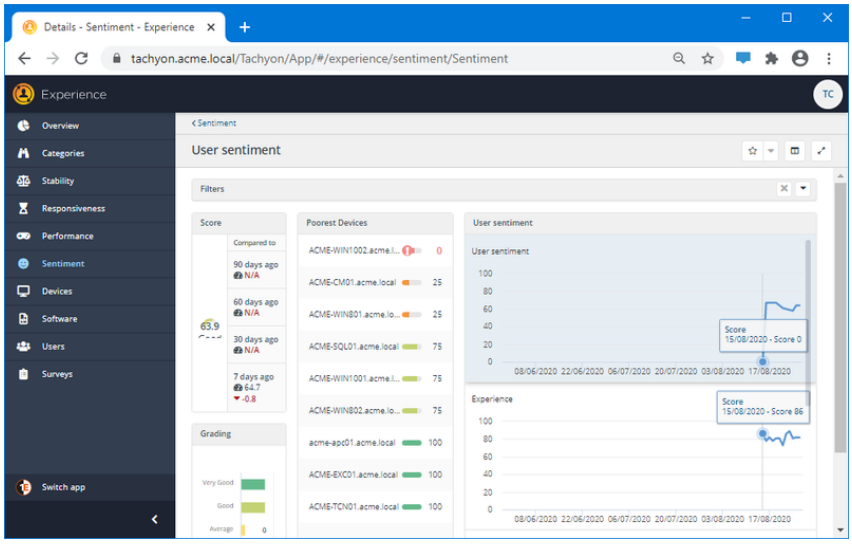
5.5.1.1.6.4 User sentiment - Latest Score tile

The default tile displayed on the **Sentiment** page is the **User sentiment - Latest Score** tile. This shows the latest User Sentiment score along with comparisons between the current date and those of 7, 30, 60 and 90 days ago. If you don't have enough data yet the relevant section of the **Compared to** column shows the text N/A to indicated that it's not applicable.



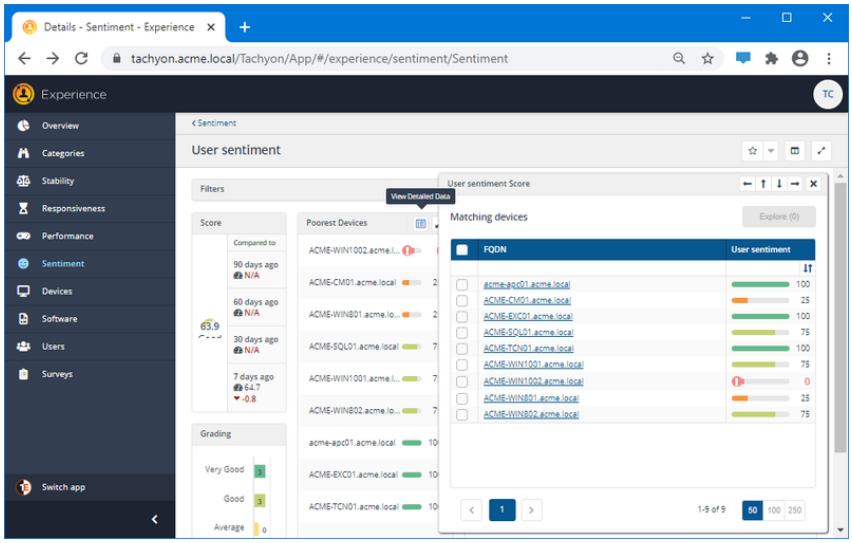
5.5.1.1.6.5 User sentiment page

Clicking on the **User sentiment - Latest Score** tile displays the **User sentiment** page. Here there are tiles for the **Score**, **Poorest Devices**, **User sentiment**, **Experience** and **Grading**.



5.5.1.1.6.5.1 User sentiment Score panel

Clicking on the **View Detailed Data** button on any of the tiles displays the **User sentiment Score** details, as shown in the picture opposite, which is a list of the devices and their current **User sentiment** scores. From here you can navigate to a device page by clicking on the device's FQDN, or make a selection and click on the **Explore** button to open the **Explorer** Application with the selected devices set as the scope.



5.5.1.2 Advanced Analytics menu

The Advanced Analytics menu contains two pages providing information to IT Support team members:

Networkpage, where they can monitor and manage network performance throughout their enterprise

Boot & Login page, where they can monitor and manage end-user boot and login experience throughout their enterprise.

5.5.1.2.1 Network page

The **Network** page provides information to IT Support team members, so they can monitor and manage network performance throughout their enterprise. By default, this page displays the following tiles:

Network - Latest Score

Operating System: UDP send time - Trend

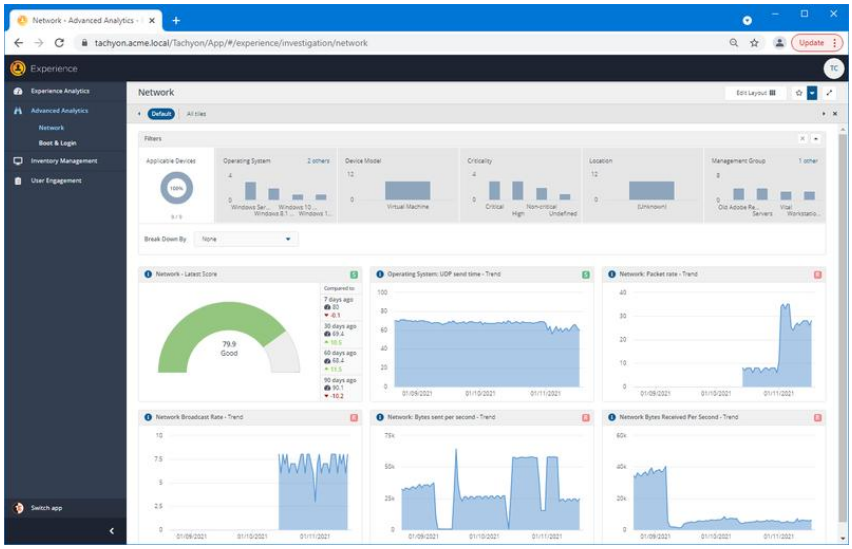
Network: Packet rate - Trend

Network Broadcast Rate - Trend

Network: Bytes sent per second - Trend

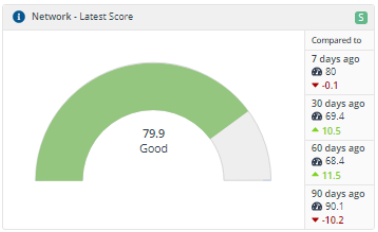
Network Bytes Received per second - Trend

Please refer to Investigating Network Performance for more information on how to use this feature.



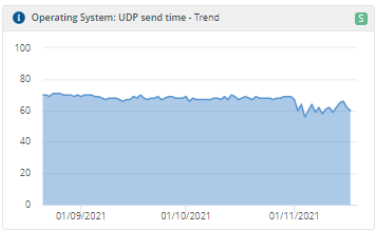
5.5.1.2.1.1 Network - Latest Score

This chart displays a score for device network stack performance based on: the Wireless signal quality, the UDP send time and the output queue length (does not include physical network considerations, such as latency).



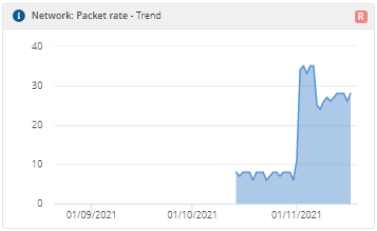
5.5.1.2.1.2 Operating System: UDP send time - Trend

This chart provides a score for the time taken to perform a basic loopback UDP send. A lower score may indicate problems with the operating system network stack.



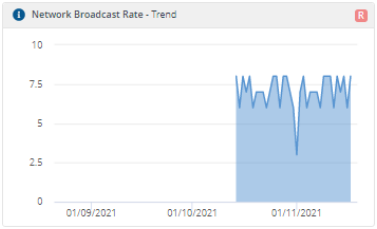
5.5.1.2.1.3 Network: Packet rate - Trend

This chart provides an overview of the sum of all TCP packets that have been sent and received per second; represents a measure of network resource utilization on the device.



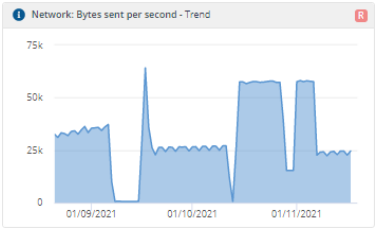
5.5.1.2.1.4 Network Broadcast Rate - Trend

This chart provides an overview of the sum of all multicast packets that have been sent and received per second (across all physical network interfaces on the device).



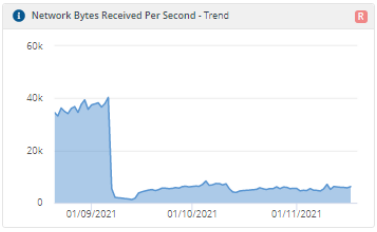
5.5.1.2.1.5 Network: Bytes sent per second - Trend

This chart provides an overview of the average number of bytes sent per second across all network adapters.



5.5.1.2.1.6 Network Bytes Received per second - Trend

This chart provides an overview of the average number of bytes received per second across all network adapters.



5.5.1.2.2 Boot and Login page

The **Boot & Login** page provides information to IT Support team members, so they can monitor and manage end-user boot and login experience throughout their enterprise. By default, this page displays the following tiles:

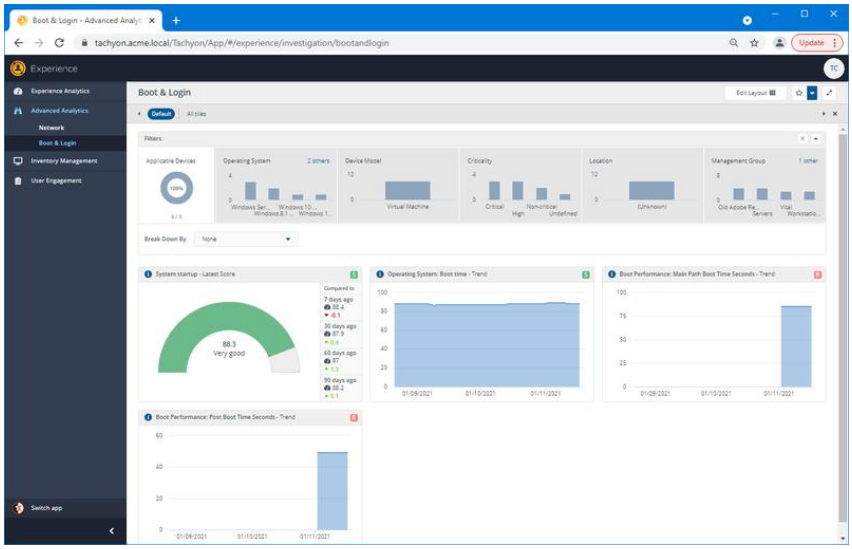
System startup - Latest Score

Operating System: Boot time - Trend

Boot Performance: Main Path Boot Time Seconds - Trend

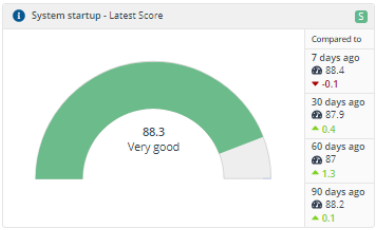
Boot Performance: Post Boot Time Seconds - Trend

Please refer to Investigating Boot and Login Performance for more information on how to use this feature.



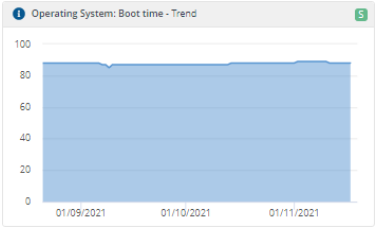
5.5.1.2.2.1 System startup - Latest Score

This chart provides a score derived from operating system startup times for devices.



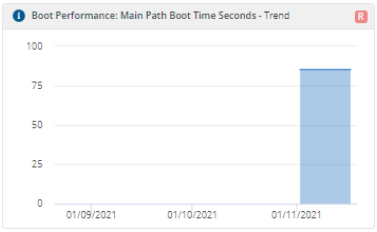
5.5.1.2.2.2 Operating System: Boot time - Trend

This chart provides a score derived from the times taken for devices to boot to the logon prompt. A lower score indicates a long boot up duration, which may affect user satisfaction.



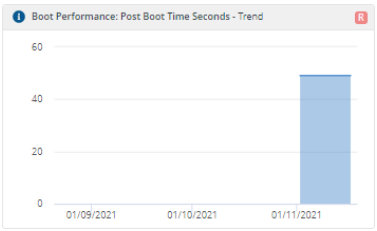
5.5.1.2.2.3 Boot Performance: Main Path Boot Time Seconds - Trend

This chart provides an overview across all devices, of the time taken (in seconds) to perform the Main Path step of the boot sequence, which starts when the Windows splash screen appears and ends when the desktop becomes available.



5.5.1.2.2.4 Boot Performance: Post Boot Time Seconds - Trend

This chart provides an overview across all devices, of the the time taken (in seconds) to perform the Post-boot step of the boot sequence, which starts when the desktop appears and ends when the system reaches a certain idle state having initialized services and applications.



5.5.1.3 Inventory Management menu

The Inventory Management menu contains three pages:

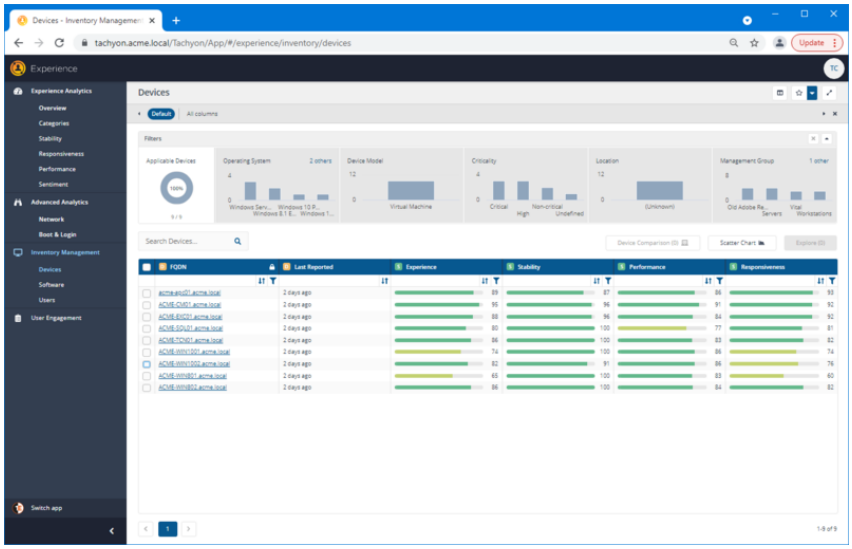
Devices page provides a list of all devices visible to Tachyon Experience

Software page provides a tabular listing of all the Software products that are installed in the environment (including executable, version, architecture).

Users page displays user experience information.

5.5.1.3.1 Devices page

The **Devices** page provides a list of all devices visible to Tachyon Experience. You can see all of their **Experience**, **Stability**, **Performance**, and **Responsiveness** statistics and sort them accordingly.



5.5.1.3.1.1 The Devices page

The Devices page allows you to view detailed information for each device in your environment by drilling into a device. From here, you can:

Select two devices and use Device Comparison to compare their settings

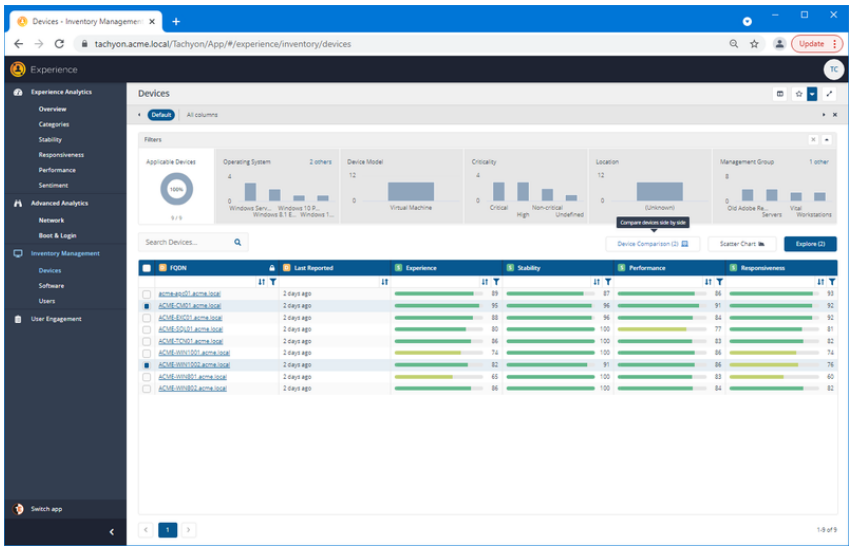
Use the Scatter Chart to plot the displayed devices on a two-dimensional graph with configurable axes

Select one or more devices and use Explore to set them as the scope for an explorer instruction

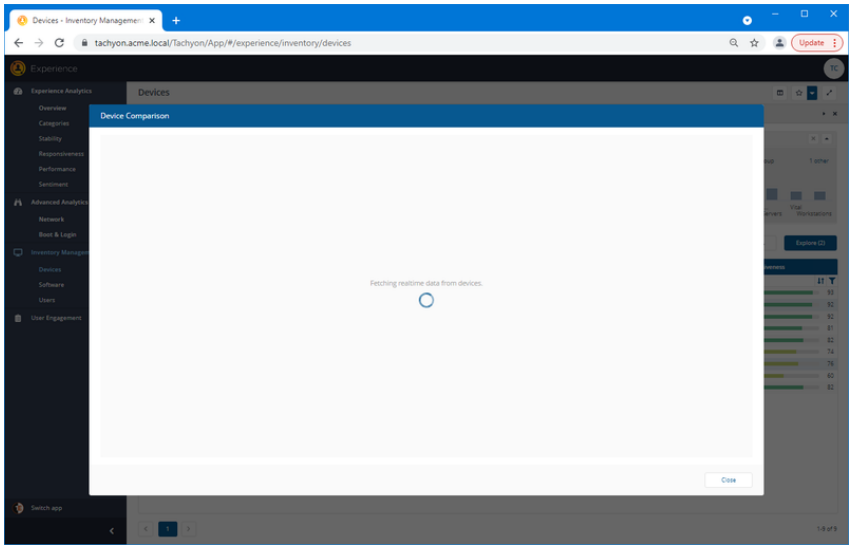
You can display the Device View for a selected device by clicking on its link in the **FQDN** column.

5.5.1.3.1.1.1 Device Comparison

Selecting two devices from the **Devices** table enables the **Device Comparison** button. Clicking on the button displays the **Device Comparison** popup.



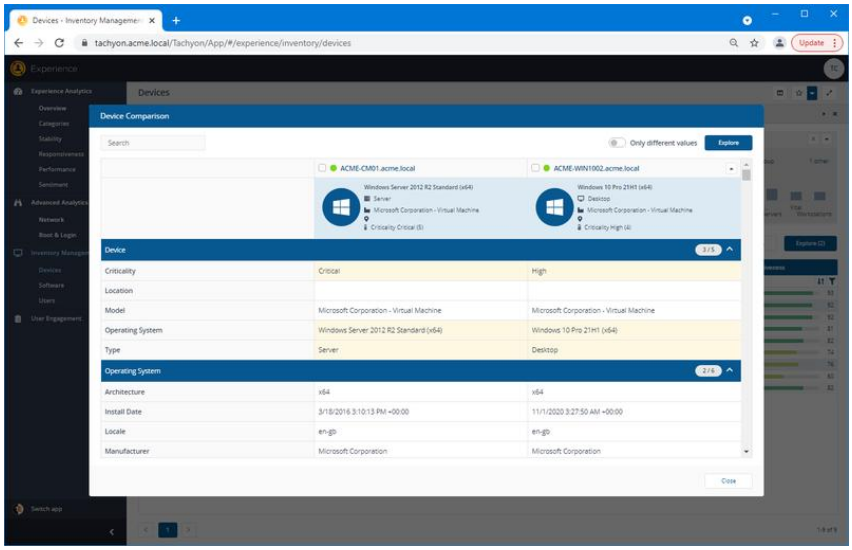
The data for the comparison is fetched in real-time from both the selected devices.



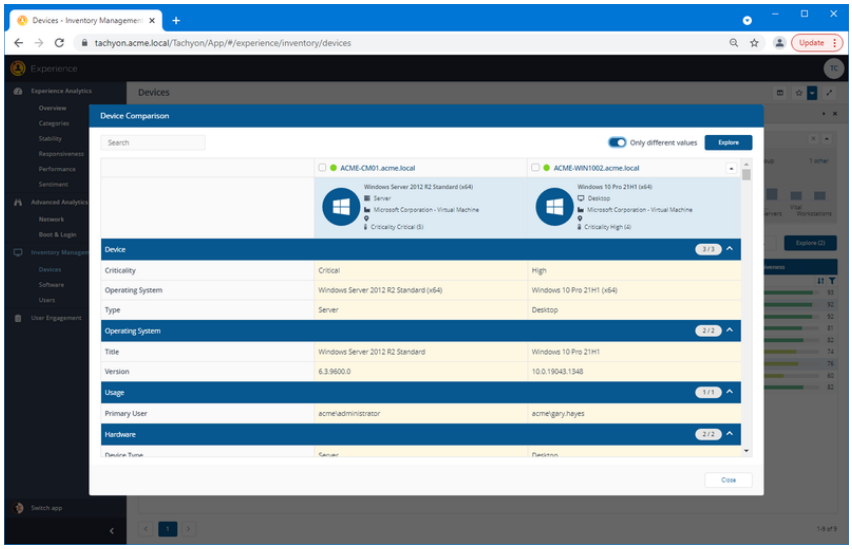
The details for the comparison are displayed in a table, with the parameter headings on the left-hand column and then one column per-device showing the values corresponding to the parameters.

Each column heading for the devices contains a checkbox, that can be used to select the device as the scope for an Explorer session by clicking on the **Explore** button. The FQDN name for each device is a link that can be used to display the Device View for that device.

The information in the table is grouped into 7 collapsible category headings: **Device**, **Operating System**, **Usage**, **Hardware**, **Software**, **Services** and **Processes**.

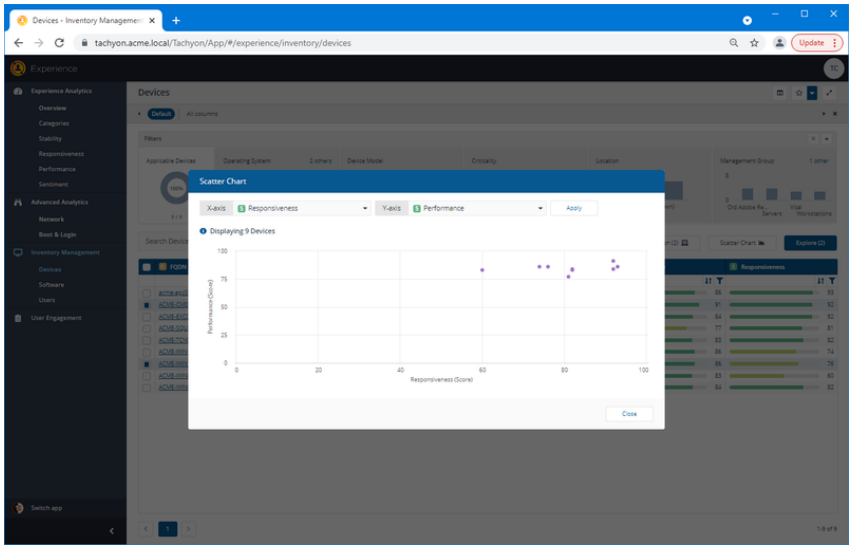


Each row where there is a difference is highlighted in yellow and where the information is the same in white. You can select to focus on only the differences by switching the **Only different values** toggle to on.

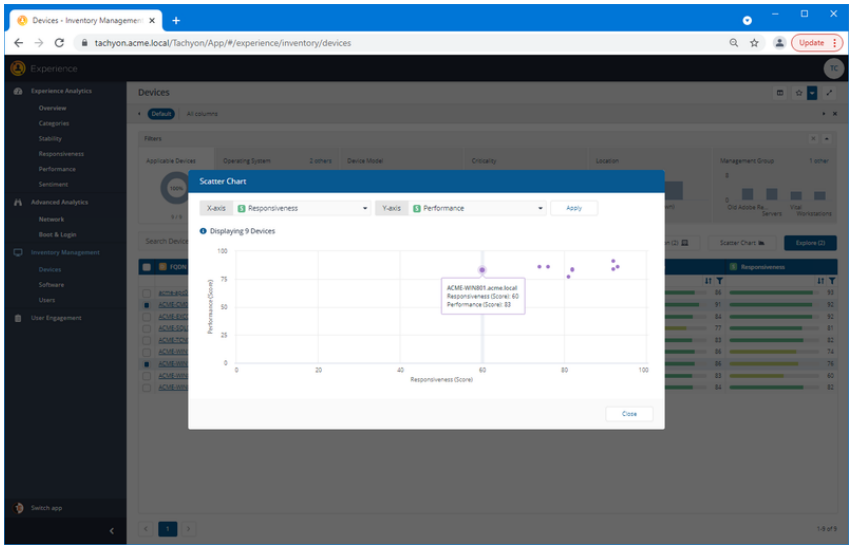


5.5.1.3.1.1.2 Scatter Chart

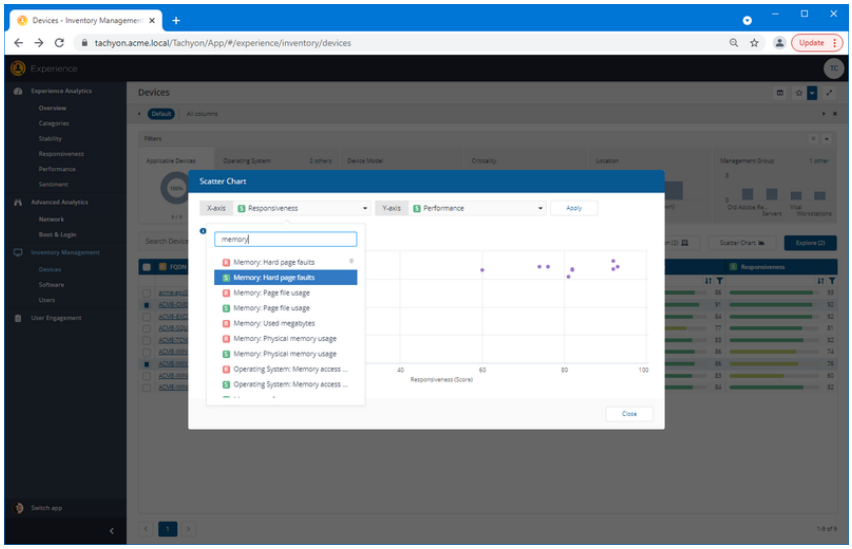
Clicking on the **Scatter Chart** button in the **Devices** page displays the **Scatter Chart** popup. The devices from the current view are plotted as points on a graph according to their **Responsiveness** scores on the X-axis and **Performance** scores on the Y-axis.



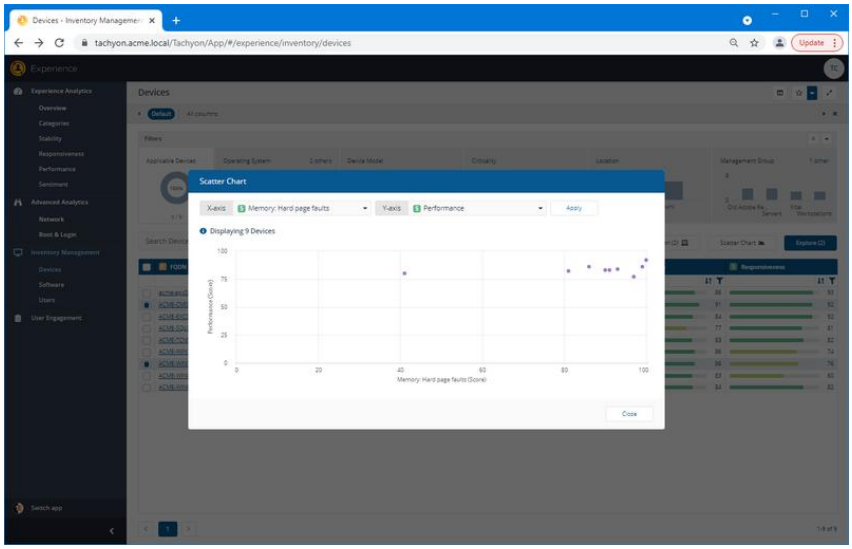
You can hover over a point on the graph to view its details.



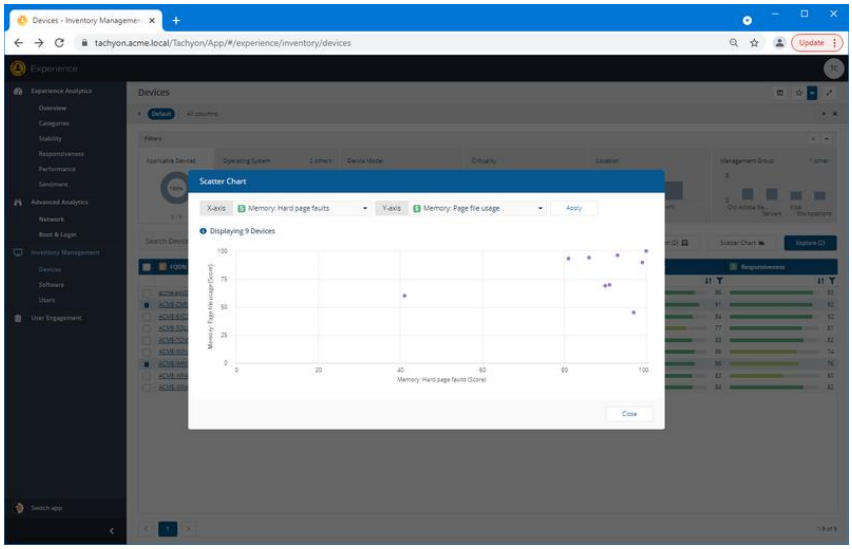
The parameters plotted on the axis can be changed using the axis dropdowns. The parameter you want to plot is selected from a list that can be filtered by typing text into the search field. The picture opposite shows the **Memory: Hard page faults** parameter selected.



You must click the **Apply** button to re-plot the graph according to the new selection.

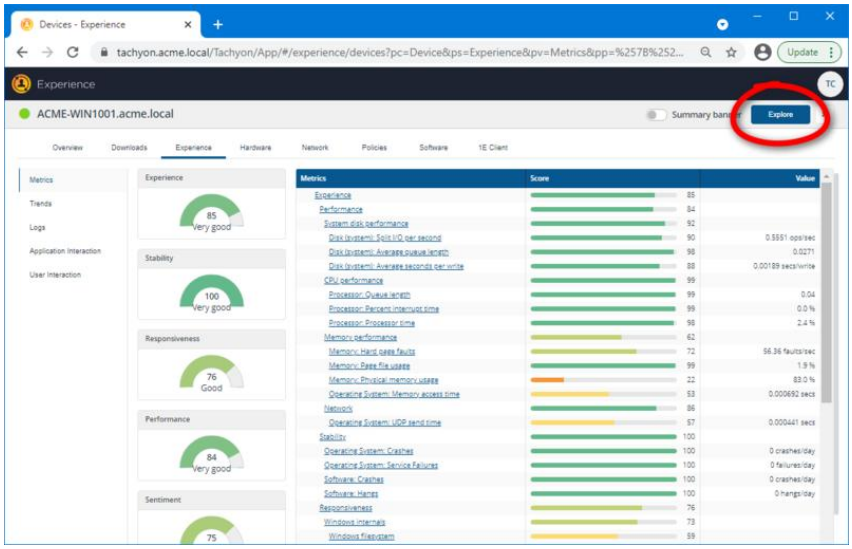


Both axes can be changed. The picture opposite shows the device **Memory: Hard page faults** plotted against the **Memory: Page file usage** scores.

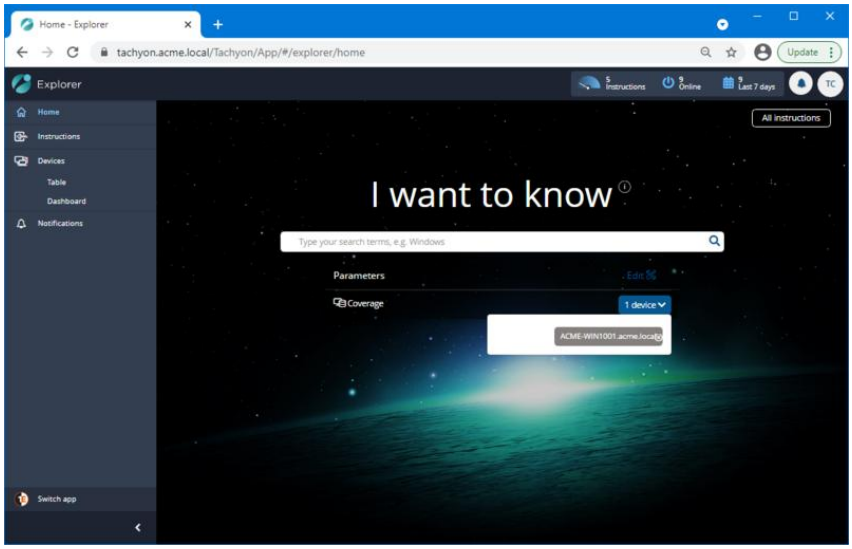


5.5.1.3.1.1.3 Explore Button

If the account you are viewing Tachyon Experience with has at least the Global Questioner role, you will also see an **Explore** button. Clicking this button will launch Tachyon Explorer.



The coverage will be set to the device you were viewing in Experience.



5.5.1.3.1.2 The Device View

Clicking on one of the links in the **FQDN** column of the **Devices** page displays the Device View for the selected device. The aim of the Device View is to provide a combined overview of all the information known about a device, along with the ability to retrieve information about the device in real-time. There are a number of tabs available in the Device View, but the **Experience** tab is specific to the Experience application.

5.5.1.3.1.3 The Device View Experience tab

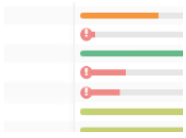
When displaying the Device view from an Experience page the view defaults to the **Experience** tab. The **Experience** tab contains information derived from and useful for Tachyon Experience. It contains the following panels:

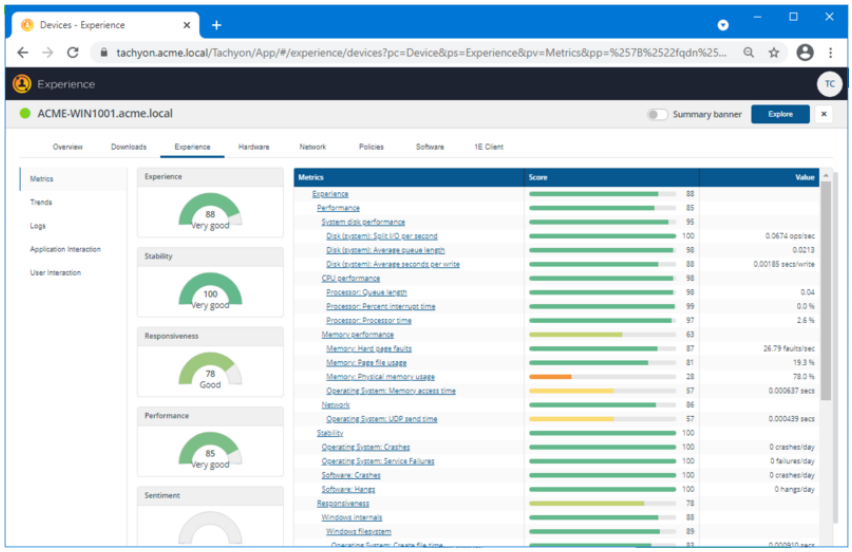
5.5.1.3.1.3.1 Metrics panel

This panel shows the current gradings for all the Metrics that are measured by Tachyon Experience.

> **Note**
>
> Only the current gradings can be seen here, there is no ability to look at the history information in this panel.

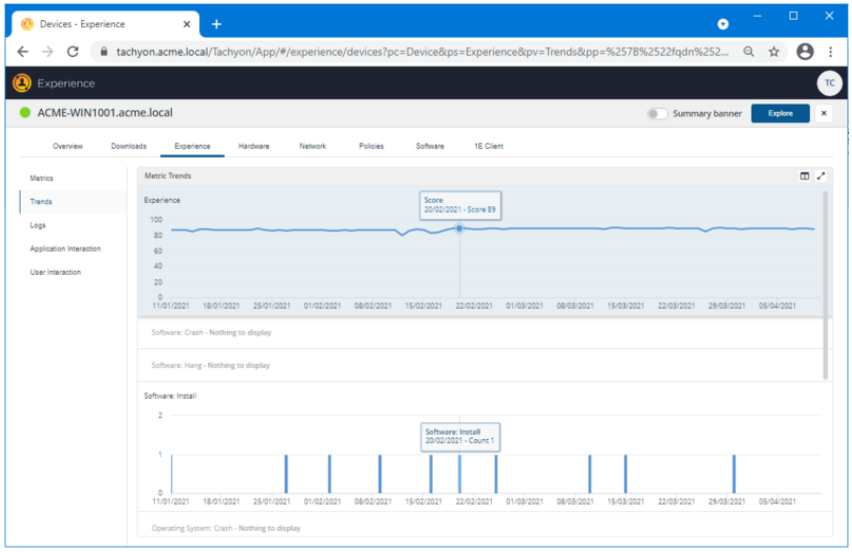
Metrics with a **Very Poor** grading are marked by lines in red with an exclamation mark.





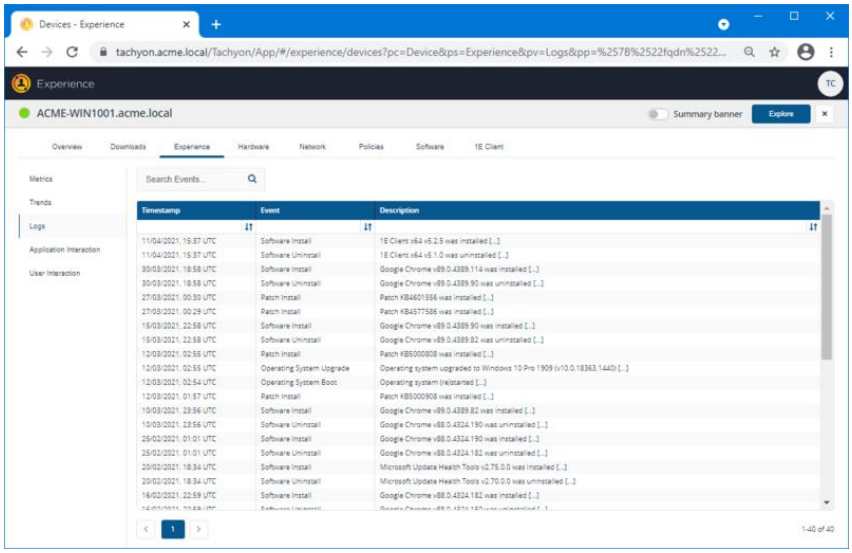
5.5.1.3.1.3.2 Trends panel

The **Trends** panel shows the Metric measurements over time, making it easy to determine trends and see what else was happening on the device as an issue progressed.



5.5.1.3.1.3.3 Logs panel

The **Logs** panel shows the Windows Event Log entries for significant events. These events are captured as they happen, the device does not wait for the daily digest to send the information to the switch.



5.5.1.3.1.3.4 Application Interaction panel

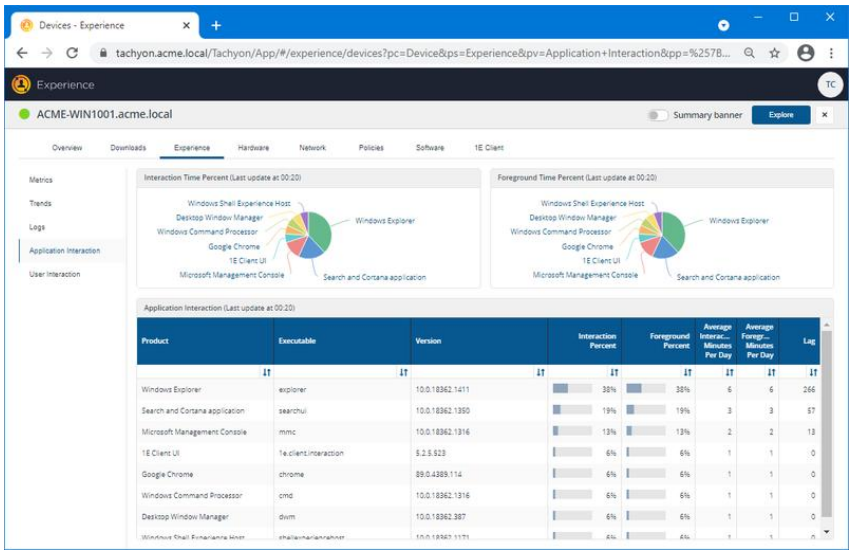
This panel provides a couple of charts and lists the applications that have most recently been interacted with on the device.

The **Interaction Time Percent** chart shows the amount of time each application on the device was interacted with as a percentage of the time for all the applications.

The **Foreground Time Percent** chart shows the amount of time each application spent in the foreground as a percentage of the time for all the applications.

The table lists the applications most recently interacted with on the device. The table can be sorted on each column.

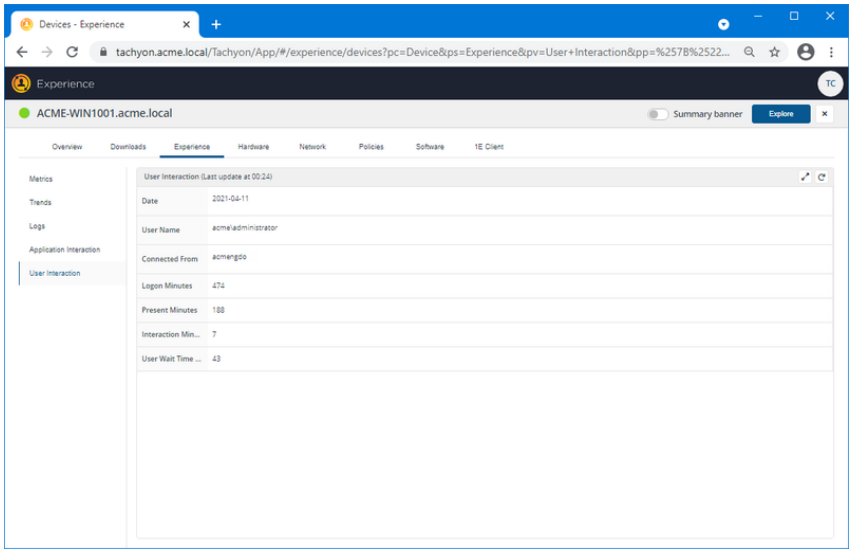
Column	Description
Product	The common name for the product.
Executable	The executable name associated with the product.
Version	The version number for the product entry.
Interaction Percent	The percentage of time the product was interacted with out of the total time all the applications were interacted with.
Foreground Percent	The percentage of time the product spent in the foreground out of the total time all the applications spent in the foreground.
Average Interaction Minutes Per Day	The daily average number of minutes the product was interacted with.
Average Foreground Minutes Per Day	The daily average number of minutes the product spent in the foreground.
Lag	The maximum lag time between interacting with the application and getting a response.



5.5.1.3.1.3.5 User Interaction panel

This panel provides information about the last known user for the device.

Row	Description
Date	The date the interaction took place.
User Name	The domain user name who performed the interaction.
Connected From	The device the user connected to the device from.
Logon Minutes	The number of minutes the specified user has been logged on for.
Present Minutes	The number of minutes the specified user was counted as present on the device while they were logged on.
Interaction Minutes	The number of minutes the specified user interacted with the device.
User Wait Time	The amount of wait time in seconds the user spent waiting for a response from an application.



5.5.1.3.1.4 Additional Device View tabs

In addition to the **Experience** tab, there are a number of other tabs, each corresponding to an app, feature or data set implemented in Introducing Tachyon:

The **Overview** and **1E Client** tabs are always present in the **Device View**. Other tabs are visible if an app has been installed and is licensed.

Each tab has one or more panels with tiles populated with data from various sources, some by instructions that are run instantly, with results cached for 3 minutes. An appropriate error message is displayed instead of a tile in the following circumstances:

If the device is offline, as indicated by the color of the icon in the top left

The user does not have at least Viewer permission to view use the license the tab or panel

The user does not have questioner permission to run the instruction

An instruction has not been uploaded.

The Device View tabs and panels page lists the names of tabs and their panels, and a description of each tile indicating how the tile is populated.

<table>
<tr><th>Tab</th><th>Panel</th><th>Description</th><th>Data source</th></tr>
<tr><td>Overview</td><td>Details</td><td>Displays a number of tiles sorted into Identification, Hardware and Operating System and Connectivity and Activity columns that show information for the selected device retrieved from the online status information stored in the Tachyon Master database.

The columns and tiles are shown in the following table:

<table>
<tr><th>Column</th><th>Tile</th><th>Description</th></tr>
<tr><td>Identification</td><td>Identification</td><td>Displays the current device:

FQDN

Name</td></tr>
</table>
</td><td>Data from Tachyon Master (the latest online status message)</td></tr>
</table>

Tab	Panel	Description			Data source
				Domain Criticality Serial Number 1E Client Tachyon GUID.	
			Location	Displays the device's: Timezone Offset Location Locale.	
			Grouping	Displays the device: Tags - freeform	

Tab	Panel	Description		Data source
			tags applied to the device Coverage Tags - any device tags applied to the device Mgmt. Groups - lists the management groups the device is a member of.	
		Hardware and Operating	Hardware	Shows hardware details for the

Tab	Panel	Description			Data source
		System		device: Virtual/Physical Manufacturer Model Device Type Chassis Type RAM CPU Type CPU Architecture SMBIOS GUID.	
		Operating System	Shows operating system, type and version for		

Tab	Panel	Description			Data source
				example: Type Version Version Number Architecture Installation.	
		Connectivity and Activity	Connectivity	Shows current device connectivity status: Status Last Connected First Connected Certificate Type	

Tab	Panel	Description			Data source
				Certificate Expiry Connection State Local IP Address MAC Address Connecting IP.	
			Activity	Shows Last Boot date and tiem and current user.	
Env. Variables	Shows a list of the environment variables set on the device.				
Resource Usage	Two panels: **Resource Usage over the last hour** - shows system disk, CPU and memory usage per minute for the last one hour	1E-TachyonPlatform-Hardware-ResourceUsage			

<table>
<tr><th>Tab</th><th>Panel</th><th>Description</th><th>Data source</th></tr>
<tr><td></td><td>Resource Usage at day/month/year time - shows executable resource usage for a specific minute:

<table><tr><th>Column</th><th>Description</th></tr><tr><td>Product</td><td>Resource name, for example 1E Client</td></tr><tr><td>Executable</td><td>Resource executable, for example 1e.client.exe</td></tr><tr><td>Instance Count</td><td>Number of currently running instances.</td></tr><tr><td>Cpu Percent</td><td>Perentage of CPU currently being consumed.</td></tr><tr><td>Memory Virtual Mb</td><td>Virtual memory consumed in Mb.</td></tr><tr><td>Memory Physical Mb</td><td>Physical memory consumed in Mb.</td></tr><tr><td>Io Read Kb Per Second</td><td>Number of associated read input/output operations per second.</td></tr><tr><td>Io Write Kb Per Second</td><td>Number of associated write input/output operations per second.</td></tr><tr><td>Handle Count</td><td>The number of object handles.</td></tr></table></td><td>1E-TachyonPlatform-Hardware-ResourceUsageByMinute</td><td></td></tr>
<tr><td>Down loads</td><td>Summary</td><td>Download activity and status for the device. Whenever you click on an FQDN on any of the Nomad pages then the</td><td>Data from Content</td></tr>
</table>

Tab	Panel	Description	Data source
		Device View will be displayed with the **Downloads** tab selected.	Distribution.
Content	Content Titles on the selected device, the default view is from **All Sources**, **All Types** and **All Status**. **Note** You may see a difference in the number of items in a device's Nomad cache versus that displayed in the Nomad app Device View. This is because if downloaded content has been deleted from Configuration Manager, the content titles cannot be resolved in the Nomad app and are not displayed. This is under consideration for re-design and may be revised in future versions of Nomad.	Data from Content Distribution.	
Nomad Configuration	**1E Nomad Branch Settings .**	1E-Nomad-NomadBranchSettings	
Experience	**Metrics**	Metrics are the data points that are collected by the 1E Client and sent to the Tachyon server. They are collected at different intervals depending on the type of data that is being collected.	Data from Experience metrics
Trends	The Trends tab shows the changes in the scores over time. Hovering over any of the bars shows the details for that time and event. If the user viewing the device details also has the ability to	Data from Experience metrics	

<table>
<tr><th>Tab</th><th>Panel</th><th>Description</th><th>Data source</th></tr>
<tr><td></td><td>at least ask a question in Explorer the Explore button will be visible.</td><td></td><td></td></tr>
<tr><td>Logs</td><td>The Event Logs tab gives you a listing of the Windows Event log entries for that device. This brings that data to this view and is very useful when determining the root cause of an issue that has been reported on the device.</td><td>Data from Experience metrics</td><td></td></tr>
<tr><td>Application Interactions</td><td>Shows user interaction times and ratios across applications measured over the last 30 days</td><td>1E-Experience-ApplicationInteraction</td><td></td></tr>
<tr><td>User interactions</td><td>Shows user interactive sessions with activity over last 30 days.</td><td>1E-Experience-UserInteractionHistory</td><td></td></tr>
<tr><td>Hardware</td><td>Disk drives</td><td>Shows disk drives, including hardware and usage information.

Column | Description
---|---
Drive | Drive letter.
Volume Name | Volume name, if set.
Drive Type | Drive type, for example:
Removable Disk</td><td>1E-Tachyon Platform-Hardware-DiskDrives</td></tr>
</table>

Tab	Panel	Description		Data source
			Local Disk Compact Disk.	
		Size Gb	Total disk size in Gb.	
		Free Space Gb	Current free space in Gb.	
		Usage Percent	Percentage used of total drive space.	
		File System	File system, for example NTFS.	
		Manufacturer	Standard or SSD drive.	
		Model	Drive manufacturer.	
		Serial Number	Unique disk serial number.	
		Partition	Drive and partition of the specific drive.	

Tab	Panel	Description		Data source
		Firmware Revision	Drive firmware version.	
		Device ID	Device ID of the specified disk.	
Peripherals	Shows the list of plug and play hardware devices (Windows only).	1E-TachyonPlatform-Hardware-Devices		
	Column: **Device Type**	Description: Hardware device, including for example things like: Battery Monitor Keyboard Mouse Ports SoftwareDevice.		
	Column: **Name**	Description: Device name.		
	Column: **Instance Count**	Description: Number of instances of a peripheral device.		
	Column: **Service**	Description: Associated Windows service, for example atapi, serial, PCI, ACPI.		
Network	**Throughput**	Shows network throughput on all adapters for the last		1E-Tachyon Platform - Network

<table>
<tr><th>Tab</th><th>Panel</th><th>Description</th><th>Data source</th></tr>
<tr><td></td><td></td><td>hour, represented by the following tiles:

Average throughput - including Timestamp, Bytes Recieved per Second, Bytes Sent Per Second

Bytes received per second

Bytes sent per second.</td><td>- Average Throughput</td></tr>
<tr><td>Interface configuration</td><td>Returns the output from the native network interface configuration command (e.g. ipconfig or ifconfig).</td><td>1E-TachyonPlatform-Network-InterfaceConfiguration</td><td></td></tr>
<tr><td>DNS</td><td>Shows the Cache and Host file tiles:

DNS Cache Contents - with the entries from local DNS cache, Host Name and Address.

HOSTS file - shows the content of the drivers/etc/hosts file.</td><td>1E-TachyonPlatform-Network-DnsCache

1E-TachyonPlatform-Network-HostFileContent</td><td></td></tr>
<tr><td>TCP connections</td><td>Returns a list of established TCP connections.

<table><tr><th>Column</th><th>Description</th></tr><tr><td>Process Name</td><td>Local process name.</td></tr><tr><td>Process Id</td><td>Uniquely identifies an active process.</td></tr><tr><td>Class</td><td>Class of Internet networking protocol.</td></tr></table></td><td>1E-TachyonPlatform-Network-TcpConnections</td><td></td></tr>
</table>

Tab	Panel		Description	Data source
	Local Address	Local network address.		
	Local Port	Network port used by a specific process.		
	Remote Address	Source IP address from which the traffic came from.		
	Remote Port	Remote port used by a specific process.		
	Latency Ms	The time taken in milliseconds for data or a request to go from a source to a destination.		
Listening ports	Returns a list of processes which are listening for network connections.		1E-TachyonPlatform-Network-ListeningPorts	
	Column	Description		
	Process Name	Local process name.		
	Process Id	Uniquely identifies an active process.		
	Class	Class of Internet networking protocol.		
	Local Address	Local network address.		
	Local Port	Network port used by a specific process.		
	Product	Related product, for example host process for Windows Services,		

<table>
<tr><th>Tab</th><th>Panel</th><th>Description</th><th>Data source</th></tr>
<tr><td></td><td>Local Security Authority Process, SCNotification.</td><td></td><td></td></tr>
<tr><td>ARP Cache</td><td>Returns a list of processes which are listening for network connections and also shows routing tables.</td><td>1E-TachyonPlatform-Network-ArpCache

1E-TachyonPlatform-Network-RoutingTable</td><td></td></tr>
<tr><td>WIFI</td><td>Shows a list of visible wifi networks, including basic network properties.

<table>
<tr><th>Column</th><th>Description</th></tr>
<tr><td>SSID</td><td>WiFi network name.</td></tr>
<tr><td>Is Connected</td><td>Shows as either true or false, dependent on whether the corresponding adapter is connected to the network.</td></tr>
<tr><td>Is Hidden</td><td>Shows as true if the WiFi network is not broadcasting a public SSID.</td></tr>
<tr><td>Is Secure</td><td>Shows as either true or false:

true - if the WiFi network is secure

false - if the network is open.</td></tr>
<tr><td>Signal</td><td>Shows WiFi signal quality; from 0 (worst) to 100 (best).</td></tr>
<tr><td>Authentication</td><td>The default authentication mechanism supported by the network.</td></tr>
<tr><td>BSSI IDs</td><td>The Service Set Identifier (SSID) of the network, it will</td></tr>
</table>
</td><td>1E-TachyonPlatform-Network-WiFiNetworks</td><td></td></tr>
</table>

Tab	Panel		Description	Data source
		be empty if the network is hidden.		
	Encryption	Shows the default encryption mechanism supported by the network.		
	Adapter	Shows the WiFi network adapter name to which this network is visible.		
Policies	**Rules Compliance**		Column / Description: **Rule Name** — Name of rules applied to the current device. The viewable list relates to the selected Tachyon policy from the policy dropdown on the page. **State** — If the device state is Compliant, Noncompliant or Not Applicable.	Data from Guaranteed State

Tab	Panel	Description		Data source
		Type	Rule type: Check - allows you to verify that a device has a particular state, such as a registry key having a specific value Fix - allows you to define a desired state for the device and then enforce that state.	
		Effectiveness	Policy rule effectiveness is the usefulness of policy rules and is represented as either: Disabled - the rule has not yet been enabled from the	

Tab	Panel	Description	Data source
		Guaranteed State Rule Administration page, so it is not currently active Unassigned - the rule is enabled, but has not been deployed to any devices Ineffective - the rule has been deployed, but no devices have changed their compliance position for this rule in the last thirty days Effective - the rule has been deployed and at least one device has changed	

Tab	Panel	Description		Data source
			its compliance position for this rule in the last thirty days.	
		History	Rule history.	
Software	**Installations**	Shows (per-device) installed software.		1E-TachyonPlatform-Software-Installations
		Column	Description	
		Product	Software product name.	
		Publisher	Software publisher.	
		Version	Product version number.	
		Architecture	Instruction set architecture (ISA) version.	
		Install Date	Software installation date.	
Windows	Shows list of installed Windows services and their current state.	1E-TachyonPlatform-Software-Services		

<table>
<tr><th>Tab</th><th>Panel</th><th>Description</th><th>Data source</th></tr>
<tr><td>services</td><td>Column
Description

Name
Windows service name.

State
Windows service state, Running or Stopped.

Startup Type
Windows service startup type, for example Automatic, Automatic (Delayed Start), Manual, Disabled.

Process Id
Uniquely identifies an active process.

Description
Windows service description.

Logon Account
Windows service logon account context.

Type
Windows services type, for example file system driver, kernel driver, shared process.</td><td></td><td></td></tr>
<tr><td>Env. Variables</td><td>Shows operating system environment variables.</td><td></td><td>1E-TachyonPlatform-Software-EnvironmentVariables</td></tr>
<tr><td>Processes</td><td>Shows detailed information about all running processes.

Column
Description

Product
Software product name.

Executable
Executable name.</td><td></td><td>1E-TachyonPlatform-Software-Processes</td></tr>
</table>

Tab	Panel	Description	Data source
	Version	Product version number.	
	Devices count	How many devices are reporting.	
	Crashes	Number of times this software crashed during the last 24-hour reporting period.	
	Hangs	Number of times this software crashed during the last 24-hour reporting period. **Note** Software crash and hang information is obtained from Windows event data. For background information on Windows events and the event viewer refer to https://support.microsoft.com/en-gb/help/302542/how-to-diagnose-system-problems-with-event-viewer-in-microsoft-windows	
	Performance anomalies	Number of performance anomalies detected in this software during the last 24-hour reporting period.	
	I/O write KB/s	Average disk I/O read rate per second during the last 24-hour reporting period.	

Tab	Panel	Description	Data source
	I/O write KB/s	Average disk I/O write rate per second during the last 24-hour reporting period. **Note** For background information on analyzing disk storage performance refer to https://docs.microsoft.com/en-gb/archive/blogs/cotw/analyzing-storage-performance	
	Virtual Memory Usage KB	Average Virtual Memory Usage KB during the last 24-hour reporting period. **Note** For an explanation of Windows Virtual Memory organization refer to https://answers.microsoft.com/en-us/windows/forum/windows_10-performance/physical-and-virtual-memory-in-windows-10/e36fb5bc-9ac8-49af-951c-e7d39b979938 and https://support.microsoft.com/en-us/help/2160852/ram-virtual-memory-pagefile-and-memory-management-in-windows	
	Processor Time Seconds	Each instance of the executable will burn processor time. This column gives the average of the total time consumed by each process instance per second. Each instance uses the sum of all time used by each core in parallel. Therefore, it is possible to see more seconds here than in a day	

Tab	Panel	Description	Data source
		(usually 60 x 60 x 24 = 86400) for the whole column, if your system is working extremely hard 24x7. The theoretical maximum would be somewhere near ***number of cores*** x ***seconds per day*** . Hence, 'Processor Time' rather than 'Human Time'	
	Processor Time %	This is an easier notion than Processor Time Seconds. This is the average of the processor consumption of each instance. Each instance of this process will have caused different percentages of compute resource in all the processors and cores to be used over time (unless they have specifically requested certain core affinity). For each minute each process is running, a profile of the usage is built for the whole day. This value is the average of all of those samples. There is no way to work out, for any one of the process instances involved, how long any particular instance was running for. This could indicate a process that is going wild with resources, but it would take more investigation on the device to discover for how long this is happening. It is perfectly possible to see all the values in this column adding up to more than 100% as the processes were not necessarily running at the same time. **Note** For further information on Processor time refer to https://social.technet.microsoft.com/wiki/contents/articles/12984.understanding-processor-processor-time-	

Tab	Panel	Description	Data source

and-process-processor-time.aspx

Responsiveness Impact %

An indicator of how reactive a process is to activity by other processes on the device. Typically, anti-virus products watch and respond to potentially suspicious activity such as increased network traffic. Anti-virus products will differ in their impact on the overall performance of a device.

Note

Responsiveness Impact % is used to indicate how sensitive a process appears to be to the use of system resources by other processes on a device. For example, Security Protection software present on a device may reveal a spike in its activity whenever a new process is started on that device.

This would typically be because the Security Protection software may wish to ensure that the new process starting on the device is present in a security white list. Other software may also react to activity by other processes and by reacting they impact system resource uses, thereby adversely affecting the user's experience. So it is useful to be able to identify

Tab	Panel	Description	Data source
		software with the highest Responsiveness Impact on a device and potentially investigate further. **Note** Responsiveness Impact % represents the proportion of the increased CPU activity detected by the 1E Client as a result of performing a set of operating system-level operations that can be attributed to a given running process. Examples of these would be Windows registry and resource creation operations. It is reported as a percentage to normalize results across devices that offer a range of computing power. For example, if *software.exe* on a device is attributed a Responsiveness Impact of 53% this means that more than half of the spike in CPU usage caused by software monitoring activity on that device can be attributed to *software.*	
	Handle Count	Average number of Windows handles used by this software during the last 24-hour reporting period. **Note**	

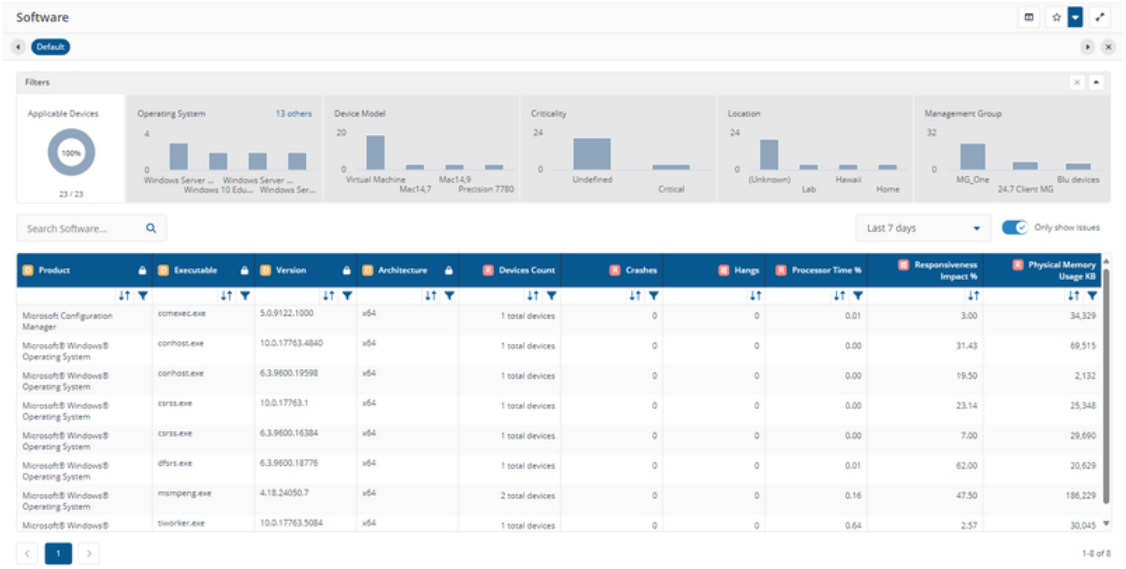
Tab	Panel		Description	Data source
		For further information on Windows handles refer to https://docs.microsoft.com/en-us/windows/win32/sysinfo/handles-and-objects For tips on examining open handles for any Windows process refer to https://docs.microsoft.com/en-us/sysinternals/downloads/handle and https://techcommunity.microsoft.com/t5/windows-blog-archive/pushing-the-limits-of-windows-handles/ba-p/723848		
	Physical Memory Usage KB	Average Physical Memory Usage KB during the last 24-hour reporting period. **Note** Please refer to https://docs.microsoft.com/en-us/sysinternals/downloads/rammap for a useful tool to examine physical memory allocation on a device.		
1E Client	**Binaries**		Shows a list of the binary files in the executable folder of the 1E Client. Column: **File Name** Description: Associated 1E	1E-Tachyon Platform-Client-Binaries

Tab	Panel	Description		Data source
			Client file name.	
		File Version	Software version.	
		File Size	File size in bytes.	
		Description	File description	
		Date Created	The date the file was written to disk.	
		Date Modified	The date the file was last saved.	
Configuration file	Shows the full content of the 1E Client configuration file, including: Logging settings Communication settings Agent settings Module settings.			1E-TachyonPlatform-Client-ConfigFileContent
Extensibility	Shows extensibility objects (modules and providers) loaded by the 1E Client. Column: **Type** — Description: Module or Provider component.			1E-TachyonPlatform-Client-Extensibility

Tab	Panel		Description	Data source
	Binary Name	Associated 1E Client binary name, for example 1E.Client.Module.Interaction.dll		
	Name	Name, for example Interaction.		
	Version	1E Client version, for example 5.2.5.251		
Local Storage	Shows **Data Files** and **Client Inventory Database Use** tiles that display the list of: Data files (logs, databases, etc) created by the 1E client Tables in the 1E Client Inventory database, along with a row count per table.		1E-TachyonPlatform-Client-DataFiles 1E-TachyonPlatform-Client-InventoryDatabaseUse	

5.5.1.3.2 Software page

The Software page provides a tabular listing of all the Software products that are installed in the environment (including executable, version, architecture). The second set of columns in the list provide additional metrics or event details associated with the Software products.



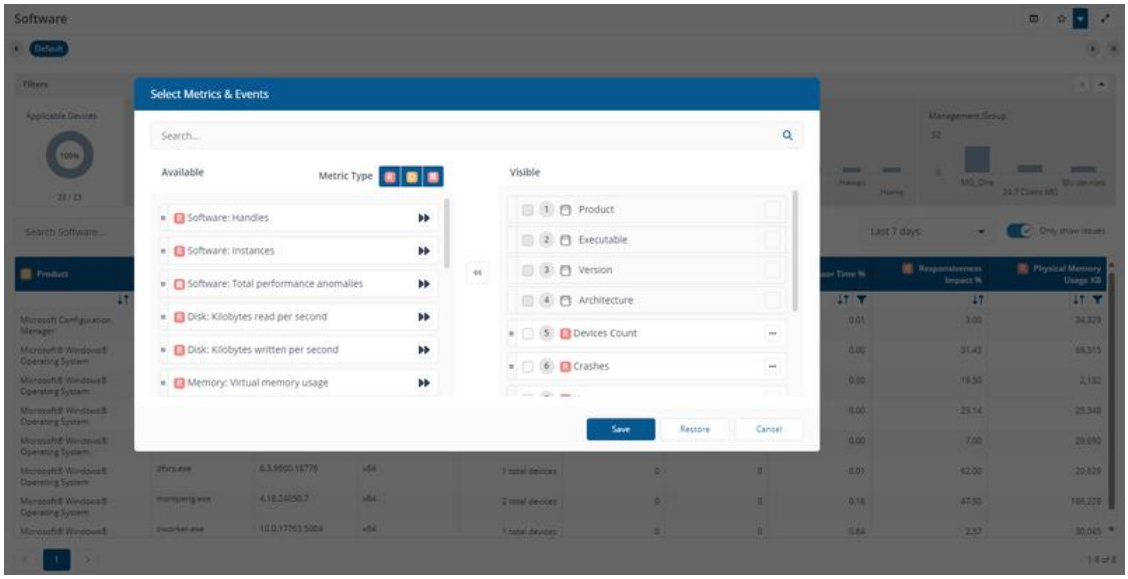
5.5.1.3.2.1 Filtering and navigation

The drop-down selection at the top right of the page allows you to select to display data for the last 90, 60, 30 or 7 days.

The **Filters** at the top of the page, also lets you focus the data, allowing you to center your insights on specific areas of the environment. For example, specific Operating Systems and/or Locations.

The table can be sorted by each column (ascending or descending), as well as filtered based on the available columns values.

You also have the ability to add or remove columns from the tabular listing, which is present at the bottom of the page, based on the level of detail that your investigation requires. You can also set the new structure of the page as a persistent preset.



Clicking on a row filters the table to only display entries that match the **Product**, **Executable**, **Version** and **Architecture** values for that row. The table displayed subsequently omits the **Product**, **Executable**, **Version** and **Architecture** columns, as these will all be the same, so you can focus your attention on the rest of the data.

5.5.1.3.2.2 Software page metrics

The other metrics or events that can be added and removed from the list are:

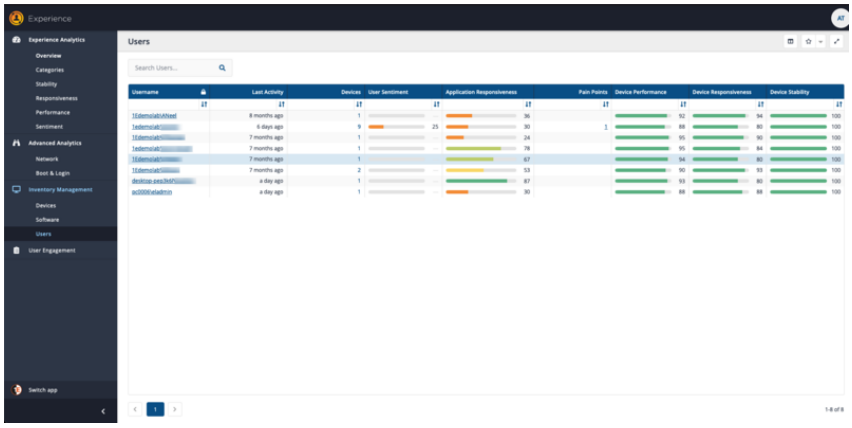
Metric	Description
Devices Count	Number of devices on which the Software product and its associated process is installed.
Crashes	Number of crashes that have occurred for the Software product's process during the reporting period.
Hangs	Number of hangs that have occurred for the Software product's process during the reporting period.

Metric	Description
Processor Time %	Average processor time for the Software product's process during the reporting period.
Sensitivity/Responsiveness Impact %	How sensitive this software product's process appears to be in relation to operating system activity used to indicate how reactive a process is to activity by other processes on the device.
Physical Memory Usage KB	Average memory usage in KB for the Software product's process during the reporting period.
Virtual Memory Usage KB	Average Virtual Memory Usage KB for Software product's process during the reporting period.
Handles	Average number of Windows handles used by this Software product's process during the reporting period.
Processor Time Seconds	Average total process time consumed by the Software product's process instance per second during the reporting period.
Kilobytes read per second	Average KB read from disk per second by the Software product's process during the reporting period.
Kilobytes write per second	Average KB written to disk per second by the Software product's process during the reporting period.
Disk Read IOPS	Average disk I/O read rate per second of the Software product's process during the reporting period.
Disk Write IOPS	Average disk I/O wire rate per second of the Software product's process during the reporting period.
Bytes Received per Second	Average network bytes received per second for the Software product's process during the reporting period.
Bytes Sent per Second	Average network bytes sent per second for the Software product's process during the reporting period.
Bytes Exchange per Second	Average sum of network bytes received and sent per second for the Software product's process during the reporting period.

Metric	Description
Total Megabytes Sent	Total network megabytes sent for the Software product's process during the reporting period.
Total Megabytes Received	Total network megabytes received for the Software product's process during the reporting period.

5.5.1.3.3 Users page

The **Users** page displays user experience information, with measurements of how well their devices are providing them with a good experience combined with their user survey responses.



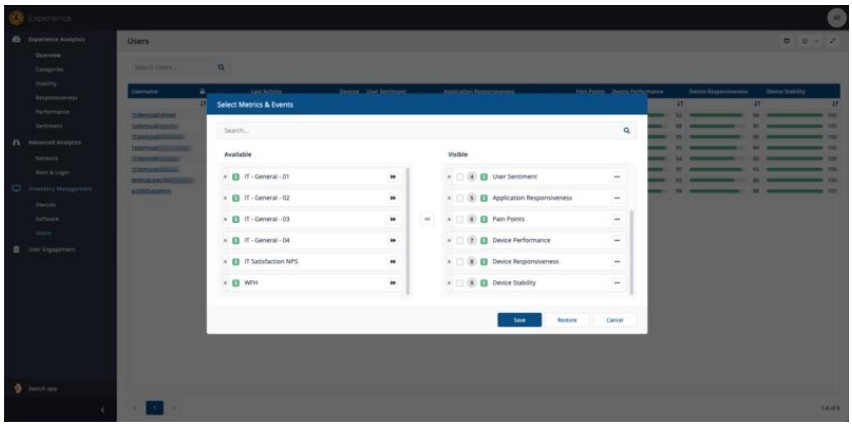
5.5.1.3.3.1 The Users page

Here you can find all of the user-related information in Experience. The main part of the page is the Users table, which displays the following information:

Column	Description
Username	The name of the user. This is a link to a page that provides data specific to that user, as gathered by Experience.
Last Activity	The last time data was gathered for the user.
Devices	The number of devices the user is associated with.
User Sentiment	The user's latest User Sentiment score.
Application Responsiveness	The latest score for how reactive the user's sessions have been.

Column	Description
Pain Points	The number of entries where the latest User Sentiment score is marked as Poor (orange) or Very Poor (red with an exclamation mark). The number is a link, which displays the particular user's Sentiment Survey responses, filtered to show the latest and just Poor or Very Poor ratings.
Device Performance	The average device performance for the user and their devices.
Device Responsiveness	The lowest score for device responsiveness for the user across all their devices.
Device Stability	The score for device stability for the user across all their devices.
Additional Metrics	Any Metric that has been created by an Experience Survey Administrator as part of defining a new User Sentiment Survey. These aren't shown by default but can be added from the **Select Metrics** popup.

You can also control the information that is displayed in the table using the **Select Metrics** button in the page header, which displays the Select Metrics popup, allowing you to determine which columns get displayed and in which order.

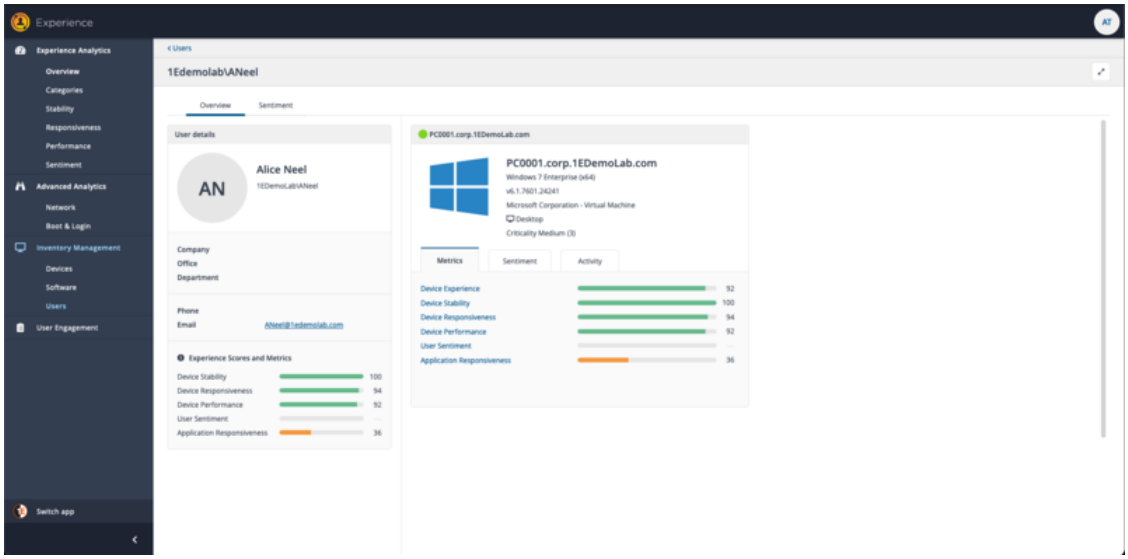


5.5.1.3.3.2 The Users page - Overview tab

This page is displayed when you click on a username on the **Users** page and shows all of the details that have been gathered or derived for that user. There are two main tabs on the page: **Overview**, as shown in the picture opposite, and **Sentiment**, which displays a list of the user's survey responses.

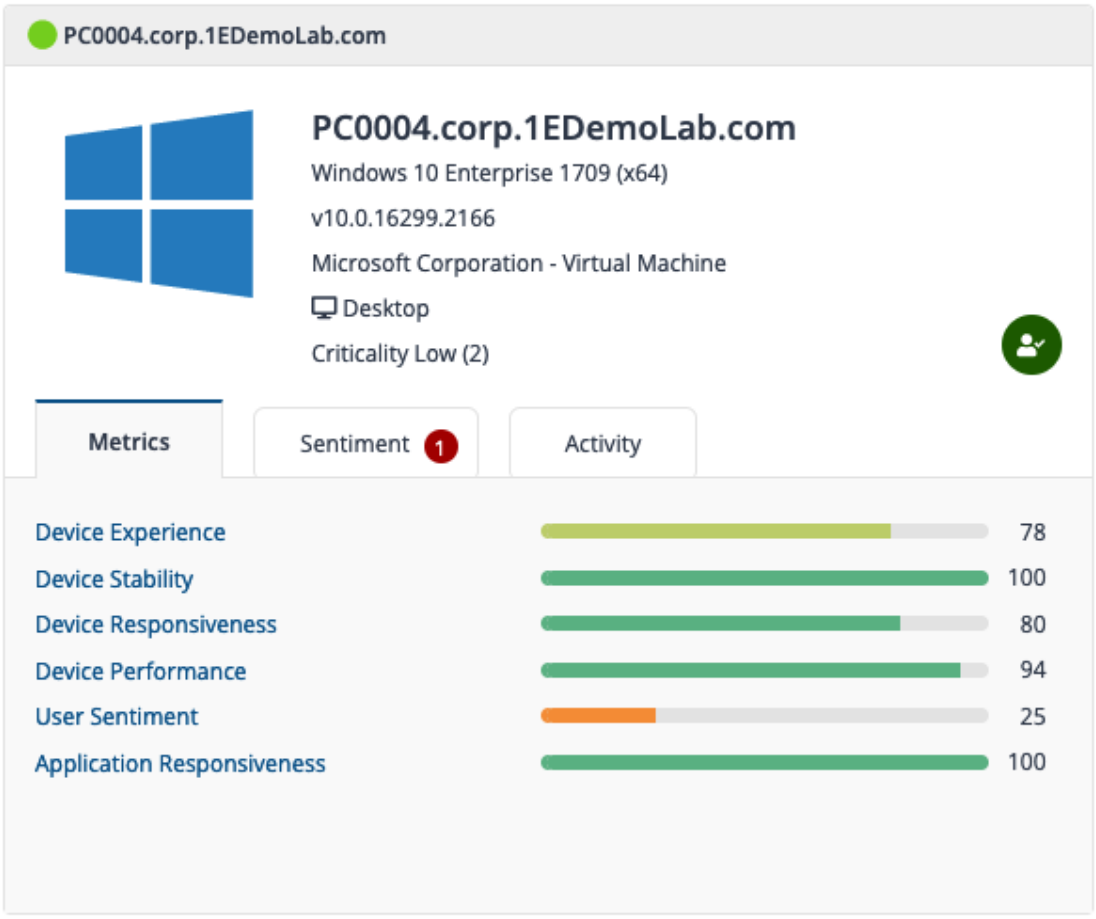
The **Overview** tab displays the following information:

User details - a panel that displays information for the user that is held in AD and the aggregated scores for that user, as derived by the Experience application from all of the devices the user is associated with and their User Sentiment Survey responses.



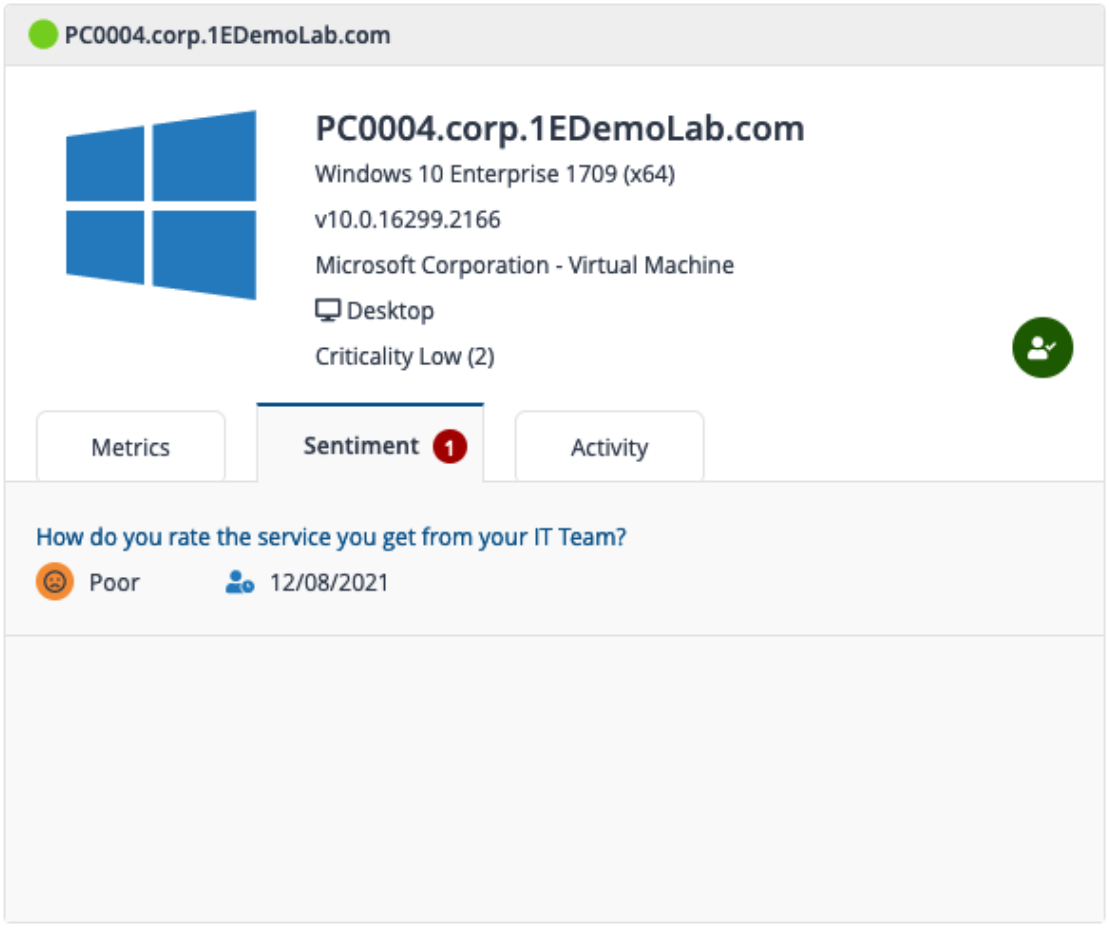
5.5.1.3.3.2.1 The Device Panel Metrics tab

To the right of the **User details** panel are device panels for all of the devices the user is associated with. The device panel displays some basic information about the device, as gathered by Tachyon, and three tabs: **Metrics**, **Sentiment** and **Activity**.



5.5.1.3.3.2.2 The Device Panel Sentiment tab

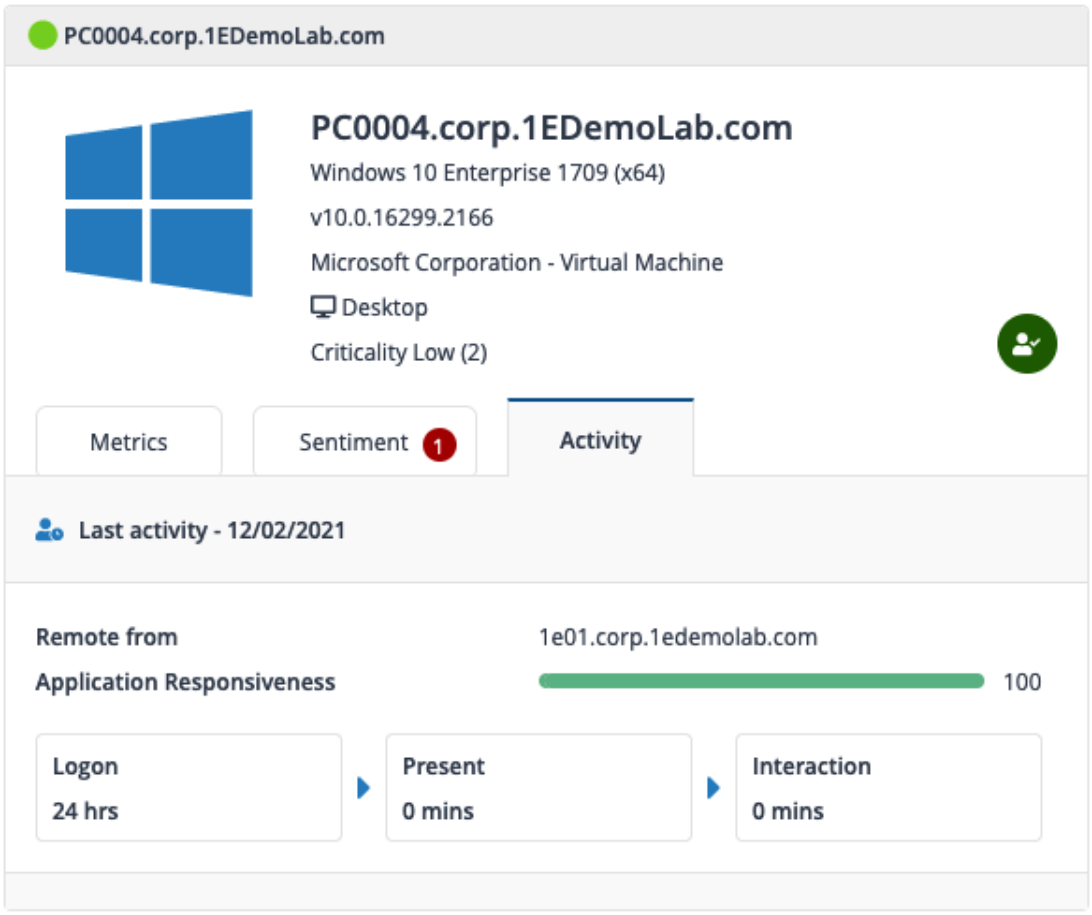
The picture opposite shows the Device Panel **Sentiment** tab for **ACME-WIN1002.acme.local**. This displays the last responses to User Sentiment Surveys made by the user on that device, clicking on the question link displays the user page **Sentiment** tab filtered to show just the responses to that question on that device.



5.5.1.3.3.2.3 The Device Panel Activity tab

The **Activity** tab shows when the user was last logged on to the device, where they accessed it from, how well their session is performing in terms of how reactive it is.

There is also an indication of how long they have been logged on, how long they've been present at the device and how long their current interaction with the device has been.



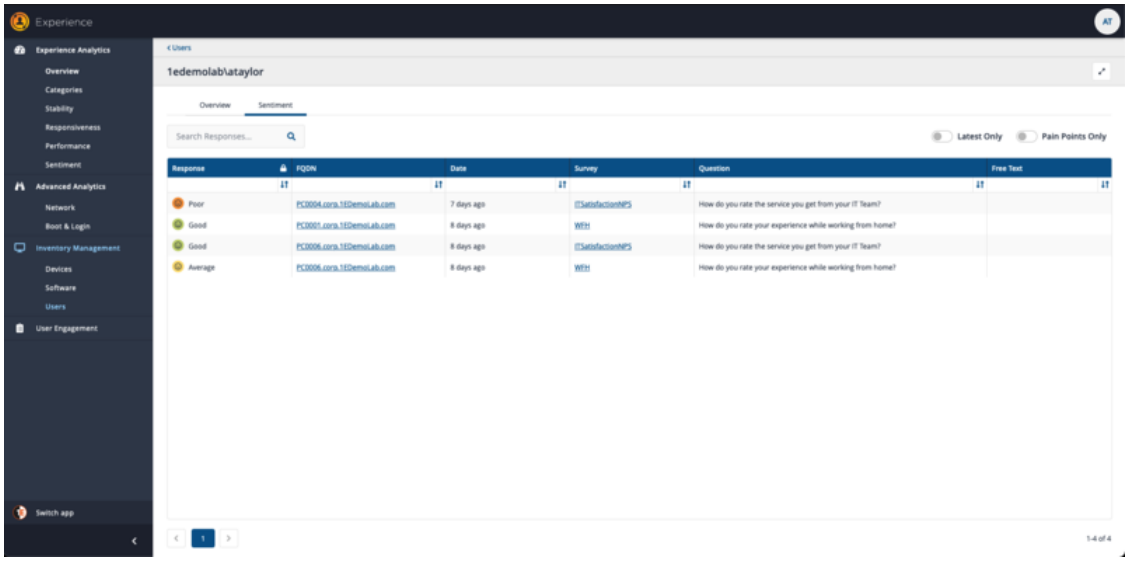
5.5.1.3.3.3 *The User page - Sentiment tab*

Here you can see all of the responses made by a user to any User Sentiment Surveys they have received. The main part of this page is a searchable Responses table:

Column	Description
Response	The response they made to a User Sentiment Survey.
FQDN	The FQDN for the device where they made the response. This is a link to the Devices page for the device, where you can view all of the device metrics.
Date	How long ago they made the response.
Survey	The User Sentiment Survey name. This is a link to the Survey page for the survey, where you can view all the Survey responses.
Question	The question for the User Sentiment Survey.

Column	Description
Free text	Any free text they entered when responding.

You also have the option for viewing the latest responses to the survey by switching the **Latest Only** toggle to on. You can also select to display only the responses that are rated **Poor** or **Very Poor** by switching the **Pain Points Only** toggle to on.



5.5.1.4 User Engagement page

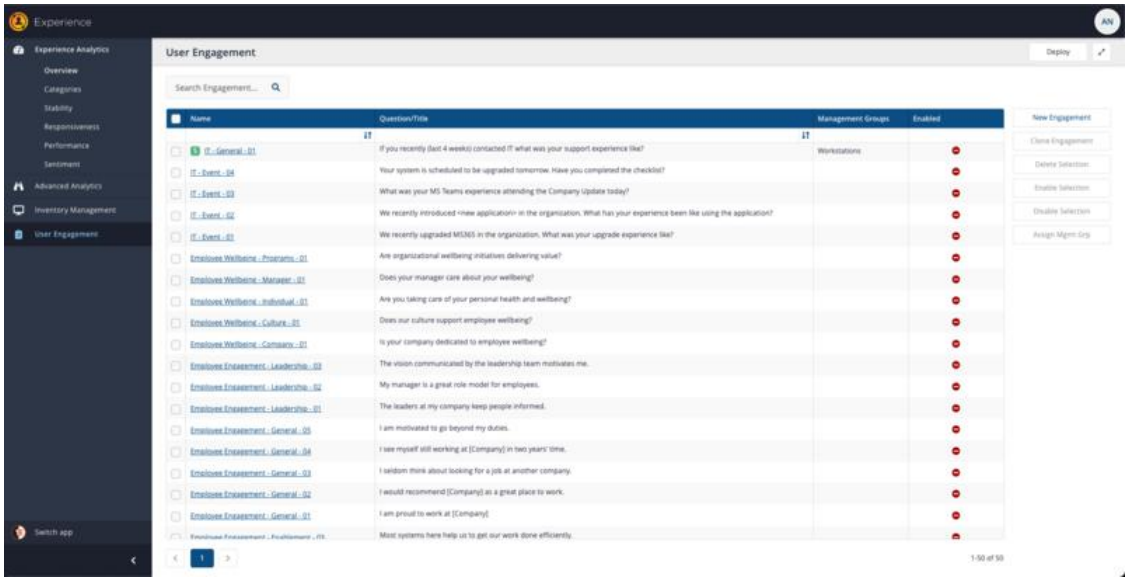
The **User Engagement** page lets you create and manage Sentiment and informational surveys, to gain direct feedback related to end-user experience, as well as create and manage Announcements to communicate with your end-users.

There are three types of **User Engagement**:

Sentiment Surveys - have well-defined responses that contribute to the overall Sentiment score, and the returned results can be visualized under the format of charts on the Sentiment page.

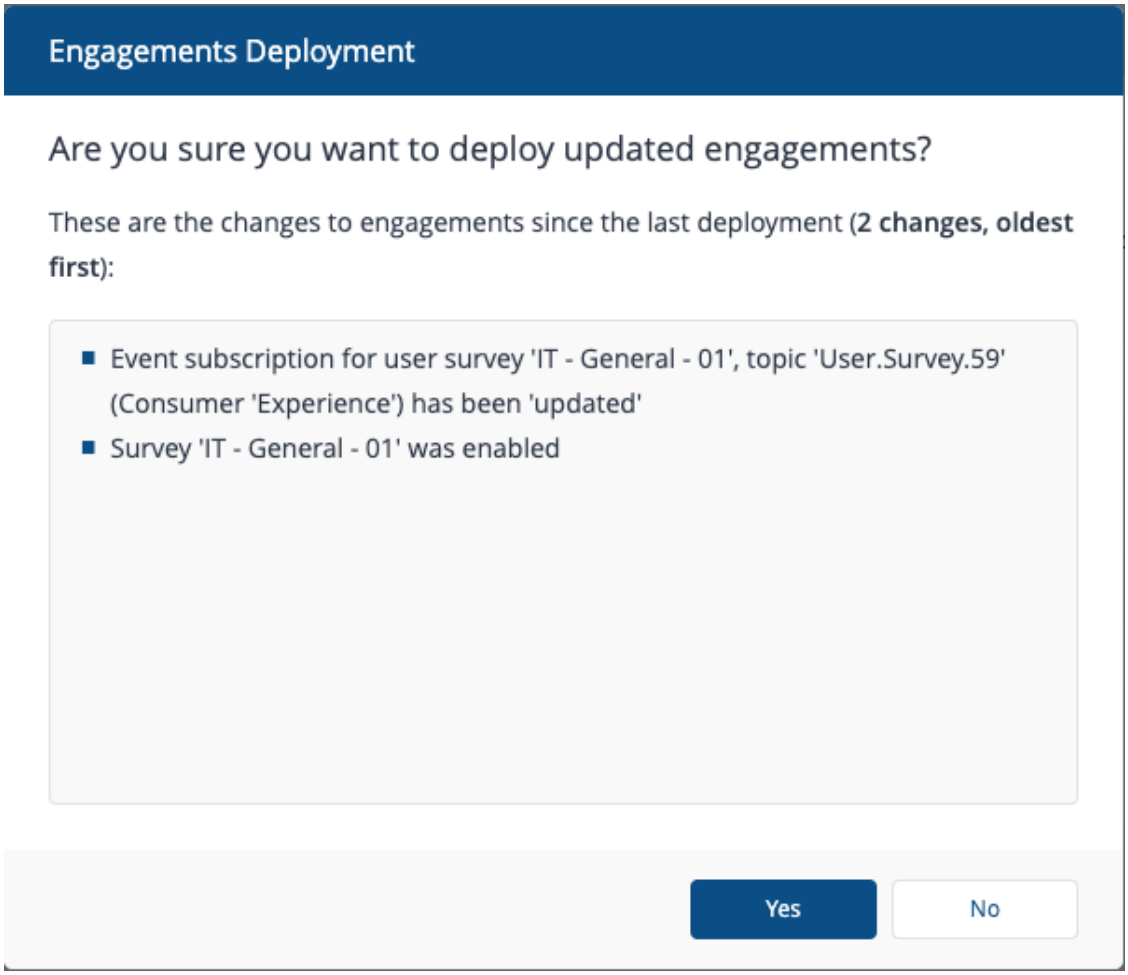
Info Surveys - can be customized to a greater extent than the Sentiment surveys, but they do not contribute to the overall Sentiment score.

Announcements – these are one-way communications which can be used for a variety of use cases, such as broadcasting to end-users information about organizational changes, IT news and updates and more.



5.5.1.4.1 The User Engagement page

At the top of the page, in the header, is a **Deploy** button. This must be used whenever you want to apply any of the changes you make to the devices targeted by either Surveys or Announcements. When you click the **Deploy** button, an **Engagements Deployment** popup appears, as shown in the picture opposite, with a list of changes that have been made.



The main part of the **User Announcements** page is represented by a searchable table:

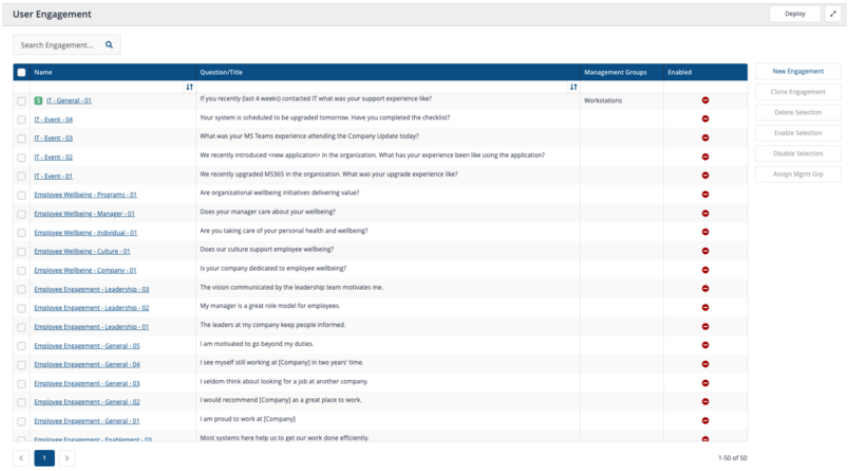
Column	Description
Name	The name of the **Engagement**. This also is a link to the User Engagement details page that provides all the information you need to monitor related to either the Survey's responses or User Engagement results. For Sentiment Surveys, the name is also a Metric that contributes towards the Sentiment score. You can monitor it using a chart on the **Sentiment** page, and appears under the **Sentiment** heading of the Device Metrics - displayed when viewing device details from the Devices page. Sentiment Surveys are marked by a Survey icon - S Announcements are marked by an Announcement Icon - A

Column	Description
Question/Title	Shows the question set for the Survey or, for Announcements, the Title.
Management Groups	The Management Groups set for a User Engagement determine which devices the Survey or Announcement is sent to.
Enabled	This indicates whether the User Engagement is enabled or not. Only enabled Engagements that are deployed become visible to end-users.

There are also a number of action buttons, related to the selections in the table.

Button	Description
New Engagement	Displays the **New Engagement** page where you can create a new Sentiment Survey, Info Survey or Announcement. This button is only enabled if there are no selections in the User Engagement table.
Clone Engagement	Displays the **New Engagement** page pre-filled with the details from the Survey or Announcement currently selected in the User Engagement table. This button is only enabled if there is a single selection in the**User Engagement**table.
Delete Selection	Deletes the selected Survey(s) and/or Announcement(s) in the User Engagement table. Clicking this button displays the **Engagement Deletion** popup. This button is only enabled if there is one or more selections in the**User Engagement**table.
Enable Selection	Enables all the selected Survey(s) and/or Announcement(s) in the User Engagement table regardless of their current enabled state. Clicking this button displays the **Enable Engagement** popup. This button is only enabled if there is one or more selections in the**User Engagemen**t table.
Disable Selection	Disables all the selected Survey(s) and/or Announcements in the User Engagement table, regardless of their current enabled state. Clicking this button displays the **Disable Engagement** popup.

Button	Description
	This button is only enabled if there is one or more selections in the **User Engagement** table.
Assign Mgmt Grp	Assigns Management Groups to the selected Survey(s) and/or Announcements in the User Engagement table. Clicking this button displays the **Assign Management Groups** popup. This button is only enabled if there is one or more selections in the**User Engagement**table.



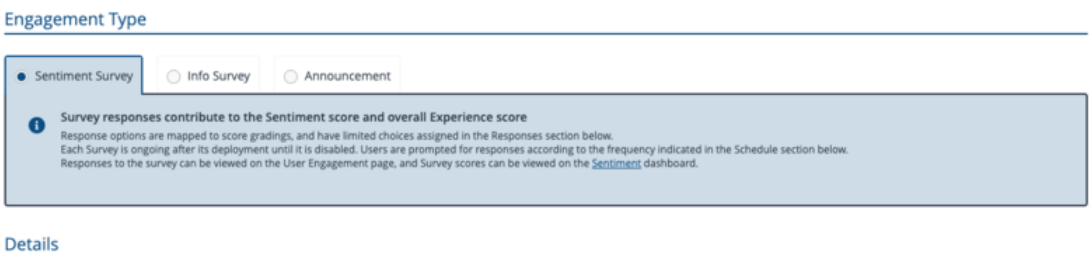
5.5.1.4.2 The New Engagement page

Clicking on the **New Engagement** button in the User Engagement table displays the **New Engagement** page, where you can define all the parts to your new Engagement.

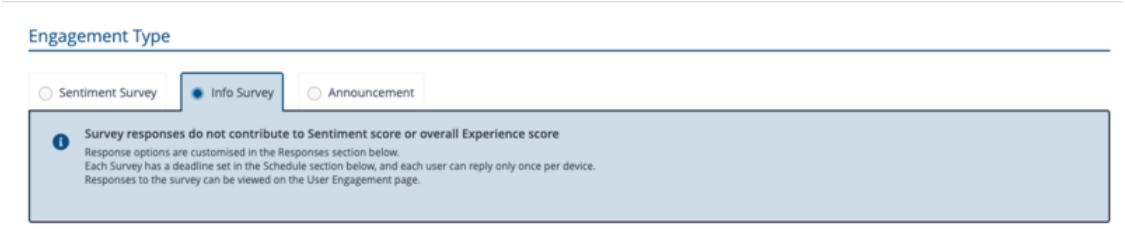
5.5.1.4.2.1 Engagement Type

The first choice is the **Engagement Type** here you can choose between Sentiment Survey, Info Survey or Announcement types. The controls displayed for each type are different.

The default **Engagement Type** selected on the **New Engagement** page is **Sentiment Survey**, as shown in the picture opposite.



If you want to define an **Info Survey** or an **Announcement** you must select that option under the **Engagement Type** heading.

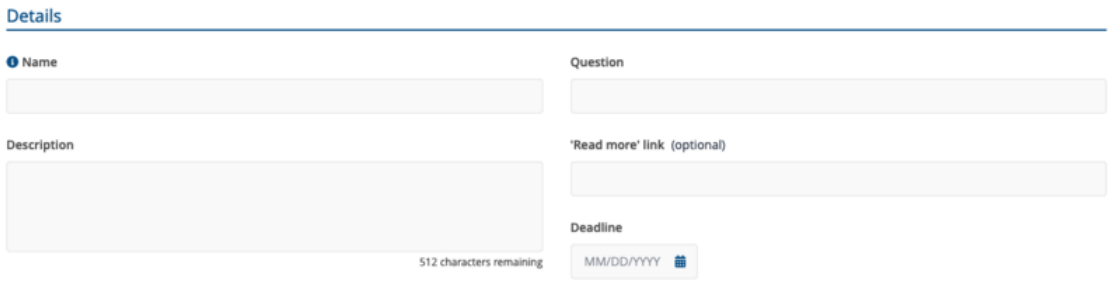


5.5.1.4.2.2 Survey Details

For Sentiment and Info Surveys here you define the **Name**, **Question**, **Description** and an optional **Link** to further information. The Details section is **almost the same** for Sentiment Surveys and Info Surveys, with one difference detailed in the last row of the following table.

Field	Description
Name	Defines how the Survey is referred to in the Experience UI. For Sentiment Surveys, the Name also defines the name of the Metric the responses will be scored on.
Question	Sets the question you will be asking your end-users. You should design your questions carefully, as they will be sent to end-users, and you will want to maximize your responses. Some guidance and thoughts can be found on Getting feedback via User Sentiment Surveys: Names, Questions, Descriptions and Responses. The **Question** can be a maximum of **128** characters, including the question mark.
Description	Used to support and provide context for the **Question**, the **Description** is also displayed to end-users. The **Description** can be a maximum of **512** characters.
Link (optional)	Lets you specify the URL to any additional information you want to add to help support and provide context for the question. The text for the link is displayed to end-users as **Click here to find out more**. This field is optional.
Prompt Question Cadence or Deadline	This section is different for **Sentiment Surveys** and **Info Surveys** and reflects the nature of the two types of Survey. For **Sentiment Surveys** you are trying to get information on a Metric that you want to measure progress on over time. This means that you want to prompt your end-users to respond on a regular basis. For this reason this section for

Field	Description
	Sentiment Surveys provides an option where you can set to **Prompt question every x days**. For **Info Surveys** you are trying to get feedback on a particular topic on a one-off basis. Your end-users aren't likely to all respond immediately, so you want to send a cut-off date that prevents the Survey from going stale, but still allows your end-users to send responses when they can. For this reason, this section for Info Surveys provides a **Deadline** field with a date picker that lets you choose when to stop prompting users that haven't yet responded.



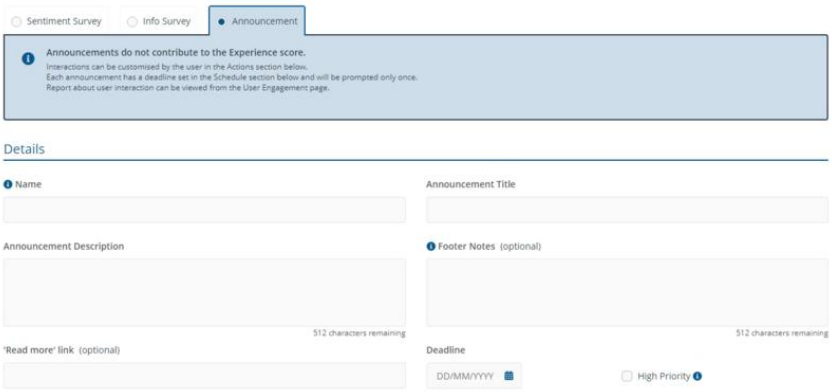
5.5.1.4.2.3 Announcement Details

For **Announcements** here you define the **Name**, **Announcement Title**, **Announcement Description, Footer Notes**, an optional **Link** to further information, the **Deadline**, as well whether the Announcement should be **High Priority**.

Each section described in the following table:

Field	Description
Name	Defines how the **Announcement** is referred to in Experience.
Announcement Title	Sets the title that end-users will see when the **Announcement** will display on their device. The **Title** can be a maximum of **128** characters.
Announcement Description	Used to for the actual content of the **Announcement,** and is displayed to end-users. The **Description** can be a maximum of **512** characters.
Footer Notes (optional)	This section can be used to add disclaimers or contact information relevant for the **Announcement**.

Field	Description
	The **Footer Notes** can be a maximum of **512** characters.
Deadline	For **Announcements** you are trying to broadcast information on a particular topic on a one-off basis. Your end-users aren't likely to all review the Announcement immediately, and the Announcement may cease to be relevant after a certain period of time, so you want to send a cut-off date that prevents the Announcement from going stale. For this reason, this section for Announcements provides a**Deadline**field with a date picker that lets you choose when to stop prompting users that haven't yet seen the announcement.
High Priority	For Announcements considered urgent, and need to be immediately displayed on the end-user devices, select this option. If **High Priority**is selected, the 1E Client, which manages the timing for any engagement displayed to the end-user, will show the announcement immediately after the announcement has been deployed, and the 1E Client receives it.



5.5.1.4.2.4 Survey Responses

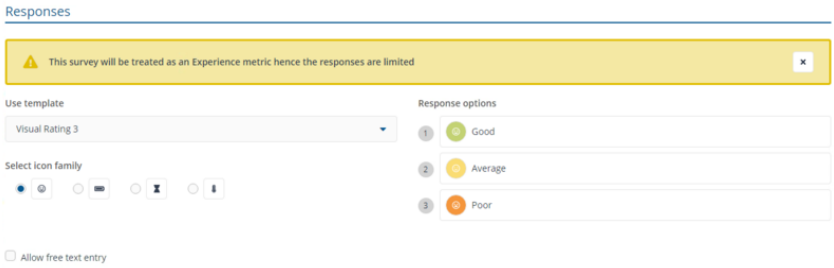
The Responses section of a Survey differs slightly depending on whether you are creating a Sentiment Survey or Info Survey. The main headings are the same, though. The picture opposite shows the Responses section for a Sentiment Survey.

Field	Description
Use template	Provides a template to base the responses on. For Sentiment Responses the selected templates are fixed and cannot be edited. For Info Surveys you can edit

Field	Description
	the text for the responses added by selecting a template and then add or delete more responses, up to a maximum of 10.

Template	Description
Visual Rating 3	Provides 3 options: **Good**, **Average** and **Poor** with icons that help to visually describe the rating.
Visual Rating 5	Provides 5 options: **Very Good**, **Good**, **Average**, **Poor** and **Very Poor** with icons that help to visually describe the rating.
Numeric Rating 3	Provides 3 options: **Good**, **Average** and **Poor** with numbers that rank the rating.
Numeric Rating 5	Provides 5 options: **Very Good**, **Good**, **Average**, **Poor** and **Very Poor** with numbers that rank the rating.
Custom	This option is only available to Info Surveys and starts off with no items that are preset. When using this option, you will also be prompted to add at least two options to the Info Survey.

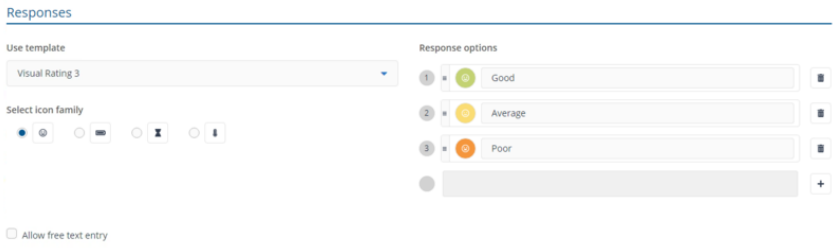
Select icon family	This heading is only displayed if you have selected either of the Visual Rating templates. It is available to both types of Survey and lets you select the family of icons that will be used to represent the visually rated options. There are four family options available: Smileys, Bars, Hourglasses and Thermometers. The icons chosen are for display purposes only and have no effect whatsoever on the responses or their score.
Response options	This field shows the options that correspond to the currently selected template and icon family (if appropriate). For Info Surveys the names, icons used and number of options can be edited.
Allow free text entry	This checkbox sets whether the end-user gets the option to enter free text to support or qualify their selection. When checked, the end-user will see a text edit field with the label **Anything more you'd like to tell us?** The free text responses can be viewed along with the response entry in the Survey Responses page.



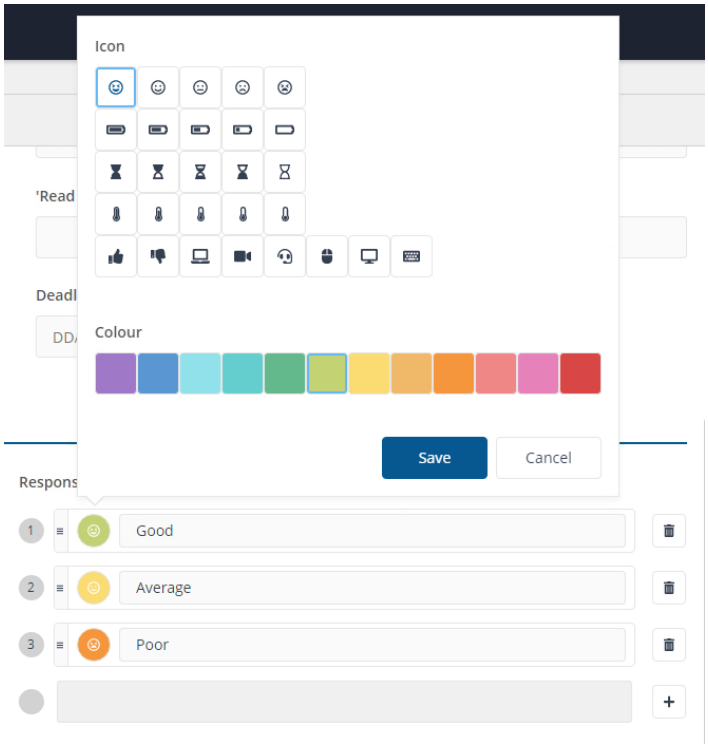
The picture opposite shows the Responses section for Info Surveys.

Here you can see that there is a delete option at the end of each response option and there is a + button for adding more options. You can add up to 10 options in total.

Clicking in the text field for an option lets you edit the text.



Clicking the colored circle for an option displays a popup where you can change the color and icon used to display the option, as shown in the picture opposite. Click **Save** when you've finished making changes.

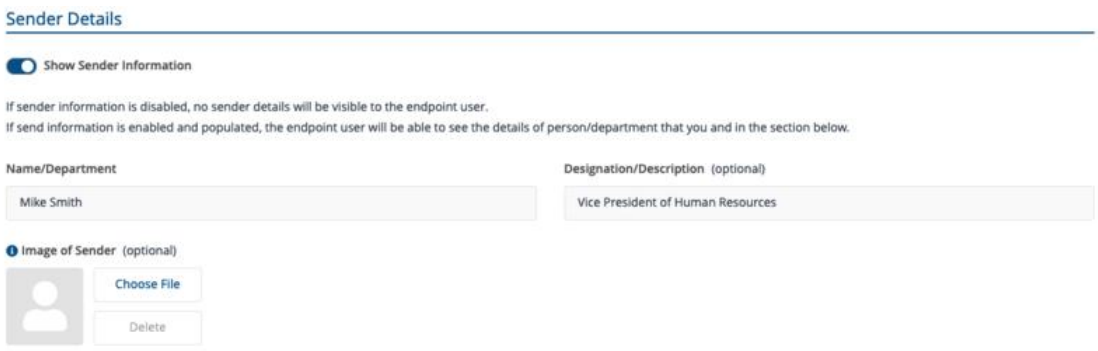


5.5.1.4.2.5 Announcement Sender Details

The **Sender Details** section of **Announcements** allows personalization of this type of user engagement, by adding additional fields to the Announcement. This section can be disabled from an Announcement by switching the **Show Sender Information** Toggle to **Off**.

Each section of **Sender Details** is described in the following table:

Field	Description
Name/Department	Sets a Name or a Department on behalf of whom the Announcement is sent and which the end-users will see when the announcement is displayed on their device. The Name/Department can be a maximum of**64**characters.
Designation/ Description (optional)	Sets the Designation or the Description associated with either the Name or Department, which the end-users see when the announcement is displayed on their device. **Designation** can be used to add a **Role** or **Function** if the Sender is an **Individual**. The Description can be used to add the Department Description, when the Sender is a Department. The**Designation/Description**can be a maximum of**128**characters.
Image of Sender (optional)	Sets an **Image** associated with either the Sender Name or Department, which the end-users will see when the announcement is displayed on their device. If no image is selected, the default user interaction image/logo, as configured for the 1E Client will be used for the announcement. **Note** The supported file types are .png and .jpg and the maximum size is 200 KB.



5.5.1.4.2.6 Announcement Actions

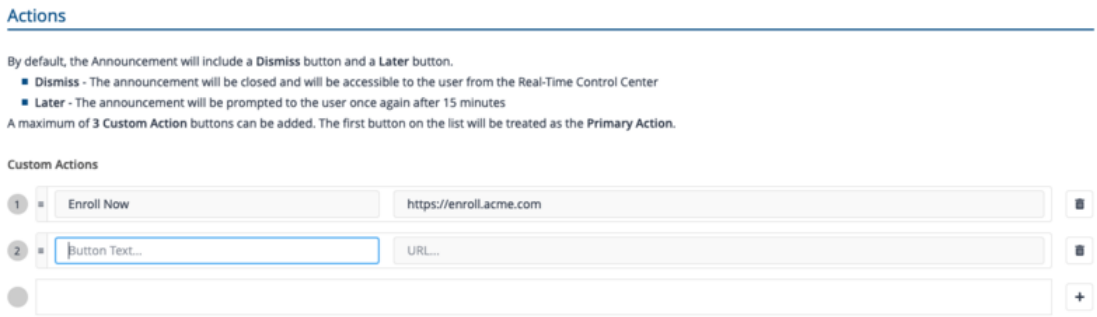
By default, any created Announcement includes a **Dismiss** button and a **Later** button.

Dismiss - The announcement is closed and will be accessible to the user from the Real-Time Control Center (1E Client User Interface)

Later - The announcement will be prompted to the user again after 15 minutes.

If additional actions under the format of buttons, a maximum of **3 Custom Action** buttons can be added. The first button on the list will be treated as the **Primary Action**.

For the Tachyon Platform 8.0 release, the only supported actions are under the format of URLs, which are displayed as buttons to end-users.

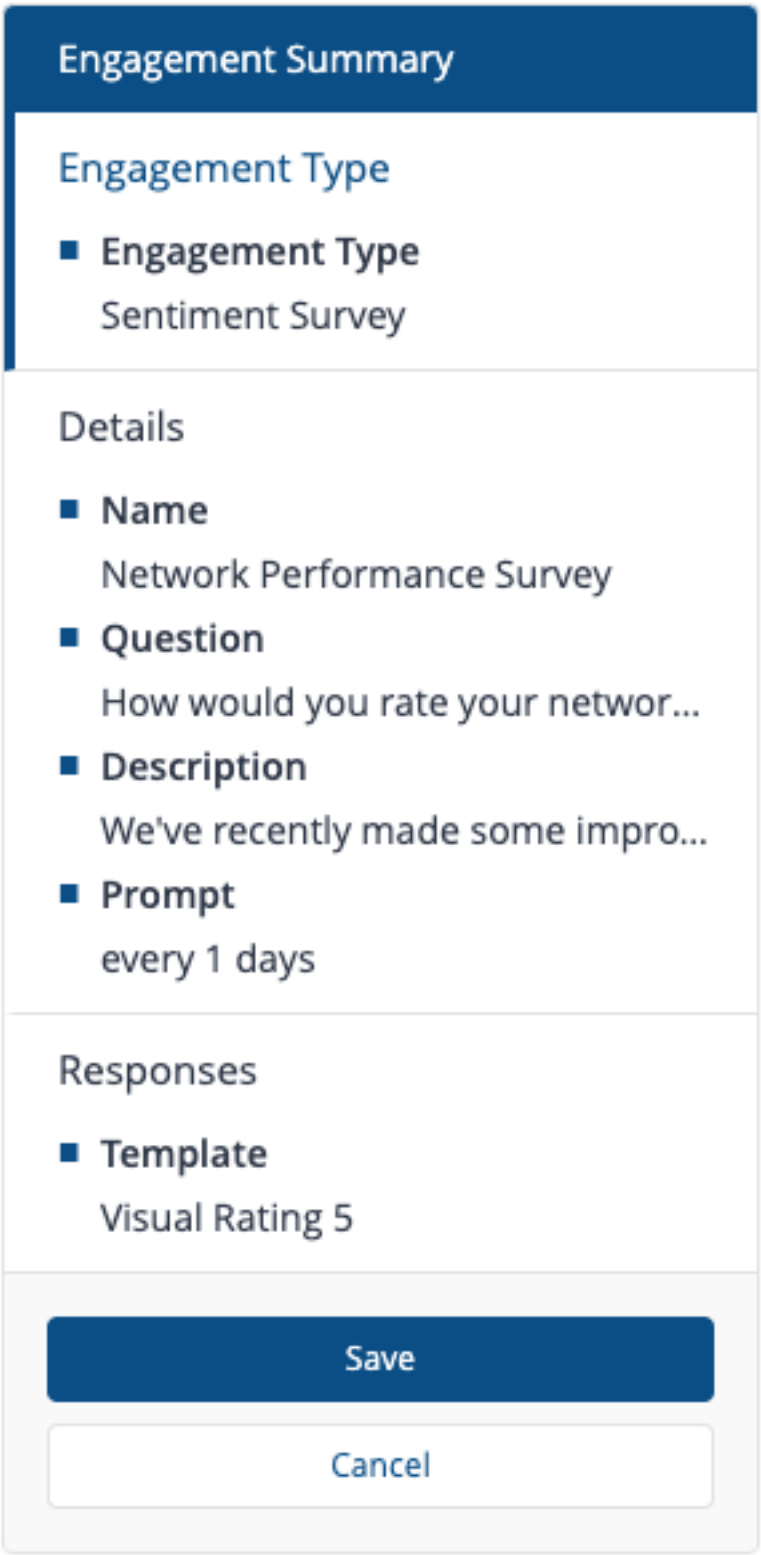


5.5.1.4.2.7 User Engagement Summary

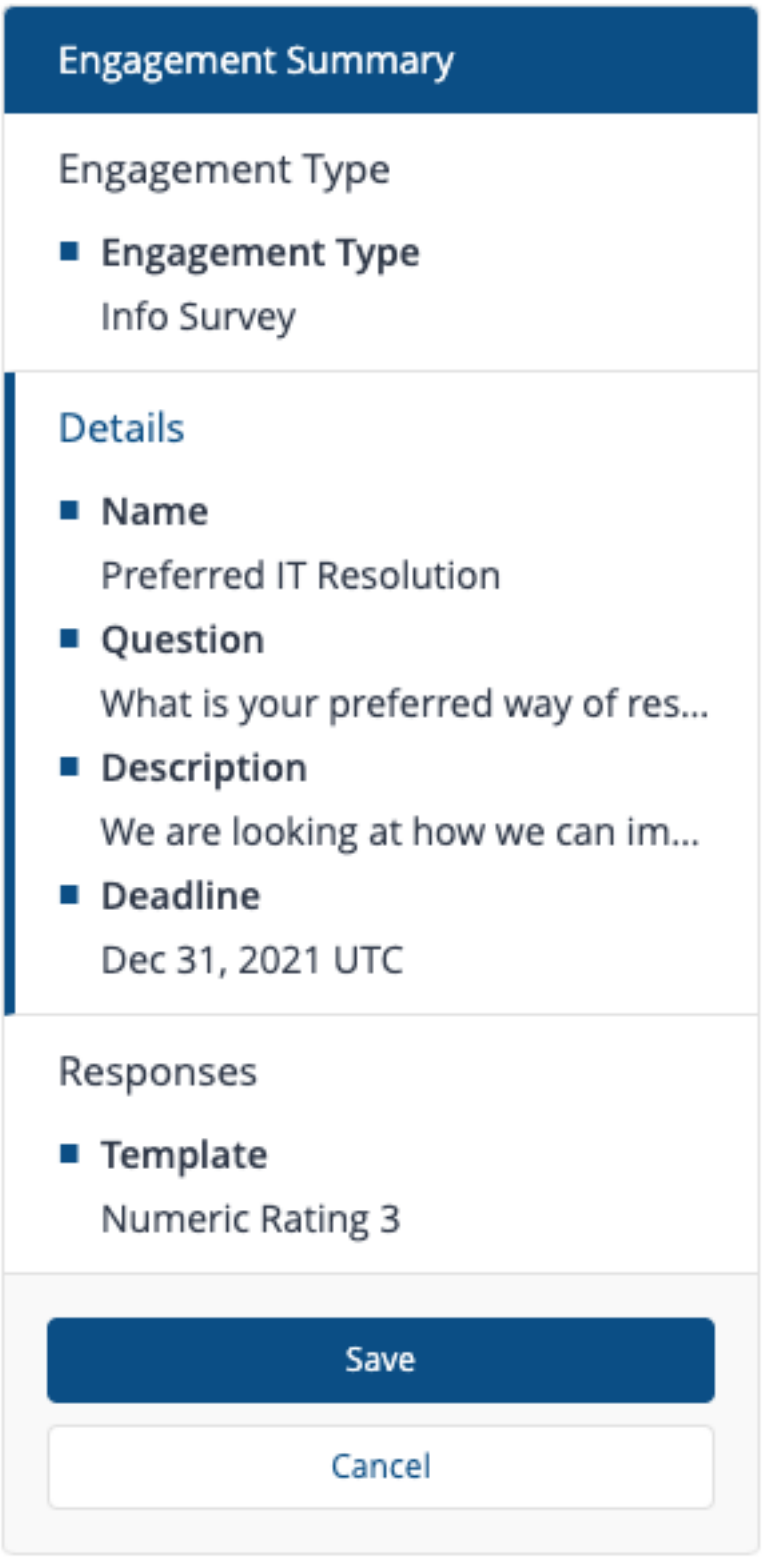
This section provides a summary of the entries that you've made in the **New Engagement** page. It also contains the **Save** and **Cancel** buttons.

There's a slight difference between the headings in the **Engagement Summary** for the different types of Surveys or Announcement. Sentiment Surveys have a heading called **Prompt**, Info Surveys have a heading called **Deadline** and Announcements have headings that include the **Sender Details and Actions**.

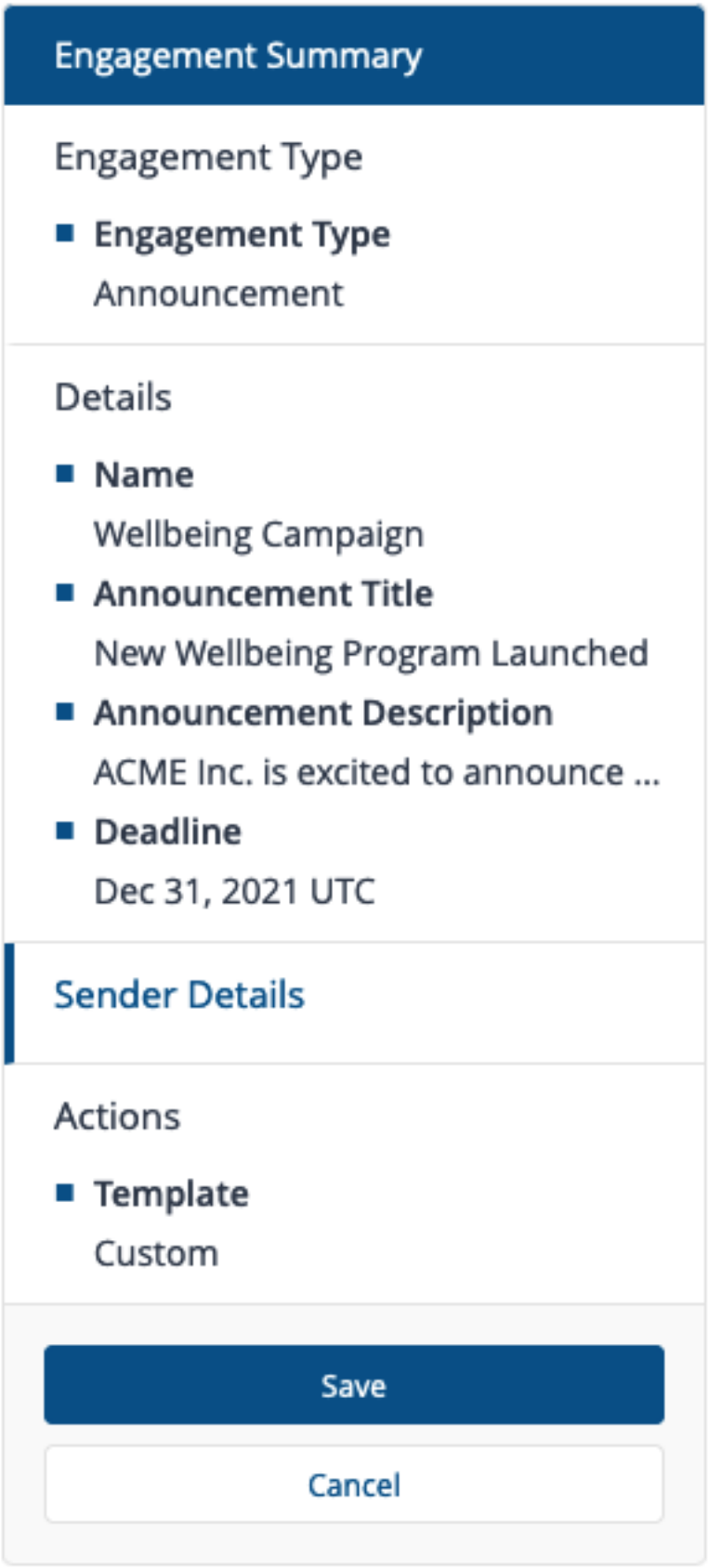
The picture opposite shows the **Engagement Summary** for a Sentiment Survey.



The picture opposite shows the **Engagement Summary** for an Info Survey.



The picture opposite shows the **Engagement Summary** for an Announcement.


Engagement Summary
Engagement Type
Engagement Type
Announcement
Details
Name
Wellbeing Campaign
Announcement Title
New Wellbeing Program Launched
Announcement Description
ACME Inc. is excited to announce ...
Deadline
Dec 31, 2021 UTC
Sender Details
Actions
Template
Custom
Save
Cancel

When you have finished making changes to your Survey, you click **Save** to close the **New Survey** page. At this point, your new Survey will need to be enabled and deployed before it appears to end-users. You will also check the Management Group assigned to the Survey.

5.5.1.4.3 Clone Selection

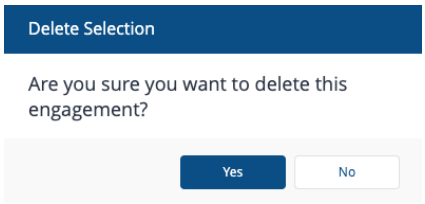
There are a number of reasons why you would choose to create a copy of a User Engagement. You may want to create a survey with a new question and description but keep everything else the same as an existing one. Also, User Engagements cannot be edited, once you have created a User Engagement the only way to change it is to create and edit a copy. Subsequently, you would then need to disable the previous one and enable and deploy the copy.

You can copy a single existing User Engagement by selecting it from the User Engagement table and clicking the **Clone Selection** button. This displays the **New Engagement** page pre-filled with all the details from the selected User Engagement. When doing this, you must change the name of the Engagement, so it doesn't clash with the previous one. You then modify the rest of the parameters as needed and click **Save** to save the copy.

5.5.1.4.4 Delete Selection

To delete one or more User Engagements, select them from the User Engagements table and click the **Delete Selection** button. An **Engagement Deletion** popup will be displayed asking you to confirm the deletion. Click **Yes** to remove the Selection from Experience.

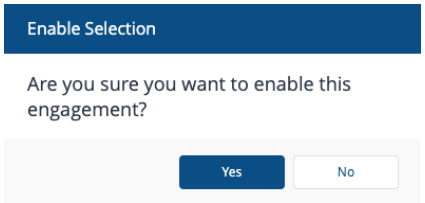
The User Engagement will no longer appear in the User Engagement table, however, before the deletions take effect on any previously targeted devices they must be deployed.



5.5.1.4.5 Enable Selection

To enable one or more User Engagements, select them from the User Engagement table and click the **Enable Selection** button. An **Enable Engagement** popup will be displayed asking you to confirm that you want to enable the selected Engagement. Click **Yes** to enable the selected Engagement.

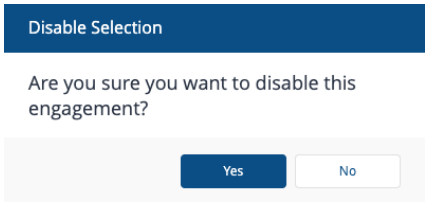
The selected User Engagement will appear as enabled in the User Engagement table, however, before the enablement changes take effect on any targeted devices they must be deployed.



5.5.1.4.6 Disable Survey

To disable one or more User Engagements, select them from the User Engagement table and click the **Disable Selection** button. A **Disable Engagement** popup will be displayed asking you to confirm that you want to disable the selected User Engagement. Click **Yes** to disable the selected User Engagement.

The selected User Engagement will appear as disabled in the User Engagement table, however, before the disablement changes take effect on any targeted devices they must be deployed.



5.5.1.4.7 Assign Mgmt Grp

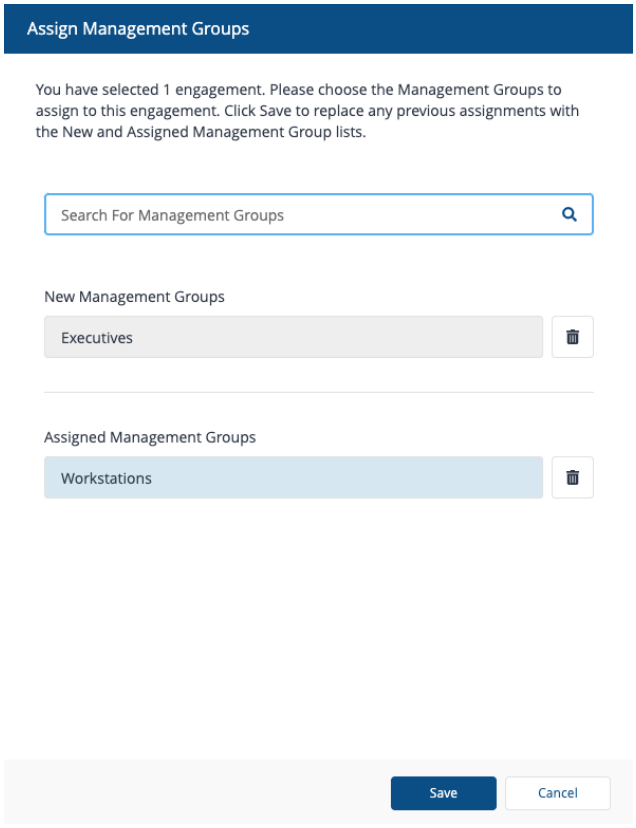
Before an Info Survey or Announcement can be deployed, you will need to set a Management Group to define the devices where the Survey and or Announcement will be sent. For Sentiment Surveys, the default **All Devices** Management Group is set when it is created.

You can set the Management Groups for one or more selected Surveys or Announcements in the User Engagement table by clicking the **Assign Mgmt Grp** button. Doing this displays the **Assign Management Groups** popup.

You can search for previously created Management Groups in the search field and add them to the **Assigned Management Groups** by clicking on the list of matches.

Clicking **Save** will assign the Management Groups to all the selected User Engagements.

Before changes to the Management Groups for a Survey or an Announcement take effect, you must deploy them.



5.5.1.5 Filters

Information about how to use the **Filters** bar that appears at the top of Experience pages.

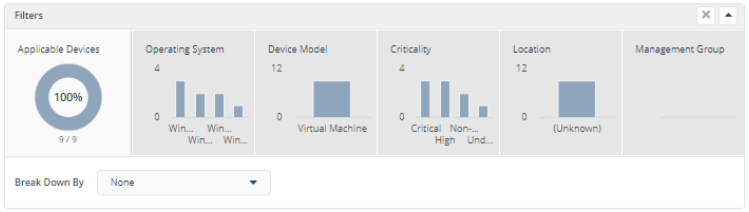
5.5.1.5.1 Experience Filters

The **Filters** bar appears at the top of most of the pages in Experience. Each section in the **Filters** bar allows a user to quickly and easily filter based on different categories. When a filter is set it applies to all the tiles on the page.

On the Stability, Responsiveness, Performance and Sentiment pages there is also a **Break Down By** selector that reconfigures the charts to show the data divided up into the selected category.

On the **Overview**, **Categories**, **Devices**, and **Software** pages there is no option for **Break Down By**.

On the **Users** and **Surveys** pages the **Filters** bar is not available.



5.5.1.5.2 The Filters bar

The following sections are displayed on the **Filters** bar:

Section	Description
Applicable Devices	This section shows the total number of devices that have been selected for the current view and the percentage of the environment those devices comprise. If no filtering is selected, the applicable devices will be 100% of the environment and will display the total number.
Operating System	This section will allow you to create a filter based on the Operating System. The bars represent the different operating systems that make up the environment.
Device Model	This section will allow you to create a filter based on the Model. The bars represent all the models that are in the environment.
Criticality	This section will allow you to create a filter based on the Criticality setting of the devices. Criticality is set using a Tachyon instruction. The details on setting Criticality can be found here Using Device Criticality.
Location	This section will allow you to create a filter based on the Location setting of the devices. Location is set using a Tachyon instruction. The details on setting Location can be found here Using Location.
Management Group	This section will allow you to create a filter based on the Management Group membership(s) of the devices. Each bar represents a Management Group in Tachyon. The details on Management Groups can be found here Management Groups page page.
Collapse/Expand	The Up or Down Arrow on the far right of the Filters and Breakdown bar allows you to collapse or expand the bar. Collapsing removes the details from view and leaves only the title of the bar. This allows you to focus on the details of the data when you have the filter of your choice created.

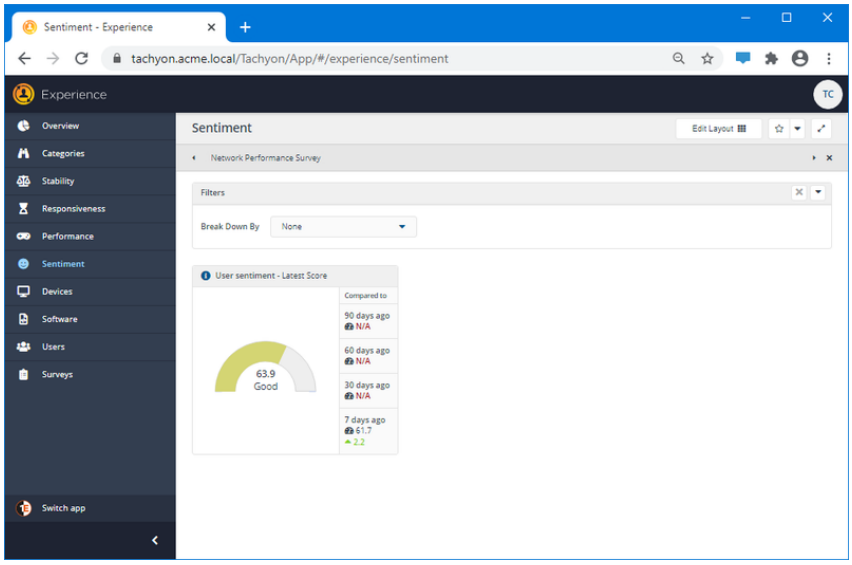
5.5.1.5.3 Using the Filters Bar

The Filters bar can be used to immediately apply filters and, on some pages, to also apply a break down to the data that is displayed.

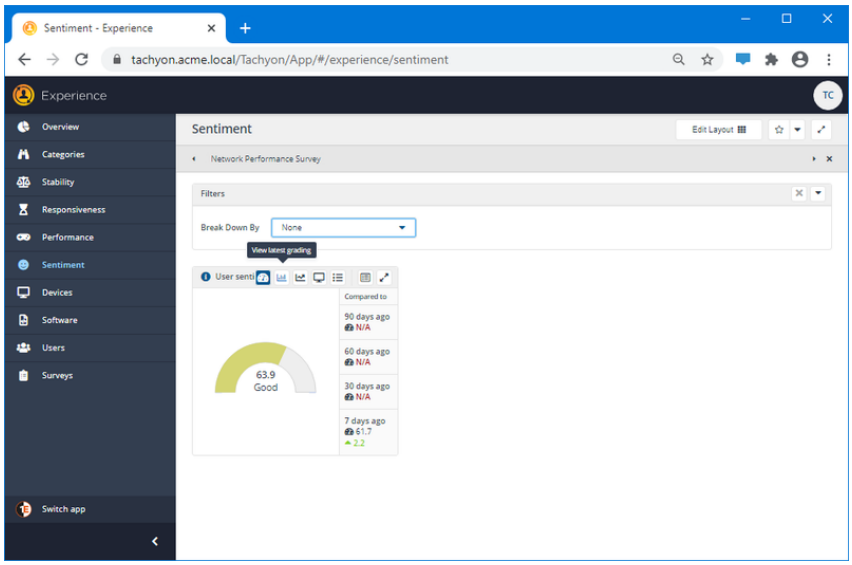
5.5.1.5.3.1 Using the Break Down By selector

We'll first take a look at the Break Down By selector, which is available on the Stability, Responsiveness, Performance and Sentiment pages.

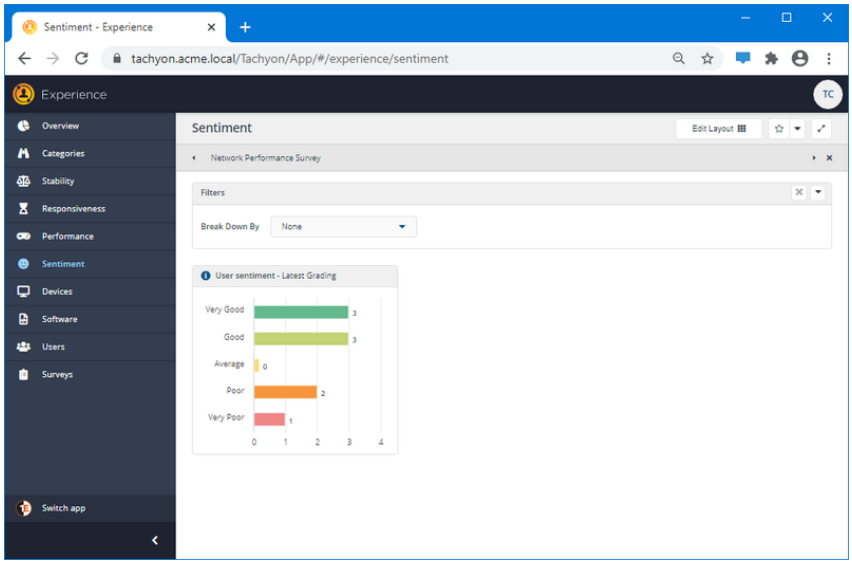
The picture opposite shows the **Sentiment** page with the **Break Down By** selector visible.



To show the effects of the **Break Down By** selector we are going to change the chart to **View latest grading**, which is done from the title bar of the chart - as shown in the picture opposite.



The picture opposite shows the **User sentiment - Latest Grading** chart before the **Break Down By** has been applied.



The **Break Down By** selector lets you choose from:

Operating System

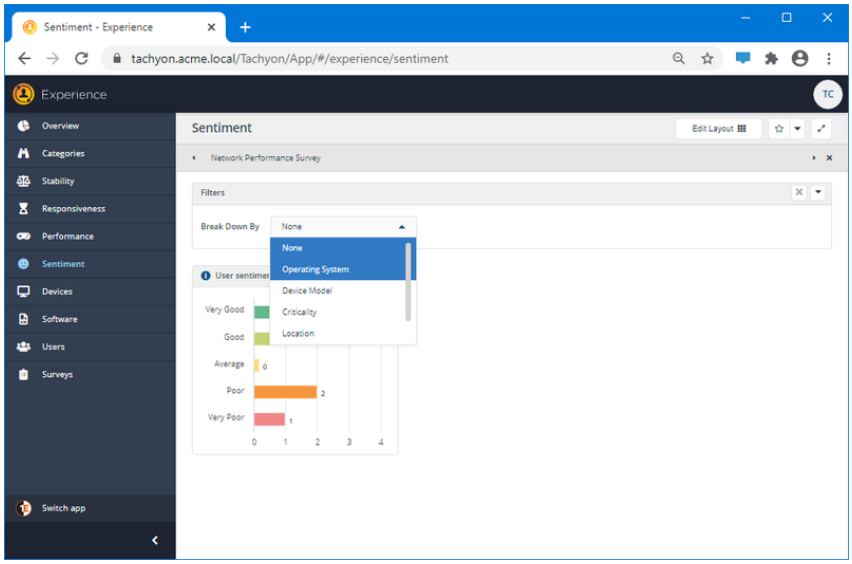
Device Model

Criticality

Location

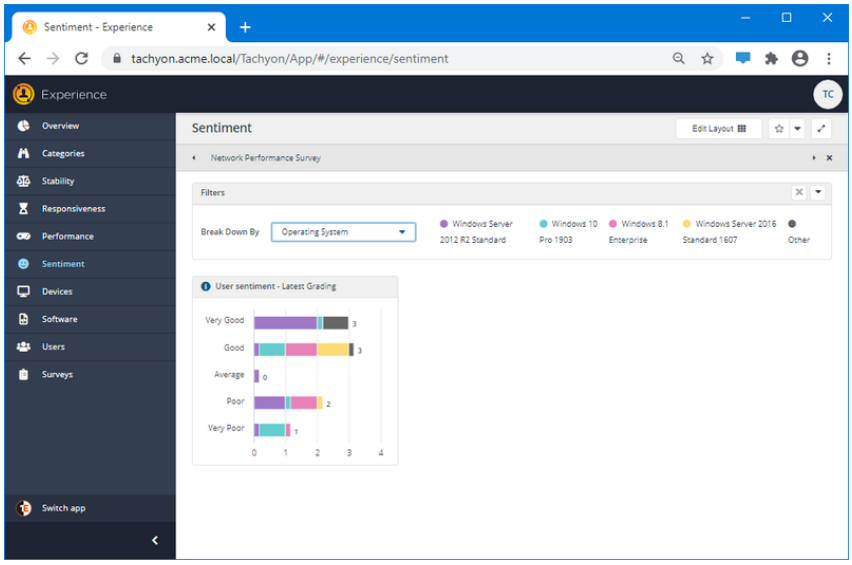
Management Group

In our example we're going to use the **Operating System** break down.

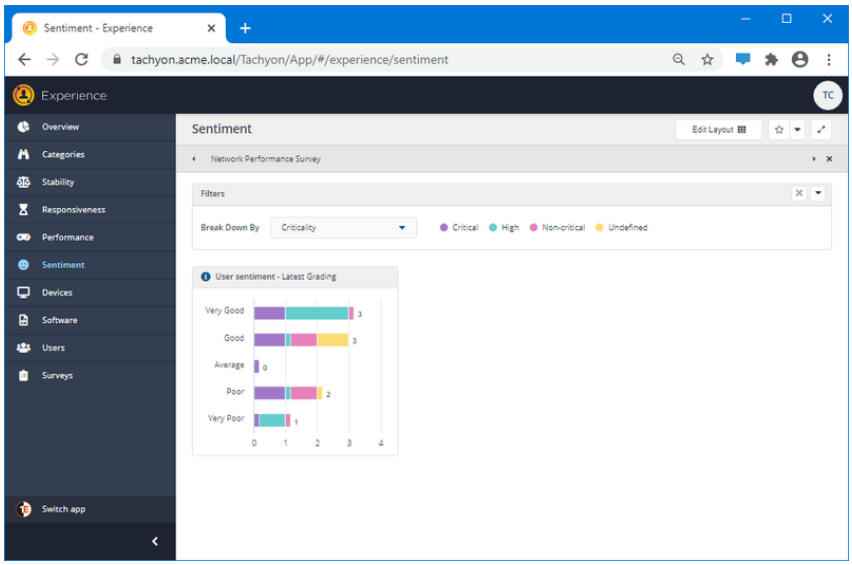


The picture opposite shows how the individual categories for the **User sentiment** break down according to the **Operating System**. The color for each different detected type of OS is displayed in the **Filters** bar and can be used as a key for the information displayed in the chart.

So here you can see that the **Good** grading is broken down into **Windows 10**, **Windows 8.1** and **Windows Server 2016** Operating Systems.



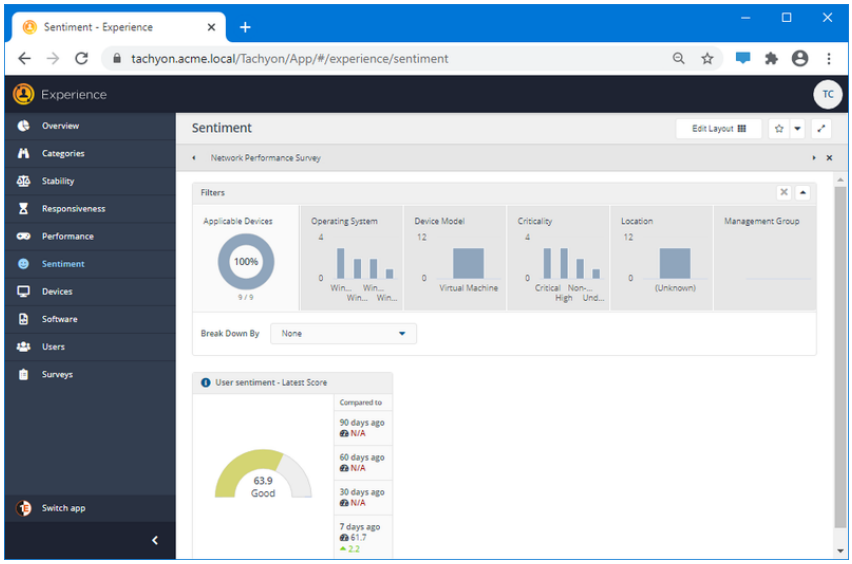
It's easy to change the parameter you break down by to see different aspects of the grading. Here the picture opposite shows the **User sentiment** chart broken down by the **Criticality** set for the devices. Here you can see the **Very Good** grading consists of **Critical** and **High** devices**.**



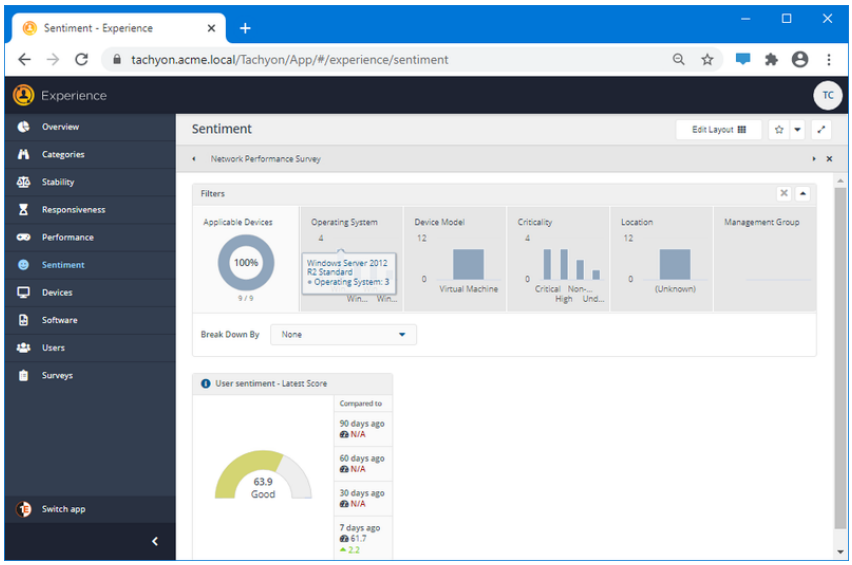
5.5.1.5.3.2 Applying filters with the Filters bar

It is possible to create filters for multiple categories using the Filters bar. The filters are applied as you make selections and additional sections can be selected in order to further refine your dataset. You can also combine filters with the break down, on pages where that option is available. The picture opposite shows the Sentiment page with the **Filters** bar displayed.

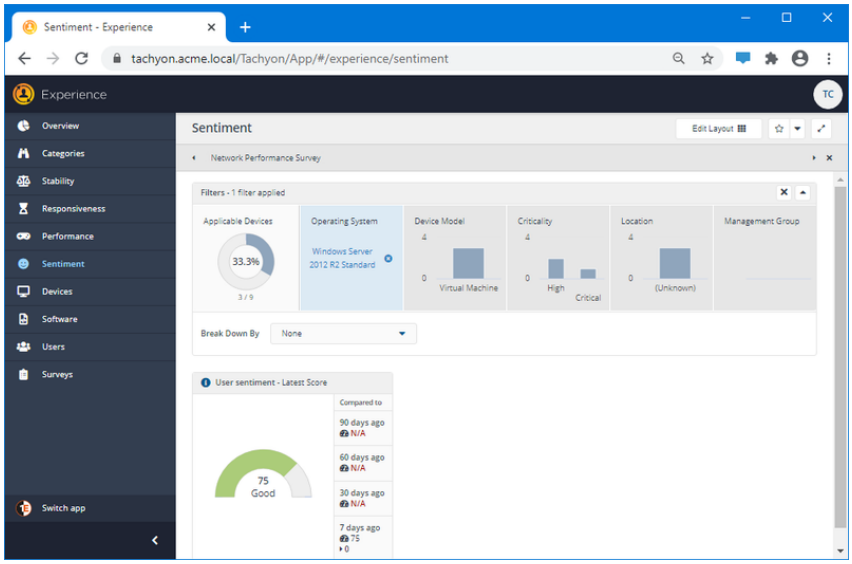
Each section in the bar provides a different way of instantly filtering the data that is displayed on the page and shows the different values available to choose from within that heading. The Operating System section, for example, shows a bar chart with all the different Operating Systems represented in the data being displayed. In the picture opposite this shows four values.



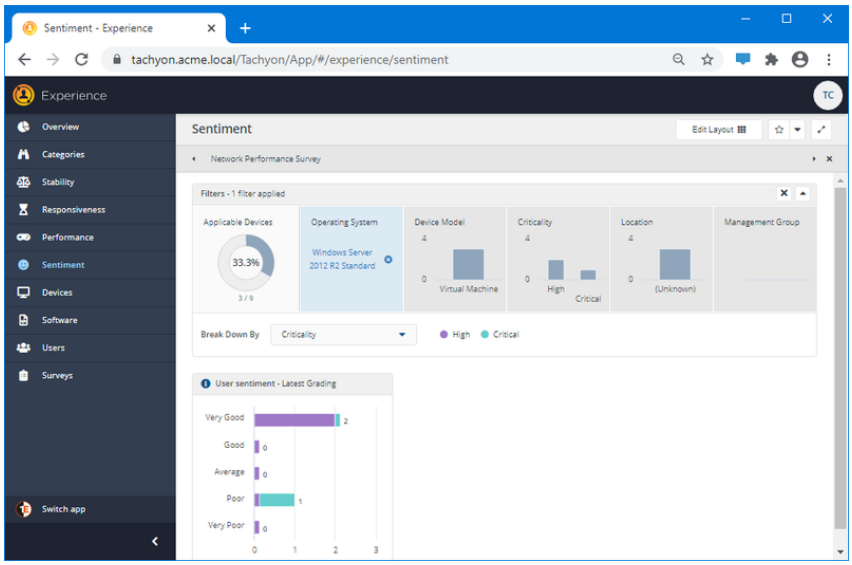
You can see what each of the columns in the bar chart represent by hovering over it with the mouse. In the picture opposite you can see that the first column is for the **Windows Server 2012 R2 Standard** OS and there are **3** instances of that type in the data.



Clicking on a bar filters the data to just show those devices that have that value. For example, the picture opposite shows the result of filtering on the **Windows 2012 R2 Standard** OS. The **Applicable Devices** section of the bar changes to show how much of the overall data is being displayed as a result of filtering, here you can see that the selected OS forms **33.3%** of the overall data. The **User sentiment - Latest Score** chart changes to show the score for just those devices.



You can combine the filter with a break down using the **Break Down By** selector. The picture opposite shows the **Criticality** break down for **Windows Server 2012 R2 Standard** OS across the 5 grades.



5.5.1.6 Tile Buttons

The Stability, Responsiveness, Performance, and User Experience pages all have a set of tiles that allow navigation or a change of view. Each tile has a set of menu buttons in its upper right. The buttons are hidden until you hover over the tile. Hovering over the button itself, brings up the name of the button.

This image shows the buttons exposed. The buttons in order from left to right are:

View Latest Score button

View Latest Grading button

View Trend button

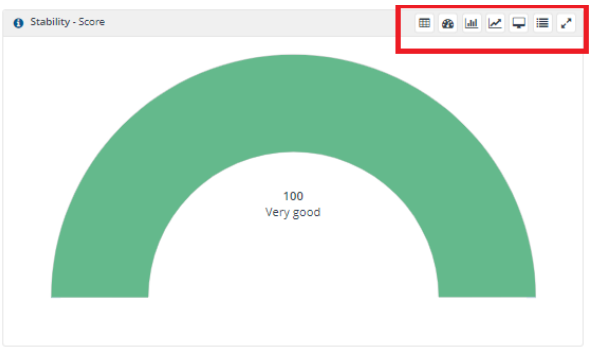
View Poorest Devices button

View What's Changed (last 7 days) button

View Detailed Data button

Expand button

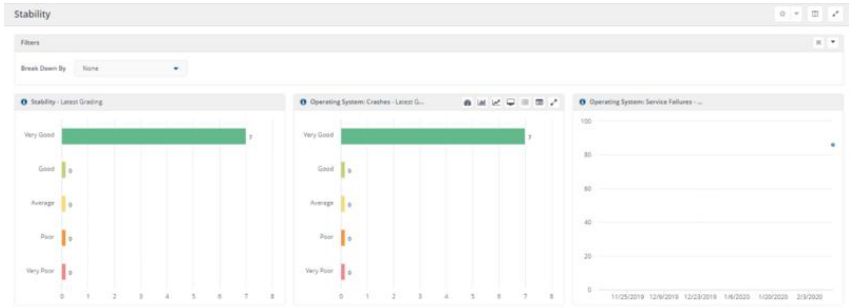
The first three of the buttons change that tile's focus to another view (if you do not have that one currently selected).



5.5.1.6.1 View Latest Score button

View Latest Score button does not do anything if the latest score tile is exposed in the first tile position. If you have changed the tile to View Latest Grading, clicking the first button will change it back to the default View Latest Score.

This image shows an example where the second button on the first tile (View Latest Grading) was selected previously. The first tile now shows the default view of the second tile.



5.5.1.6.2 View Latest Grading button

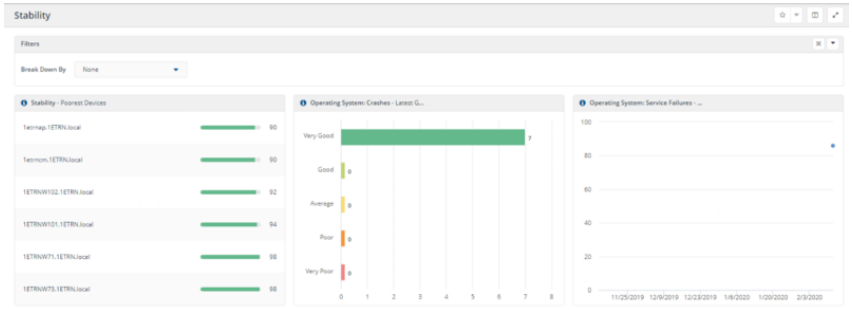
This button will change the view of the current tile to the latest grading tile.

5.5.1.6.3 View Trend button

This button will change the view of the current tile to Trend view.

5.5.1.6.4 View Poorest Devices button

This button will change the current view of the tile to the top 5 poorest devices for that category.

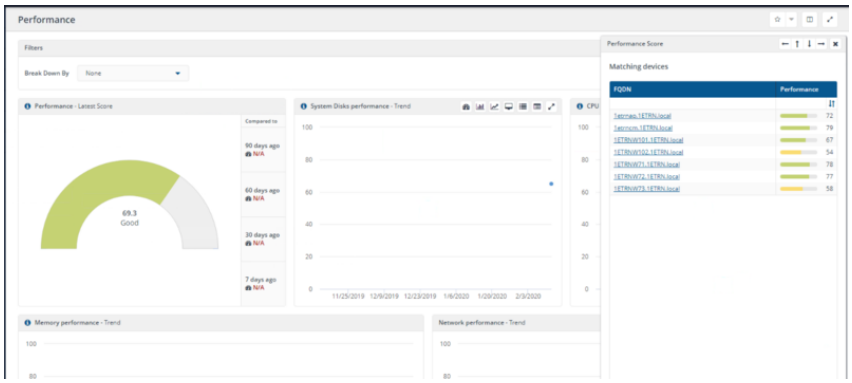


5.5.1.6.5 View What's Changed (last 7 days) button

This button will show what has changed over the last seven days.

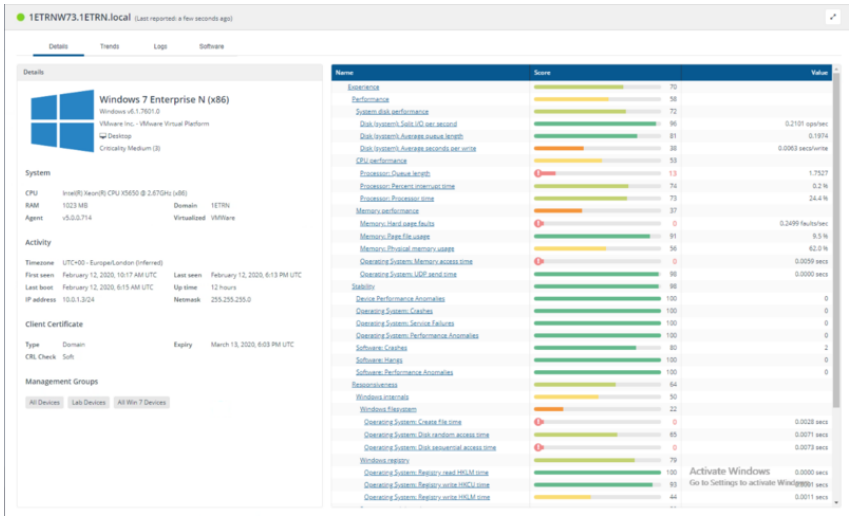
5.5.1.6.6 View Detailed Data button

The View Detailed Data button brings up a list of devices with each device's score for that category. This is the View Detailed Data from the Performance page - Performance Score tile. The colored bars show the grading category for that particular score (Very good, Good, Average, Poor or Very Poor).



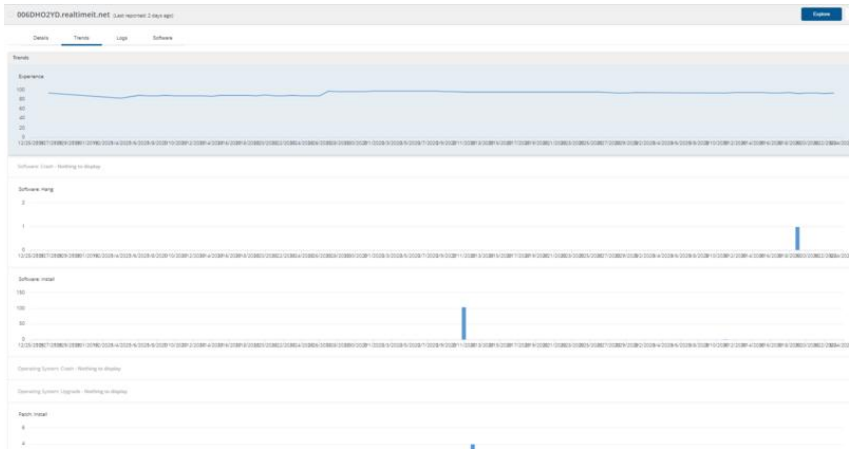
5.5.1.6.6.1 Details tab

Selecting one of the devices opens the Device's raw data. The Details tab shows all the metrics that make up the score for that device. The first line shows the overall Experience score. The subsequent lines shows the metrics under each category (Performance, Stability and Responsiveness).



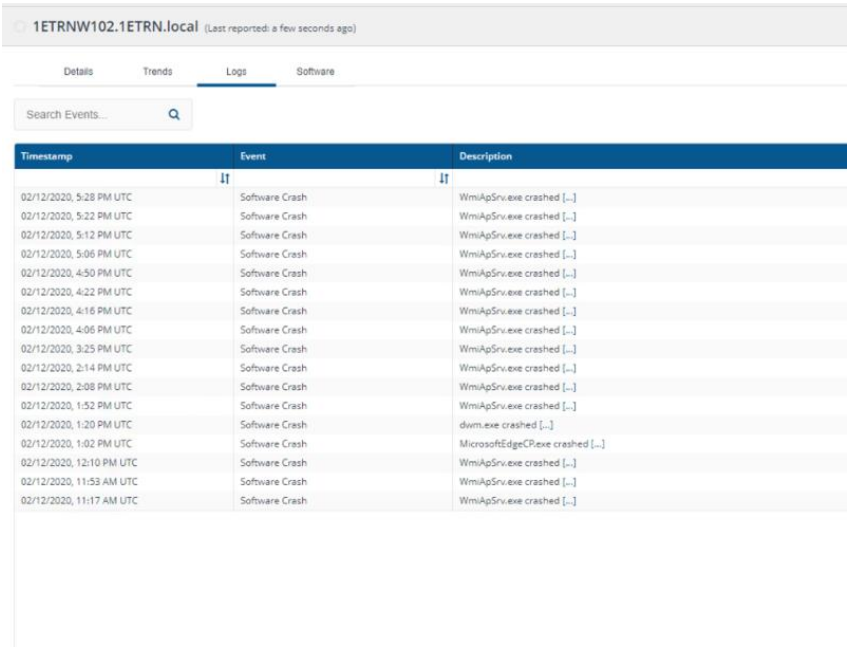
5.5.1.6.6.2 Trends tab

The Trends tab shows the changes in the scores over time. Hovering over any of the bars shows the details for that time and event. If the user viewing the device details also has the ability to at least ask a question in Explorer the Explore button will be visible.



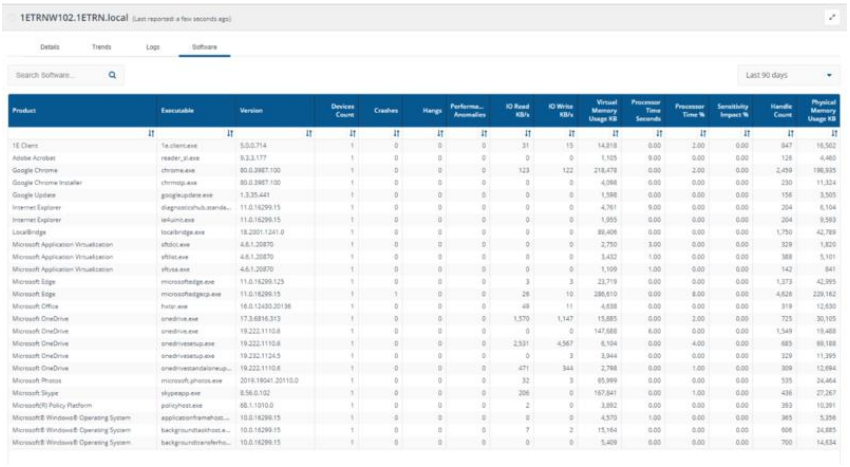
5.5.1.6.6.3 Logs tab

The Event Logs tab gives you a listing of the Windows Event log entries for that device. This brings that data to this view and is very useful when determining the root cause of an issue that has been reported on the device.



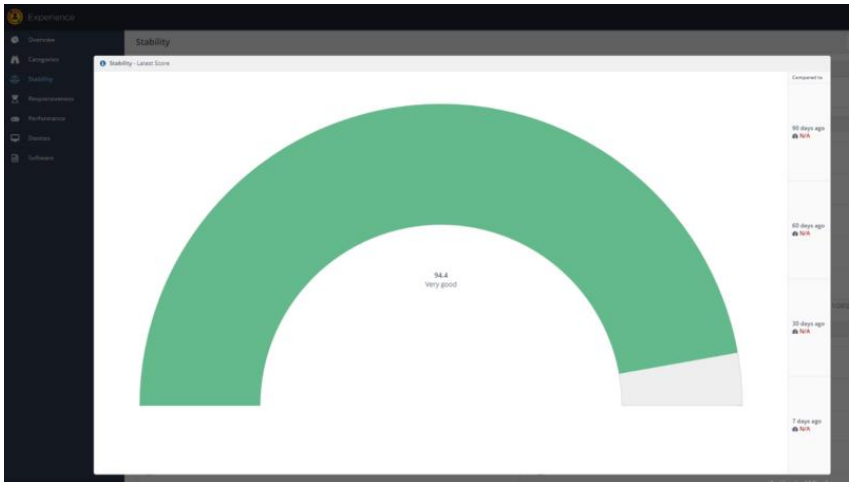
5.5.1.6.6.4 Software tab

The Software tab lists all the software that is installed on the device. This view also shows the metric data for that software. Clicking the ellipsis will show the entire list with the raw scores for each one.



5.5.1.6.7 Expand button

Clicking the Expand button in the far right pops the tile out of the dashboard and enlarges it.



5.5.2 Score reference

This reference provides details on how the scores are collected and calculated.

5.5.2.1 The Scores

5.5.2.1.1 How Experience calculates the scores

The Experience Score is an overall number that represents the user experience of a given device. It is a total of weighted scores in the four categories - Performance, Stability, Responsiveness, and User Sentiment. The total possible score overall or in any given category is 100.The scoring number is assigned a Grade based on the chart below. Grades appear in the user interface as different colors.

This information is provided to give you an understanding of the makeup of the scores.

5.5.2.1.2 Grading

Experience scores are divided into one of five gradings.

Very Good

Good

Average

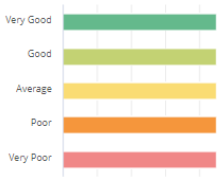
Poor

Very Poor

The ranges for each grading is listed in this table.

Grading	Score range	Bar Color
Very Good	100 - 81	Dark Green

Grading	Score range	Bar Color
Good	80 - 61	Olive Green
Average	60 - 41	Yellow
Poor	40 - 21	Orange
Very Poor	20 - 0	Red (Exclamation Point)



5.5.2.1.3 Categories

Experience uses four categories to calculate the overall Experience Score.

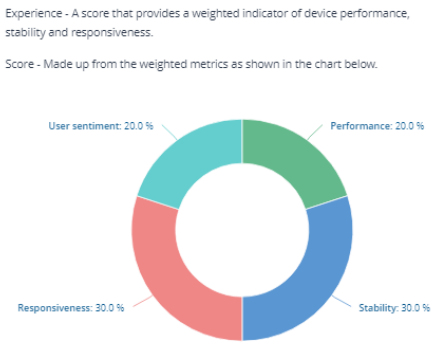
Category	Description
User sentiment	The score for this category is based on the responses to user surveys.
Stability	The score for this category is based on the "crashiness" of the applications and the Operating System that the applications are installed on.
Responsiveness	The score for this category is based on our patented technology that we call "Synthetic Micro-Transactions". We run these periodically on the device and perform different tests to measure the responsiveness of the device. This information cannot be obtained from any other solution.
Performance	The score for this category is based on the typical Windows performance type data - CPU usage, Memory Usage, Processes, etc.

5.5.2.1.4 Experience overall score

The User Experience score provides an indicator of device performance, stability and responsiveness. It is derived from weighted User sentiment, Performance, Stability and Responsiveness scores.

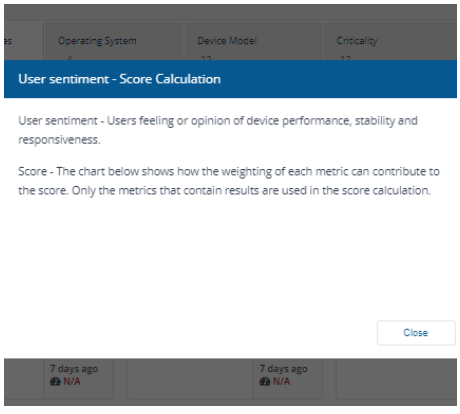
Metric	Description
User sentiment	A measure of end-users feelings about their experience based on user surveys.

Metric	Description
Performance	Hardware utilization
Stability	System stability
Responsiveness	System responsiveness



5.5.2.1.5 User sentiment

The User sentiment score is derived from the responses to user and metric surveys.

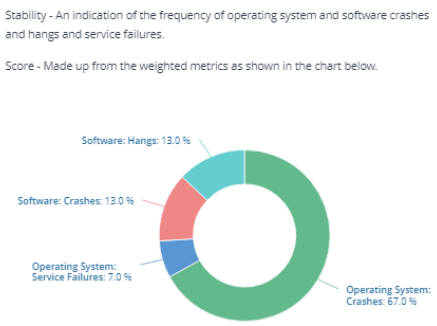


5.5.2.1.6 Stability

The Stability score is derived from four scores based on the number of crashes and hangs for software and for the Operating System itself.

What is measured	Description
Operating System: Crashes	Scores the frequency of operating system crashes (Blue Screens, or unexpected shutdowns). A lower score indicates crash activity, which is likely to be caused by a faulty or misconfigured device drive.

What is measured	Description
Operating System: Service Failures	Scores the frequency of service failures (where a service fails to start or shutdown correctly). A lower score indicates problematic services which may need to be investigated.
Software: Crashes	Scores the frequency of software crashes. A lower score indicates a high rate of crashes. The Devices screen Logs tab can assist with investigation of software crashes.
Software: Hangs	Scores the frequency of software hangs (where an application becomes unresponsive). A lower score indicates a high rate of hangs.



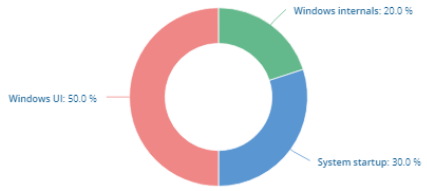
5.5.2.1.7 Responsiveness

The Responsiveness score is derived from the scores of Windows internals, system startup, and Windows UI.

What is measured	Description
Windows Internals	Windows internals provides an indication of the timeliness of Windows System resource creation and availability
System Startup	Derived from Operating System: Boot time
Windows UI	Provides an indication of windows creation and operation

Responsiveness - An indication of the timeliness of operating system startup and system resource creation and availability.

Score - Made up from the weighted metrics as shown in the chart below.



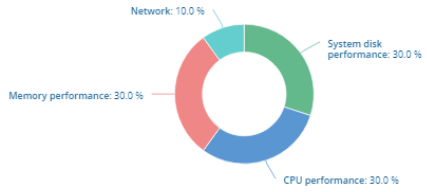
5.5.2.1.8 Performance

The Performance score is derived from the scores of disk performance, CPU performance, and memory performance.

What is measured	Description
System disk performance	System disk performance
CPU performance	CPU performance
Memory performance	Memory performance

Performance - A score that provides a weighted indicator of the load and throughput of processor, memory and disk resources.

Score - Made up from the weighted metrics as shown in the chart below.



5.5.2.1.9 Metrics and algorithms

Metrics are the datasets that are collected by the 1E Client and sent up the Tachyon server daily. Metrics are either Raw or Aggregate. Raw metrics have a scoring algorithm applied to them to derive a score. Operating System: Create file time is a raw value metric. The data will simply be the time it takes to create a file on that device. For example, the actual time it takes to create a file on a specific device is 0.008 seconds. So the value for the metric will be 0.008. Once the algorithm is applied the score will be 58.

An aggregated metric is calculated from other metrics.

An aggregate score will never have an associated value since it was never directly derived from Raw data.

For example, Performance score is calculated by applying weightings to three other scores - System disk performance, CPU performance and Memory performance. The weightings are determined by the impact to end user experience for that item. Things that impact the user greater are weighted higher.

5.5.2.1.10 Normalization algorithms

Tachyon Experience uses the following algorithms to derive a score for that metric.

Scoring Algorithm	Fixed Parameters	Description
SweetSpot	Minimum, maximum and sweet spot	**Sweet Spot Scoring Algorithm** Based on a bell curve. Define a range (minimum and maximum) and a sweet spot within that range. Score is based on the distance from the nearest edge (minimum or maximum) to the sweet spot value. **Example**: SweetSpot(0,100,15) given a value of 30 gives you a score of 83 which is a Good grading
Percentage	value	**Percentage Scoring Algorithm** Expect a value in the range of 0 - 100 and return that same value as the score. Dropping off any decimal points. **Example**: A 9.6 value would give you a score of 9 which is a Very Poor grading
Inverse Algorithm	Inner algorithm	**Inverting Algorithm** The result of this algorithm subtracts 100 from the value dropping any decimals. **Example**: A 9.6 value would give you a score of 91 (100 - 9 = 91) which is a Very Good grading
Constant	constant score	**Constant Scoring Algorithm** No matter the incoming value, return a constant score Example: A value of 42 would give you a score of 42 which is a Poor grading

Scoring Algorithm	Fixed Parameters	Description
Bounded Range	Minimum and maximum	**Bounded Range Scoring Algorithm** Expect a value in the range of (minimum, maximum) and return a score of 0-100 based on the position, dropping any decimals. **Example**: BoundedRange(10,120) given a score of 119 would give you a score of 1 which is a Very Poor grading

5.5.2.1.11 Experience Metrics

The following table outlines the Experience Metrics that are collected and scored for each device and how they are classified:

Experience	a score that provides a weighted indicator of device performance stability and responsiveness.		
Performance	a score that provides a weighted indicator of the load and throughput of processor memory and disc resources.		
	System disc performance	an indicator of system disc load and throughput	
		Disc (system): split I/O per second	scores the I/O operations that were broken into multiple requests on the system disc. A lower score may indicate excessive disc

		fragmentation.
	Disc (system) : average queue length	scores the average queue length for the system disc. A lower score indicates that this disc is not keeping up with the I/O backlog.
	Disc (system): average seconds per write	scores the average time taken for the system disc to perform a right. A lower score indicates that this disc is taking too long to service write requests.
CPU performance	an indication of processor load and throughput.	
	Processor: queue length	scores the CPU Q length (backlog of processing work). A lower score means that the CPU is not keeping up with the workload.

	Processor: percent interrupt time	scores the amount of time the CPU spent servicing interrupts. A lower score may indicate faulty or misconfigured hardware/ drivers.
	Processor: processor time	scores the CPU load. A lower score indicates that the CPU is fully loaded, and additional processing power may be required.
Memory performance	a score that indicates memory load and system paging activity.	
	Memory: hard page faults	Scores the amount of memory pages that had to be read from disc based storage. A lower score indicates this device is low on available physical memory.

Memory: page file usage	Scores the percentage of the page file that is in use. A lower score indicates more high page file use, which may mean the device is low on available physical memory.
Memory: Physical memory usage	Scores the percentage of physical memory in use. A lower score indicates higher memory consumption, and therefore less available physical memory.
Operating System: Memory access ti me	Score the time taken to allocate, zero and free a block of memory. A lower score indicates that the operating system is slow to server

		memory requests, which may affect application performance.
Network	A score that indicates the local network stack performance (not including physical network considerations, such as latency).	
	Operating System: UDP send time	Scores the time taken to perform a basic loopback UDP send. A lower score may indicate problems with the operating system network stack.
	Network: Output queue length	Scores the network transmission backlog based on the length of the output packet queue.
	Network: Wireless signal quality	Scores the signal quality of the wireless network connection

			on the device.
Stability	An indication of the frequency of operating system and software crashes and hangs and service failures.		
		Operating System: Crashes	Scores the frequency of operating system crashes (Blue Screens, or unexpected shutdowns). A lower score indicates crash activity, which is likely to be caused by a faulty or misconfigured device driver.
		Operating System: Service Failures	Scores the frequency of service failures (where a service fails to start or shutdown correctly). A lower score indicates problematic services, which may need to be investigated.

		Software: Crashes	Scores the frequency of software crashes. A lower score indicates a high rate of crashes. The Devices screen Logs tab can assist with investigation of software crashes.
		Software: Hangs	Scores the frequency of software hangs (where an application becomes unresponsive). A lower score indicates a high rate of hangs.
Responsiveness	An indication of the timeliness of operating system startup and system resource creation and availability.		
	Windows internals	An indication of the timeliness of Windows system resource creation and availability.	
	Windows filesystem	A score that indicates file system and disk access speed.	

Operating System: Create file time	Scores the time taken to create an empty, temporary file. A lower score indicates that the operating system may be underperforming in terms of basic file operations.
Operating System: Disk random access time	Scores the time taken to perform a random access disk operation on the system drive. A lower score indicates poor random disk access performance.
Operating System: Disk sequential access time	Scores the time taken to perform a sequential access disk operation on the system drive. A lower score indicates poor sequential

		disk access performance.
Windows registry	An indication of Windows registry access speed.	
	Operating System: Registry read HKLM time	Scores the time taken to read from the HKLM Windows Registry hive. A lower score indicates poor registry read performance, which in turn may affect application performance.
	Operating System: Registry write HKCU time	Scores the time taken to write to the HKCU Windows Registry hive. A lower score indicates poor registry write performance, which in turn may affect application performance.
	Operating System: Registry write HKLM time	Scores the time taken to write to the HKLM Windows Registry hive.

		A lower score indicates poor registry write performance, which in turn may affect application performance.
Processes and threads	A score that indicates Windows process and thread creation and startup speed.	
	Operating System: Create process time	Scores the time taken to create a new process. A lower score indicates that the operating system is taking a long time to create new processes.
	Operating System: Create thread time	Scores the time taken to create a new thread within a process. A lower score indicates that the operating system is taking a long time to create new threads.
	Operating System: OpenHandle time	Scores the time taken to acquire a

		basic operating system resource. A lower score indicates that applications may underperform because the operating system is slow to service resource requests.
	Operating System: Load DLL time	Scores the time taken to load and unload a DLL in a process. A lower score indicates library loading is slow, which may affect the startup time of applications.
System startup	An indication of the timeliness of operating system startup.	
	Operating System: Boot time	Scores the time taken for the device to boot to the logon prompt. A lower score indicates a long boot up

		duration, which may affect user satisfaction.
Windows UI	An indication of graphical window creation and operation speed.	
	Operating System: Create window time	Scores the time taken to generate an empty window. A lower score indicates poor Windows desktop performance, which may cause applications to appear unresponsive.
	Operating System: Message dispatch time	Scores the time taken to dispatch and confirm processing of a windows message. A lower score indicates poor message processing throughput, which may affect application

			responsiveness.
User sentiment	Users feeling or opinion of device performance, stability and responsiveness.		
	User Sentiment Survey metrics	These have been added by an Experience Survey administrator. The information shows the text of the question related to the survey metric.	

5.5.2.2 Metrics Collection Details

5.5.2.2.1 Metrics

Metrics are the data points that are collected by the 1E Client and sent to the Tachyon server. They are collected at different intervals depending on the type of data that is being collected.For example, CPU usage might be collected each hour but crash information is collected at the time of the crash. If the 1E Client cannot connect to the Tachyon switch, the client still collects the data but will hold the information until the next time the switch can be contacted. The 1E Client will send all the collected data at that time.

5.5.2.2.2

5.5.2.2.3 Data Collection Intervals

Some metrics for Experience are collected as daily summaries. These are sent to the Tachyon Switch each night at midnight. If the 1E Client cannot contact the server at midnight the daily digest data is saved at the device and is sent to the server the next time the server can be contacted. In this version, there is not the ability to force the 1E Client to send the information outside of the nightly cycle.

The data that is collected in the daily digest is:

Device resource usage

Device Performance, responsiveness and stability data

Software stability and resource usage

The Stability Data is reported in real-time to the Tachyon Switch. These include:

Software installs/uninstalls

Patch installs/uninstalls

Operating System reboots

Application crashes

Application hangs

Operating System crashes

Windows service failures

5.5.3 Experience Product Packs reference

Reference information for **Experience** feature-related Product Packs that are included in the **Tachyon Platform** zip. These Product Packs are required to support various features of **Experience.**

The **Tachyon Platform** zip is downloaded from the 1E Support Portal (1eportal.force.com/s/tachyontopicdetail). Additional Product Packs are available from Tachyon Exchange (tachyonexchange.1e.com) that are not documented here.

Classic Product Packs contain instructions, for use in Explorer and other Tachyon applications.

Integrated Product Packs contain policies, rules and fragments for use by Guaranteed State, and may also include instructions.

5.5.3.1 Instructions

This product pack contains Server instructions.

Server instructions are special type of instruction, which cannot be run in Explorer. They are for internal use only, run on the server, and used to carry out on-demand or scheduled processing of data across various datasources, such as SQL databases. For example, the Dashboards app uses them to populate tiles and charts with data from Tachyon Master and Experience databases.

5.5.4 Glossary

A glossary of Tachyon Experience terminology.

5.5.4.1 Experience alphabetical glossary

Term	Definition

Algorithms

Tachyon Experience uses the following algorithms to derive a score for that metric.

Scoring Algorithm	Fixed Parameters	Description
SweetSpot	Minimum, maximum and sweet spot	**Sweet Spot Scoring Algorithm** Based on a bell curve. Define a range (minimum and maximum) and a sweet spot within that range.

Term	Definition		
			Score is based on the distance from the nearest edge (minimum or maximum) to the sweet spot value. **Example**: SweetSpot(0,100,15) given a value of 30 gives you a score of 83 which is a Good grading
	Percentage	value	**Percentage Scoring Algorithm** Expect a value in the range of 0 - 100 and return that same value as the score. Dropping off any decimal points. **Example**: A 9.6 value would give you a score of 9 which is a Very Poor grading
	Inverse Algorithm	Inner algorithm	**Inverting Algorithm** The result of this algorithm subtracts 100 from the value dropping any decimals. **Example**: A 9.6 value would give you a score of 91 (100 - 9 = 91) which is a Very Good grading
	Constant	constant score	**Constant Scoring Algorithm** No matter the incoming value, return a constant score Example: A value of 42 would give you a score of 42 which is a Poor grading
	Bounded Range	Minimum and maximum	**Bounded Range Scoring Algorithm** Expect a value in the range of (minimum, maximum) and return a score of 0-100 based on the position, dropping any decimals. **Example**: BoundedRange(10,120) given a score of 119 would give you a score of 1 which is a Very Poor grading

Term	Definition
Categories	Experience uses four categories to calculate the overall Experience Score.

Category	Description
User sentiment	The score for this category is based on the responses to user surveys.
Stability	The score for this category is based on the "crashiness" of the applications and the Operating System that the applications are installed on.
Responsiveness	The score for this category is based on our patented technology that we call "Synthetic Micro-Transactions". We run these periodically on the device and perform different tests to measure the responsiveness of the device. This information cannot be obtained from any other solution.
Performance	The score for this category is based on the typical Windows performance type data - CPU usage, Memory Usage, Processes, etc.

Categories page

The Categories page shows a dashboard of the scores from each of the four categories:

Stability

Responsiveness

Performance

Sentiment

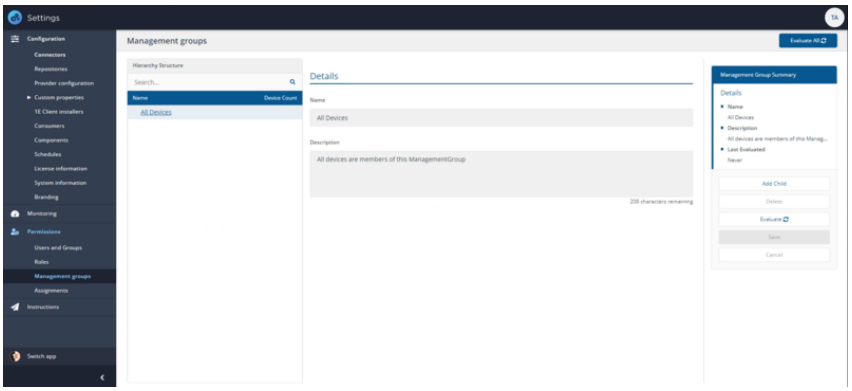
Daily Digest

Some metrics for Experience are collected as daily summaries. These are sent to the Tachyon Switch each night at midnight. If the 1E Client cannot contact the server at midnight the daily digest data is saved at the device and is sent to the server the next time the server can be contacted. In this version, there is not the ability to force the 1E Client to send the information outside of the nightly cycle.

The data that is collected in the daily digest is:

Device resource usage

Term	Definition
	Device Performance, responsiveness and stability data Software stability and resource usage
Device Criticality	**Using Device Criticality** Assigning Criticality to devices according to their importance within your organization.
Devices page	The **Devices** page provides a list of all devices visible to Tachyon Experience. You can see all of their **Experience**, **Stability**, **Performance** and **Responsiveness** statistics and sort them accordingly.
Experience Score	The Experience Score is an overall number that represents the user experience of a given device. It is a total of weighted scores in the four categories - Performance, Stability, Responsiveness, and User Sentiment. The total possible score overall or in any given category is 100.
Filters bar	The **Filters** bar appears at the top of most of the pages in Experience. Each section in the **Filters** bar allows a user to quickly and easily filter based on different categories. When a filter is set it applies to all the tiles on the page. On the Stability, Responsiveness, Performance and Sentiment pages there is also a **Break Down By** selector that reconfigures the charts to show the data divided up into the selected category. On the **Overview**, **Categories**, **Devices**, and **Software** pages there is no option for **Break Down By**. On the **Users** and **Surveys** pages the **Filters** bar is not available.
Grading	Experience scores are divided into one of five gradings. Very Good Good Average Poor Very Poor

Term	Definition
Location	Tachyon Explorer allows you to use Location when defining coverage for an instruction. For example, you can choose to target an instruction to be sent only to devices whose location has been set.
Metrics	Metrics are the datasets that are collected by the 1E Client and sent up the Tachyon server daily. Metrics are either Raw or Aggregate. Raw metrics have a scoring algorithm applied to them to derive a score.
Management Groups	**Management Groups page** Management Groups are containers used to group devices and the software installed on those devices. Management Groups are defined using configurable rules that look at various properties of the devices and their installed software, these are then evaluated to determine the group membership. This means that Management Group membership adapts to changes to the devices and software in your environment. 
Overview page	The **Overview** page is the starting place for any Tachyon Experience journey. Here you can get immediate answers to how your enterprise is performing from an end-user perspective and you can drill-down to get details on specific problem areas and find routes to immediate resolutions. Your key indicator is the **Experience - Latest Score** chart, which gives your enterprise a score out of 100 based on a combination of measured events and user surveys. The closer you are to 100 the better the IT experience your end-users are having. The **Experience - Latest Grading** chart provides a breakdown of the experience score showing how many devices and users fall into each of the five experience grades - ranging from **Very Good** to **Very Poor**. This helps

Term	Definition
	interpret the experience score and see how it maps onto end-user experiences. The **Experience - What's Changed (last 7 days)** chart provides an overview of the significant changes, good or bad, that have occurred during the past week. Finally you can use the **Experience - Trend** chart to check how well your enterprise is performing over time in terms of how your end-users see it. You could use this chart to help gauge progress on any improvement programs you might have put in place or act as an advanced warning that there are underlying issues that are affecting your end-users and need resolving.
Performance page	The performance score is derived by measuring the performance of the device using the Windows Performance Counters. These counters measure many data points on the device including CPU usage, disk usage, memory usage, and processes. The page allows you to drill into the Latest Score tile to see the different metrics that are collected. For information on the makeup of the score see Performance Score
Performance Score	The Performance score is derived from the scores of disk performance, CPU performance, and memory performance.
Responsiveness page	The responsiveness score is derived by measuring how well Windows application perform during our "Synthetic micro-transactions". The successful and timely operation of Windows and Windows applications is key to a positive user experience on that device. The page allows you to drill into the Latest Score tile to see the different metrics that are collected. For information on the makeup of the score see Responsiveness Score
Responsiveness Score	The Responsiveness score is derived from the scores of Windows internals, system startup, and Windows UI.
Scores	The Experience Score is an overall number that represents the user experience of a given device. It is a total of weighted scores in the four categories - Performance, Stability, Responsiveness, and User Sentiment. The total possible score overall or in any given category is 100.

Term	Definition
Software page	The Software page provides a tabular listing of all the Software products that are installed in the environment (including executable, version, architecture). The second set of columns in the list provide additional metrics or event details associated with the Software products.
Stability page	The stability score is derived by measuring the "crashiness" of applications and the operating system of a device. The different types of crashes have a differing impact on the score, based on the amount of impact on the end-user. An application crash is annoying but the crash of the entire operating system could cause data loss so has more weight on the score. The page allows you to drill into the tiles to see the different metrics that are collected. For information on the makeup of the score see Stability Score
Stability Score	The Stability score is derived from four scores based on the number of crashes and hangs for software and for the Operating System itself.
Tile buttons	The Stability, Responsiveness, Performance, and User Experience pages all have a set of tiles that allow navigation or a change of view.

5.5.5 Tachyon Experience release information

5.5.5.1 Tachyon Experience 8.1 Release Notes – last updated 02-August-2022

These notes contain late-breaking information about Tachyon Experience that you need to have to successfully install and use the product. For the most up-to-date information, please see the online readme. You should read these release notes and the online documentation for Tachyon thoroughly before installing the software.

5.5.5.2 New features in Tachyon Experience 8.1

No longer requires SQL Server Analysis Server (SSAS)

On the Software page, the **Product**, **Executable**, **Version** and **Architecture** columns have been removed from the table that is displayed after clicking on a particular row. This is because the subsequent table is filtered on the selected Product, Executable, Version and Architecture values and will be the same for every row in the table. The values are displayed anyway in the heading for the page, and the columns can be added back from the Column picker if needed

User Sentiment descriptions now highlight that User Sentiment is processed once a day, rather than real-time.

5.5.5.2.1 Online help

Tachyon comes with online help that shows you how to install, configure and use the product. Click the following link to view the help:

Tachyon platform.

For support queries, please:

Use https://support.1e.com/ where you can search the KB or submit a support case.

Contact support@1e.com.

5.5.5.2.2 Known issues

The current known issues related to the installation and running of Tachyon can be found in the Troubleshooting Known issues page of the Tachyon documentation.

5.5.5.3 Tachyon Experience Release History

5.5.5.3.1 Web Release - 8.1 (31 Mar 2022)

No longer requires SQL Server Analysis Server (SSAS)

On the Software page, the **Product**, **Executable**, **Version** and **Architecture** columns have been removed from the table that is displayed after clicking on a particular row. This is because the subsequent table is filtered on the selected Product, Executable, Version and Architecture values and will be the same for every row in the table. The values are displayed anyway in the heading for the page, and the columnscan be added back from the Column picker if needed

User Sentiment descriptions now highlight that User Sentiment is processed once a day, rather than real-time.

5.5.5.3.2 Web Release -8.0 (03 Nov 2021)

Works with Tachyon Platform 8.0

The user interface has been re-organized and provides several new pages and popups:

Experience Analytics:

The existing Overview, Categories, Stability, Responsiveness, Performance and Sentiment pages are now re-organized under Experience Analytics.

Advanced Analytics:

Network: includes scored and raw metrics for Bytes Sent/Received per Second, Outbound Packets Discarded, Packet Outbound Errors, Active TCP Connections, Network Retransmit Rates, Network Usage Overall, Network Bandwidth Utilization, Wireless Send and Receive Rate, Wireless Transmit Rate. Please refer to Investigating Network Performance for more information on how to use this feature

Boot and Login: includes scored and raw metrics for Policy Processing, Startup Apps Processing Time, Main Path Boot Time, Post Boot Time. Please refer to Investigating Boot and Login Performance for more information on how to use this feature.

Inventory Management:

Devices page - displays device-centric metrics including details such as network configuration (IP, Gateway, Connection Type, OS Install Date)

Software page - displays software products with the software associated metrics and inventory details

Users page - displays information on the users known to Tachyon via the 1E Client.

User Engagements. The existing Surveys feature has been renamed and re-organized under User Engagements and extended

Announcement Feature: Engage users via announcements and urgent announcements/notifications. Please refer to Broadcasting information via Announcements for more information.

User Sentiment Surveys are now called **Sentiment Surveys**. Please refer to Getting feedback via Sentiment Surveys for more information.

General Purpose Surveys are now called **Info Surveys**. Please refer to Getting feedback via Info Surveys for more information.

Root Cause Analysis tools - two new popups have been added to the Devices page:

Device comparison: highlights the differences between two selected devices related to Operating System Details, Hardware Details, Usage Details, Installed Software, Services and Processes

Scatter chart: Quadrant placement of devices, plots devices on a chart with customizable X and Y axes (align on the grid based on metrics, scores etc.)

A variety of data types are now available to add as columns in the table views:

Score - values that have been processed and normalized by Experience, this may include consolidation and combinations of other data

Raw - the unprocessed and un-normalized values retrieved from devices

Device Details - information related to devices, such as: IP Address, DHCP Server, Operating System etc.

Software Details - information related to software, such as: the Architecture supported by the software

Event - event information retrieved from devices, such as: Software uninstall, hang and crash events; Operating System boot and crash events, and many others

Network related scores have been added to enhance the overall user experience score:

Output queue length - scores the network transmission backlog, based on the length of the output packet queue

Wireless Signal Quality - scores the signal quality of the wireless network connection on the device.

5.5.5.3.3 Web Release -1.3 (03-Mar-2021)

Works with Tachyon Platform 5.2

Deploy button on Surveys page now only deploys Experience policies

Devices page links through to Device View

1E Experience product pack to support Experience features of the Device View

Users page "User session reactiveness" column has been renamed to "Application responsiveness"

5.5.5.3.4 Web Release -1.2 (03-Sep-2020)

Experience score enhanced to include User Sentiment

End-User Surveys - two types of survey are supported: User Sentiment and General Purpose

A Users page provides information about end-users on the devices in your network

Customizable pages.

5.5.5.3.5 Web Release -1.0 (24-JUN-2019)

Experience score is based on metrics that cover three categories: Stability, Responsiveness and Performance

View experience trends over time

Interactive Overview, Categories, Performance, Stability and Responsiveness experience pages

Investigate devices with Explorer

Filter pages

5.5.5.4 Tachyon Experience features by release

A list of the Tachyon Experience features organized by the release they were implemented in. Links through to the features have been provided for convenience.

5.5.5.4.1 New features in Tachyon Experience 8.1

No longer requires SQL Server Analysis Server (SSAS)

On the Software page, the **Product**, **Executable**, **Version** and **Architecture** columns have been removed from the table that is displayed after clicking on a particular row. This is because the subsequent table is filtered on the selected Product, Executable, Version and Architecture values and will be the same for every row in the table. The values are displayed anyway in the heading for the page, and the columns can be added back from the Column picker if needed

User Sentiment descriptions now highlight that User Sentiment is processed once a day, rather than real-time.

5.5.5.4.2 Tachyon Experience 8.0

Works with Tachyon Platform 8.0

The user interface has been re-organized and provides several new pages and popups:

Experience Analytics:

The existing Overview, Categories, Stability, Responsiveness, Performance and Sentiment pages are now re-organized under Experience Analytics.

Advanced Analytics:

Network: includes scored and raw metrics for Bytes Sent/Received per Second, Outbound Packets Discarded, Packet Outbound Errors, Active TCP Connections, Network Retransmit Rates, Network Usage Overall, Network Bandwidth Utilization, Wireless Send and Receive Rate, Wireless Transmit Rate. Please refer to Investigating Network Performance for more information on how to use this feature

Boot and Login: includes scored and raw metrics for Policy Processing, Startup Apps Processing Time, Main Path Boot Time, Post Boot Time. Please refer to Investigating Boot and Login Performance for more information on how to use this feature.

Inventory Management:

Devices page - displays device-centric metrics including details such as network configuration (IP, Gateway, Connection Type, OS Install Date)

Software page - displays software products with the software associated metrics and inventory details

Users page - displays information on the users known to Tachyon via the 1E Client.

User Engagements. The existing Surveys feature has been renamed and re-organized under User Engagements and extended

Announcement Feature: Engage users via announcements and urgent announcements/notifications. Please refer to Broadcasting information via Announcements for more information.

User Sentiment Surveys are now called **Sentiment Surveys**. Please refer to Getting feedback via Sentiment Surveys for more information.

General Purpose Surveys are now called **Info Surveys**. Please refer to Getting feedback via Info Surveys for more information.

Root Cause Analysis tools - two new popups have been added to the Devices page:

Device comparison: highlights the differences between two selected devices related to Operating System Details, Hardware Details, Usage Details, Installed Software, Services and Processes

Scatter chart: Quadrant placement of devices, plots devices on a chart with customizable X and Y axes (align on the grid based on metrics, scores etc.)

A variety of data types are now available to add as columns in the table views:

Score - values that have been processed and normalized by Experience, this may include consolidation and combinations of other data

Raw - the unprocessed and un-normalized values retrieved from devices

Device Details - information related to devices, such as: IP Address, DHCP Server, Operating System etc.

Software Details - information related to software, such as: the Architecture supported by the software

Event - event information retrieved from devices, such as: Software uninstall, hang and crash events; Operating System boot and crash events, and many others

Network related scores have been added to enhance the overall user experience score:

Output queue length - scores the network transmission backlog, based on the length of the output packet queue

Wireless Signal Quality - scores the signal quality of the wireless network connection on the device.

5.5.5.4.3 Tachyon Experience 1.3

Works with Tachyon Platform 5.2

Deploy button on User Engagement page now only deploys Experience policies

Devices page links through to Device View

1E Experience product pack to support Experience features of the Device View

Users page "User session reactiveness" column has been renamed to "Application responsiveness"

5.5.5.4.4 Tachyon Experience 1.2

Works with Tachyon 5.1

The Tachyon Experience score has been greatly enhanced to include User Sentiment - this means that, not only can you monitor the stability, responsiveness, and performance of the devices on your network to deduce your end-users satisfaction with their IT services, you can send out surveys and incorporate your end-users actual feedback directly into the picture. For more information on this subject please refer to Getting feedback via Sentiment Surveys, where you can find a complete end-to-end use case on creating, deploying, responding and processing responses to User Sentiment Surveys.

The Tachyon Experience score displayed on the Overview page includes user sentiment values, please refer to The Scores for more information.

The Categories page includes a Sentiment tile showing the current User Sentiment score.

The Sentiment page lets you view the User Sentiment score on its own and drill down to view users and monitor their feedback and pain points.

End-User Surveys - two types of survey are supported: User Sentiment and General Purpose. User Sentiment Surveys contribute towards the Tachyon Experience score, General Purpose Surveys can be used to ask one-off questions of your end-users and get their feedback on any issue. The User Engagement page is where you can create, enable and deploy surveys.

A Users page is provided that lets you get information on the end-users on the devices in your network. Please refer to the Users page for more details.

Customize the Tachyon Experience pages to view the interactive charts you want to focus on - including the display of the results from your User Sentiment surveys on the Sentiment page.

5.5.5.4.5 Tachyon Experience 1.0

Works with Tachyon Platform 5.0

Tachyon Experience score - lets you monitor the performance, stability and responsiveness of the devices on your network to deduce your end-users' satisfaction with their IT services. The experience score is based on metrics that cover three categories:

Stability - derived from the frequency of operating system and software crashes, hangs and service failures

Responsiveness - based on the speed of operating system startup, system resource creation and availability

Performance - a weighted indication of load and throughput for device processor, memory and disk resources.

View experience trends over time - Tachyon Experience not only captures data on how your network devices' experience is at the moment, it also lets you view trends in how the experience score is changing over time.

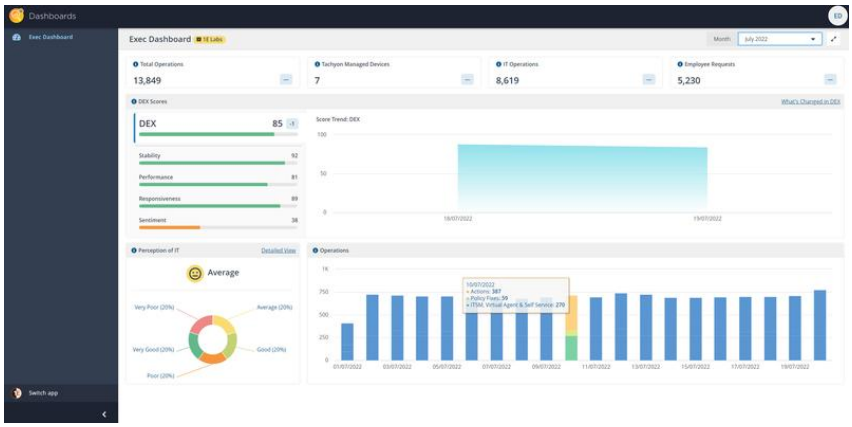
Interactive Overview, Categories, Performance, Stability and Responsiveness experience pages - let you drill down into the details of the experience scores to view the details for the performance, stability, responsiveness and associated metrics for your network.

Investigate devices with Explorer - after drilling down to identify experience issues with the devices in your network, you can make a selection and use that to prime Explorer to run instructions in real-time on just those selected devices.

Filter pages, so the interactive charts display just the data you want them to.

6 Tachyon Dashboards

Over time, Tachyon Dashboards will introduce a number of overview dashboards that give top-level information on the performance of an organization regarding various aspects of their business as measured by Tachyon applications.



6.1 Introducing Tachyon Dashboards

It's important to measure or evaluate the way that your organization is performing in terms of your employee Digital EXperience (DEX). This measure lets you know how good your employee day-to-day experience is of your company's IT systems, how happy they are working in your company, and how likely they are to stay with you.

In many organizations, the ability to gain insight into your DEX KPIs involves gathering data from multiple applications and departments, then analyzing and correlating it to determine if the user experience and sentiment are trending up or down. A bigger challenge is understanding if the tools and processes you have in place are improving end-user productivity.

Over time, Tachyon Dashboards will introduce a number of overview dashboards into the that give top-level information on the performance of an organization regarding various aspects of their business as measured by Tachyon.

The new Exec Dashboard is the first such dashboard. It solves this challenge by presenting your DEX score and key metrics on a single pane of glass in an easily consumable format. It also provides data on the adoption and usage of the various platform components, so you can quickly see how it is benefiting both end-user productivity and issue resolution. When combined with a measure of employee perception of your IT department - via Sentiment surveys, you are able to quickly see trends impacting DEX across your organization.

The Exec Dashboard displays insights into the following areas:

Coverage – Volumetric Data (how much is being managed/covered by Tachyon)

Experience Insights – Actual Values and Trends that influence your DEX score, including employee perception of IT.

This release of Tachyon Dashboards is a 1E Labs release, and introduces the following new features:

6.1.1 Exec Dashboard

Exec Dashboard is an overview page in the Tachyon portal, mainly aimed at CIO executives, showing the benefits that Tachyon provides and highlighting how the company has been performing in terms of DEX over the past few months.

The CIO wants to ensure that their IT department is supporting the business goals of the company. Using the information displayed in the Exec Dashboard, the Exec DashboardCIO delegates tasks to IT managers in order to focus on high-level IT strategy and growth. The provides a focused set of charts that give them the big picture without overwhelming detail, so they can initiate the right conversations with their IT team. The Exec Dashboard shows the following information:

Summary tiles, each tile displays a number that indicates:

Total Operations - the total number of issues that were resolved during the selected calendar month by: manual actions, automated policy fixes (resolved using Guaranteed State policies), ITSM actions (service desk tickets), actions (requested using the Virtual Assistant chatbot), and other self-service requests made by end-users

Tachyon Managed Devices - the number of devices where the installed 1E Client has contacted Tachyon platform during the selected calendar month

IT Operations - the number of issues resolved by manual actions and automated policy fixes (resolved via Guaranteed State Policies)

Employee Requests - the number of issues resolved by ITSM actions, Virtual Assistant actions, and other self-service requests made by end-users.

DEX Scores - you can use this as an indicator of how well your IT systems are working for your end-users.

A summary chart showing the Experience related overall DEX score and individual Stability, Performance, Responsiveness, and Sentiment scores during the selected calendar month.

Score Trend: DEX - A chart plotting the overall daily DEX scores during the selected calendar month.

The CIO can also select to view details on **What's Changed in DEX**. This displays a drawer showing the top 10 largest deltas, up or down, for Experience metrics that have changed during the selected calendar month.

Perception of IT - a tile that shows the feedback given by end-users about their experience of IT services. It consists of averaged responses to the **Perception Of IT** sentiment survey

Displayed at the top of the tile, the total average of all the responses during the selected calendar month as it falls into one of the Very Good, Good, Average, Poor and Very Poor response ranges.

Displayed beneath that, a donut chart showing the average scores per user - according to which of the five response ranges each user's average falls within - plotted as a percentage of the total number of users that responded.

The CIO can also select to view details on the survey responses by clicking on the **Detailed View** link.

Operations - a bar chart showing, for each day in the selected calendar month, three bars that represent: the Actions, Policy Fixes, and ITSM, Virtual Assistant & Self-service operations that took place on that day.

6.2 Implementing Tachyon Dashboards

Everything you need to know about getting Tachyon Dashboards installed and running in your environment.

6.2.1 Requirements

Information that will help you design and plan the implementation in your organization. This includes all the prerequisites and dependencies, which are necessary to get access to Dashboards.

6.2.1.1 License

To use Dashboards, you must have a suitable license included as a consumer in your platform license, which you can obtain from your 1E Account Team. You do not need the license to install the app, but you do need the license to see the app in the Tachyon portal and in the Switch app menu.

6.2.1.2 Hotfix Bundle installer account permissions

To install the Hotfix Bundle that contains Dashboards, you should use the same installation account used for the Tachyon platform.

For more information, please refer to Server installation account.

6.2.1.3 1E companion products

Dashboards currently provides a single **Exec Dashboard** page.

6.2.1.3.1 Exec Dashboard

The table below lists the tiles and charts provided by **Exec Dashboard** indicating which 1E products and apps they each depend on. If any of these products or apps are not installed or available, then the dashboard tile will show a zero, or no data, or not be included in a summed number.

Tile, chart or detail	Source
Total Operations	The sum of IT Operations and Employee Requests for the selected month. That is, the number of issues fixed either manually, by automation, ITSM actions, Virtual Agent actions, and Self Service actions.
Tachyon Managed Devices	The number of devices managed by Tachyon. These are the devices where the installed 1E Client has contacted Tachyon. The number on the dashboard is cached, but the cache is updated in real-time. It increases when new clients come online, and decreases when inactive clients are purged from the Tachyon Master database.
IT Operations	The number of issues fixed, either manually or by automation, and is the sum of the following: **Actions** are issues identified and resolved manually or scheduled. These are action instructions that have been run through Explorer, or any other app, but exclude actions run by ServiceNow ITSM and Virtual Assistant, and 1E Shopping. **Policy Fixes** are issues resolved automatically by **Guaranteed State** policies
Employee Requests	The number of issues fixed by ITSM, Virtual Agent, and Self Service. These are sum of actions instructions that have been run by ServiceNow and/or Shopping. **ITSM actions** are action instructions run by the 1E ServiceNow app **1E ITSM Connect** **Virtual Agent actions** are action instructions run by chatbots, for example the 1E ServiceNow app **1E Virtual Assistant** **Self Service actions** are self-service requests made by end-users of: **1E Shopping**, where a requested item causes an action instruction to be run on the end-user's device **1E Service Catalog Connect**, where a service request is submitted that causes an action instruction to be run. The current version of Exec Dashboard does not differentiate between actions run by the three ServiceNow apps (ITSM Connect, Virtual Agent and Service Catalog Connect) because they all use the same ServiceNow consumer. For more information about ingrating these self-service

Tile, chart or detail	Source
	products with Tachyon, please refer to: Shopping 6.1 - Enabling Tachyon integration and 1E Service Catalog Connect 2.0.
DEX Scores	The DEX score in Exec Dashboard is a combination of these Stability, Performance, Responsiveness, and Sentiment scores, obtained from **1E Experience**. The Score Trend chart shows data for selected score over the selected month. The above scores are a weighted combination of Experience metrics. The What's Changed popup shows the top and bottom 5 metrics that most significantly affected the selected month's DEX score.
Perceptions of IT	A sentiment survey that is optionally deployed using the sentiment feature of **1E Experience**.
Operations	The stacked bar chart shows the following detail for the selected month. **Actions** are issues identified and resolved manually or scheduled. These are action instructions that have been run through Explorer, or any other app, but exclude actions run by ServiceNow ITSM and Virtual Assistant, and 1E Shopping. **Policy Fixes** are issues resolved automatically by **Guaranteed State** policies **ITSM actions** are action instructions run by the 1E ServiceNow app **1E ITSM Connect** **Virtual Agent actions** are action instructions run by chatbots, for example the 1E ServiceNow app **1E Virtual Assistant** **Self Service actions** are self-service requests made by end-users of: **1E Shopping**, where a requested item causes an action instruction to be run on the end-user's device **1E Service Catalog Connect**, where a service request is submitted that causes an action instruction to be run. The current version of Exec Dashboard does not differentiate between actions run by the three ServiceNow apps (ITSM Connect, Virtual Agent and Service Catalog Connect) because they all use the same ServiceNow consumer. For more information about ingrating these self-service

Tile, chart or detail	Source

products with Tachyon, please refer to:Shopping 6.1 - Enabling Tachyon integration and 1E Service Catalog Connect 2.0.

6.2.1.4 Compatibility matrix for ServiceNow apps with and Tachyon platform

The following table contains details of all currently supported 1E ServiceNow integration apps. Use this table as a reference to ensure you are using the correct combination of apps for your needs. Each app is dependent on a 1E Core app and a Tachyon installation.

1E ServiceNow App	**Version**	**Supported versions of Tachyon platform**	**Supported versions of ServiceNow**	**Purpose**
1E ITSM Connect	3.2.1	5.2, 8.0, 8.1	Quebec, Rome, San Diego	Integrates ServiceNow ITSM with Tachyon, to provide real-time inventory and pre-approved automated fixes to first line teams from within the ServiceNow Incident page. Support for 1E Core (new in 2.0.0). Device View and Experience integration (new in v3.0). Support for domain separation

1E ServiceNow App	Version	Supported versions of Tachyon platform	Supported versions of ServiceNow	Purpose
				(multi-tenant) (new in v3.1). Support for 1E CMDB Connect app (new in v3.2).
1E Service Catalog Connect	2.0.1	5.2, 8.0, 8.1	Quebec, Rome, San Diego	Integrates ServiceNow Service Catalog with Tachyon. Provides a UI like 1E Shopping – allows WSA to be invoked by ServiceNow and report WSA requests. Guided Tour, and running any instruction (new in v2.0.1).
1E Virtual Assistant	2.0.1	5.2, 8.0, 8.1	Quebec, Rome, San Diego	Provides a Virtual Agent for ServiceNow, supporting various topics, some of which use instructions.
1E Core	2.1.0	5.2, 8.0, 8.1	Quebec, Rome, San Diego	Platform enabler.

1E ServiceNow App	Version	Supported versions of Tachyon platform	Supported versions of ServiceNow	Purpose
				Provides copy of instructions. Support for domain separation (multi-tenant) (new in v2.0). Support for 1E CMDB Connect apps (new in v2.1) including Service Graph Connector for Tachyon.
Service Graph Connector for 1E Tachyon	2.0.0	5.2, 8.0, 8.1	Quebec, Rome, San Diego	1E CMDB Connect, and Service Graph Connector for Tachyon, provide identical capabilities, your choice depends on your licensing. Either one can be optionally used for the following, among other features: populate device data in ServiceNow's CMDB through

1E ServiceNow App	Version	Supported versions of Tachyon platform	Supported versions of ServiceNow	Purpose
				1E Core and Tachyon provide the device FQDN required by other 1E ServiceNow apps, so they can use Tachyon. The latter requirement may also be met by any third party app capable of populating the device FQDN in the ServiceNow CMDB cmdb_ci_computer table. Change target from cmdb_ci_pc_hardware to cmdb_ci_computer (new in SGC 1.2.2). Populates installed software, disk usage and network attributes. Also provides custom table

1E ServiceNow App	Version	Supported versions of Tachyon platform	Supported versions of ServiceNow	Purpose
				for uninstalled software (new in SGC 2.0.0).
1.2.2	5.2, 8.0, 8.1	Paris, Quebec, Rome		
1E Tachyon CMDB Connect	1.0.0	5.2, 8.0, 8.1	Paris, Quebec, Rome	

6.2.2 Installing and upgrading

How to set up Dashboards, including a guide to upgrading, and using Tachyon Setup to install the Dashboards **Hotfix bundle**.

6.2.2.1 Installation

This version of Dashboards is available as a **Hotfix bundle**. The latest Accumulated Hotfix for Tachyon Platform Server 8.1 includes some platform changes that are required for the app to work. Dashboards is not included in the **1E Platform zip** that is used to install platform servers and other applications.

If you have not already installed Tachyon platform 8.1, please refer to Installing Tachyon.

You also need to have a Dashboards license added to your Tachyon license, which you can obtain from your 1E Account Team. It is included as a consumer in the Tachyon license file. You do not need the license to install the app, but you do need the license to see the app in the Tachyon portal and in the Switch app menu.

Next, download the latest Accumulated **Hotfix bundle** for Tachyon server 8.1 from the https://support.1e.com/. Then use setup to install the Hotfix bundle from the setup Maintenance screen. Please refer to Upload and apply a 1E Hotfix bundle.

6.2.2.1.1 What the Hotfix bundle does

Installing the Hotfix bundle using Tachyon Setup will:

Add a new **Dashboards** app to the Tachyon Platform portal

Upload a new **1E-ExecutiveDashboard.zip** product pack and create the **1E ExecutiveDashboard** instruction set from it

Create a new role **Dashboards User** that allows access to the Tachyon Dashboards app and has **Questioner** permissions to the **1E ExecutiveDashboard** instruction set.

6.2.2.2 Post-install configuration

To view and use Dashboards, a Tachyon user must be assigned to the new role **Dashboards User**, or be assigned to the **Full Administrator** role. The **Dashboards User** role, aside from allowing access to the app, also has permissions to run the questions in the **1E ExecutiveDashboard** instruction set that feed information to the tiles on the **Exec Dashboard** page.

Refer to Requirements for a list of 1E Companion products that provide source data for Dashboards features.

Refer to Dashboards post-installation tasks for enabling access to executives.

6.2.2.3 Tachyon Dashboards post-installation tasks

Post-installation tasks, which include verification checks and mandatory and optional configuration tasks.

6.2.2.3.1 Required tasks

The following tasks must be performed post-installation of the Dashboards patch, before enabling access to the application for your execs.

6.2.2.3.1.1 Accessing Tachyon Dashboards

The application will be available after installation using the following URL. For example:

> **Note**
>
> https://<platform URL>/1E/App/#/dashboards/overview

6.2.2.3.1.2 Configuring the Perception of IT survey

You have the following options:

Create a new sentiment survey called Perception of IT (recommended)

Clone an existing sentiment survey with the name **Perception of IT**

Do not use the feature - the tile will show no data, but the DEX Sentiment score will reflect any other Experience sentiment surveys that have been deployed.

For more details on creating Experience surveys, please refer to Getting feedback via Sentiment Surveys.

> **Note**
>
> The **Perception of IT** chart may show one of the following errors or messages:

Error no data - if the survey does not exist, or has been created with the wrong name. To remove error, you can create the survey, but you do not need to enable or deploy it

No Survey Responses - if the survey exists, but is not enabled and deployed

Experience Not Licensed- if your implementation does not have a license for Experience.

These messages and their error handling may change in a future version of Exec Dashboard.

6.2.2.3.1.2.1 Create a new sentiment survey called Perception of IT

Ensure you name the survey **Perception of IT**. In this version of Dashboards, it is not possible to specify a different survey name.

To create the survey, you will need to use Experience and have the **Experience Administrator** role:

Navigate to the **User Engagement** page in Experience.

Click on the **New Engagement** button.

On the **New Engagement** page, ensure the **Sentiment Survey** tab is selected.

Fill out the fields on the page according to the following recommendations:

Field	Recommendation
Name	This must be set to **Perception of IT**.
Question	This should be set to a question that is relevant to how you want your end-users to answer the response. For example, you could set this to: **How would you rate the performance of your IT department?**, as this matches with the **Visual Rating 5** template responses available to the end-users: **Very Poor**, **Poor**, **Average**, **Good** and **Very Good**. The exact wording of the question is down to your business requirements, but it should at least match the available responses to avoid confusion.
Description	This should be set to a description that helps your end-users understand why the survey is being asked and how they can respond appropriately. This provides your end-users with more context as to why they are being asked to respond. For example, this could be set to: **We would like to see if we're doing a good job of providing you with IT services.** The exact wording of the description is down to your business requirements, but it should be phrased to encourage your end-users to think about how to best respond to the survey.
'Read more' link	You could provide your end-users with more details on the importance of the survey with the **Read more** link, but this is entirely down to your own judgment as to how you want to guide them.
Prompt question every n days	This option determines when your end-users are prompted to answer the survey. You should select an appropriate period, so as not to repeatedly prompt them with requests to fill out the survey, but enough to remind them that it is there. A value of **7** days could be reasonable, this would mean that your end-users would be prompted to fill out the survey each week. Remember that they can choose to

Field	Recommendation
	fill out the survey using the Real-time Control Center menu at any time, regardless of how often they are prompted.
Use template	On the **Exec Dashboard** page, the results for the **Perception of IT** survey will be displayed according to the average responses for each user and how that average falls into the response options for the **Visual Rating 5** template. For this reason, we recommend that you set **Use template** to **Visual Rating 5** correspondingly, although the responses are averaged out, so it's not critical that this matches.
Select icon family	On the **Exec Dashboard** page, the results for the **Perception of IT** survey will be displayed using the smiley face icon family, so we recommend that you choose this option for the survey.
Allow free text entry	Setting this option is entirely your own choice. The display of the results for the **Perception of IT** survey on the **Exec Dashboard** page do not reflect this additional information, but this information can be viewed in the **Experience** App.

When the fields for the sentiment survey in the **New Engagement** page have been set, click **Save** to store them. You will be prompted that **Pending engagement changes to be deployed**. This indicates that extra steps are needed before the survey is active.

Check the checkbox at the left-hand end of the newly saved **Perception of IT** survey, and then click the **Enable Selection** button. Answer **Yes** to the **Enable Selection** prompt subsequently displayed.

Check the checkbox at the left-hand end of the newly enabled **Perception of IT** survey, and then click the **Assign Mgmt Grp** button.

In the **Assign Management Groups** popup, select a Management Group to assign to the survey. This will set the devices that will be targeted with the survey. Click **Save** to store the assignment.

> **Note**
>
> You might want to consider assigning the survey to a Management Group that contains some locally accessible test devices so that you can see how the survey will appear to your end-users. When you roll out the complete survey, you may want to target **All Devices** - or you may choose to send your survey to one department at a time, as long as you have created Management Groups that select those department devices. Bear in mind that the results in the Dashboards are presented as if they represent the responses for the end-users across the whole organization, so the most appropriate may be the **All Devices** Management Group, or one that specifically targets all end-user devices.

Click the **Deploy** button to send the survey to the devices targeted via the assigned Management Group.

6.2.2.3.1.3 *Verify installation*

Note

You must perform the verification tests provided on the Verifying page. Those tests reference each of the required tasks below.

6.2.2.4 Uninstalling Dashboards

Because this release of Dashboards is provided as a **Hotfix bundle**, it is not possible to uninstall completely. However, you can disable the **Dashboards** app and stop it from being displayed by disabling the **Dashboards** consumer using the **Settings** app.

6.2.2.4.1 Disabling the Dashboards consumer

To do this, you will need to have one of the following roles: **Full Administrator**, **Installer**, or a custom role with the **Consumer** global **Read** and **Write** permission.

Navigate to the **Configuration**→**Consumers** page in the **Settings** app.

Locate the **Dashboards** consumer in the consumer list and check the checkbox at the left-hand side of its entry in the list.

Click the **Edit** button.

In the **Edit consumer** popup uncheck the **Enabled** checkbox and click **Save**.

The **Dashboards** consumer will now be disabled. Refresh the browser and the **Dashboards** app will no longer be available.

Note

Before refreshing the browser, it will still be possible to view the Dashboards, and anyone else viewing this in another browser will still be able to see it until they refresh or login again to Tachyon platform.

6.2.2.4.2 Re-enabling Dashboards consumer

It is also possible to re-enable the Dashboards consumer to allow subsequent access to the Dashboards app. Follow the instructions above, but check the **Enabled** checkbox in step 4. instead.

6.2.2.4.3 More permanent disabling of Dashboards

If you no longer want to use the Dashboards feature or have access to this open beta, you can request 1E to remove it from your license. This will stop the application from displaying altogether and can only be reverted by requesting that it is added back into your license.

6.2.3 Verifying

Basic verification tests that cover the installation and basic use of Dashboards.These tests should be run in series. Depending on the decisions you have made during the design phase of your implementation, you may need additional tests to verify your implementation.

Note

Please ensure you complete all verification tests. They not only confirm your system is operational, but they also introduce you to concepts and tasks that you will use later when using Dashboards.

To run these tests, you need:

A valid license that includes Dashboards.

To have installed the **Hotfix bundle** that contains the Dashboards release.

To have completed all the steps on Tachyon Dashboards post-installation tasks.

6.2.3.1 Verify Tachyon Dashboards

The following verification steps check that the Tachyon Dashboards application has been installed correctly and is displaying the correct information.

6.2.3.1.1 Basic Hotfix bundle installation verification

To run the following verifications, log in with a user that has the **Full Administrator** role.

Ref	Test	Expected	Remediation
BH 01	Ensure that the application is displayed on the Tachyon home page.	Navigate to: https://<tachyonbaseurl>/tachyon/App/#/system/home Confirm the **Dashboards - 1E Labs**tile is visible.	If the tile is not visible, check that requirements 1. and 2. have been met.
BH 02	Ensure that the 1E ExecutiveDashboard.zip product pack has been loaded.	Navigate to the **Instructions→Instruction sets** page in the **Settings** app. Confirm the **1E ExecutiveDashboard** instruction set is visible and that it contains the 10 instructions from the product pack loaded by the hotfix bundle.	If the instruction set is not visible, check that requirements 1. and 2. have been met. If the instruction set is visible but does not contain any instructions, check the **Tachyon.Setup.log**, located in the same directory as **Tachyon.Setup.exe**, to see if there was an attempt to upload the instructions that failed due to licensing issues. Search for entries that contain the following text (time and date

Ref	Test	Expected	Remediation
			stamps have been left out of the text): *ERROR Tachyon.ProductPackDeploymentTool - The server reported an error while uploading ... ... [{"ErrorCode":"ProductPack.SsiIsNot1ESigned"* This may indicate that your license is not configured correctly to license the Dashboards app.
BH 03	Ensure that the new **Dashboards User** custom role has been added to the Tachyon Roles.	Navigate to the **Permissions→Roles** page in the Settings app. Confirm the **Dashboards User** role has been added. Click on the name link for the **Dashboards User** role to display the **Edit Role** page. Confirm the **Dashboards User** role has **Questioner** permissions on the **1E ExecutiveDashboard** instruction set. Exit the editor by clicking **Cancel**.	If the role has not been created there were probably errors during the installation of the **Hotfix bundle**, please check the **Tachyon.Setup.log** file, located in the same directory as **Tachyon.Setup.exe**.

6.2.3.1.2 Executive Dashboard data verification

To run the following verifications, log in with a user that has the **Full Administrator** role.

ED01	Ensure that the application is displayed after clicking on the **Dashboards - 1E Labs** tile.	The **Dashboards** app is displayed open on the **Exec Dashboard** page.	Check that you are accessing Tachyon with a user that has the **Full Administrator** role.
ED02	Ensure that the **Perception of IT** tile is showing data.	The **Perception of IT** tile displays information related to	If the tile displays the text **An error occurred**, this is usually an indication that the **Perception Of IT** survey has not

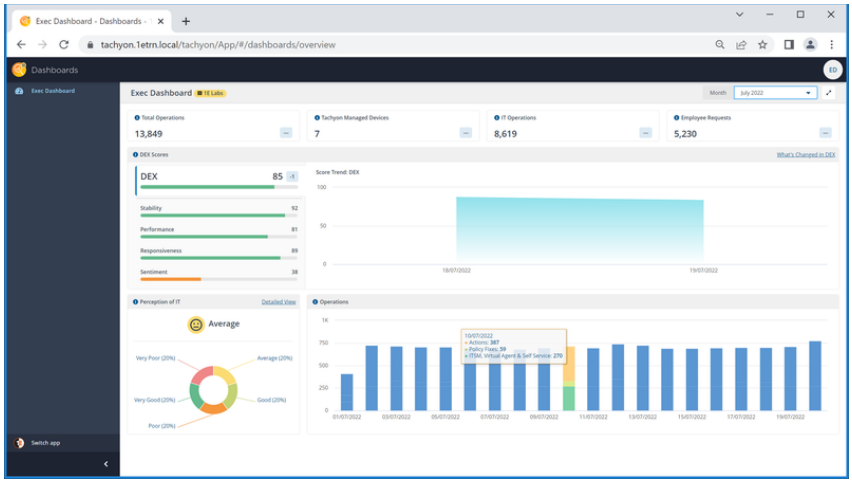
the **Perception Of IT** sentiment survey.	yet been created - ensure that requirement 3 has been fully met. If the tile displays the text **No Survey Responses**, this may be due to the following: no end-user has responded Tachyon Dashboards has not yet processed the response - this can take up to 3 minutes from when the response was received by Tachyon, as the front-end display is cached the **Perception Of IT** sentiment survey has been created but not yet deployed.

6.3 Using Tachyon Dashboards

How executive users use Tachyon Dashboards to monitor their organization's DEX performance.

6.3.1 Assessing how Tachyon contributes to company DEX performance

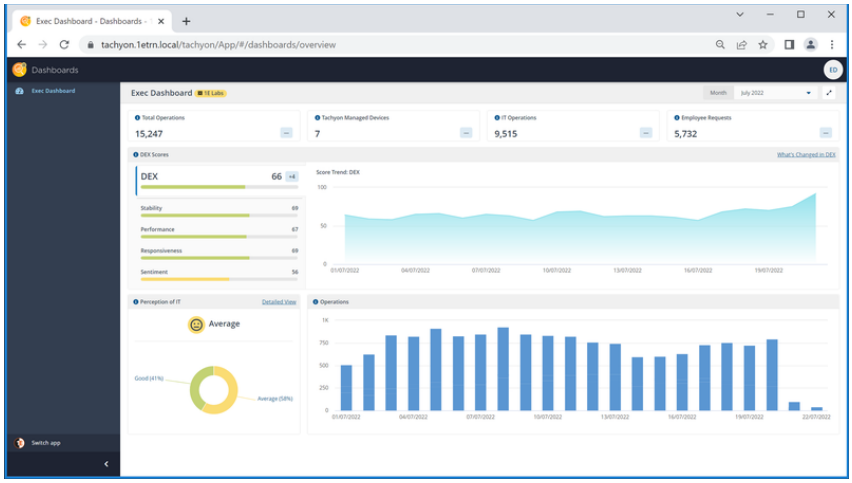
A CIO uses the dashboard to see how Tachyon is benefiting their organization, get a feel for how their company DEX is looking, and see how their users rate their IT department.



6.3.1.1 Viewing the headline information for the current month on the Exec Dashboard page

The CIO navigates to the page and sees the data for the current month displayed. Along the top row, they can see information about the way that Tachyon is performing in their environment: **Total Operations**, **Tachyon Managed Devices**, **IT Operations** and **Employee Requests**.

Tile	Description
Total Operations	The **Total Operations** figure for this month is calculated as **15,135**. This is the number of actions that have been performed on the network using Tachyon, and that's not including questions that have been asked to get back information that may have been useful in resolving end-user issues. There are a number of ways that Tachyon is prompted into action, and these fall into two main categories that are also displayed on the top-row: **IT Operations** and **Employee Requests**.
Managed Devices	This tile shows the number of devices that have connected to Tachyon during the selected month. This shows how many devices are being managed using Tachyon and having actions performed on them. In this example, we're showing a lab environment with only a few devices.
IT Operations	The **IT Operations** figure shows the number of Tachyon actions performed by the IT department using Tachyon, either run manually or using a scheduled instruction from Tachyon Explorer, or automatically performed using Guaranteed State.
Employee Requests	Employee requests show the number of Tachyon actions that have been run as a result of users requesting items via ITSM, through the Virtual Assistant or using Shopping to select an instruction.



6.3.1.1.1 Checking the daily details for Total Operations

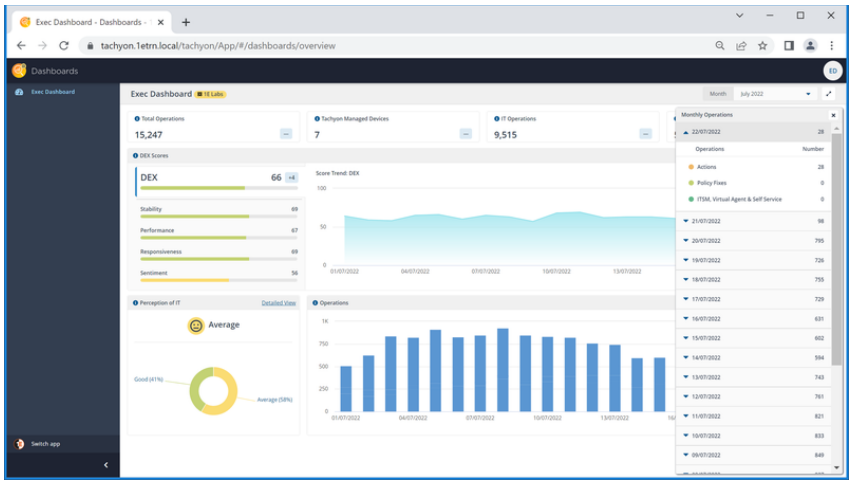
Clicking on the **Total Operations** tile provides details on how that figure is derived for each day in the current month. This shows the CIO that so far today:

Their IT team was responsible for **464** actions, either run manually from Tachyon Explorer or using a scheduled instruction

Guaranteed State has automatically made **54** fixes to devices

Users have requested via ITSM, Virtual Assistant and Self-service instruction items in Shopping, **270** actions

leading to a total of **788** Tachyon operations for the day so far.



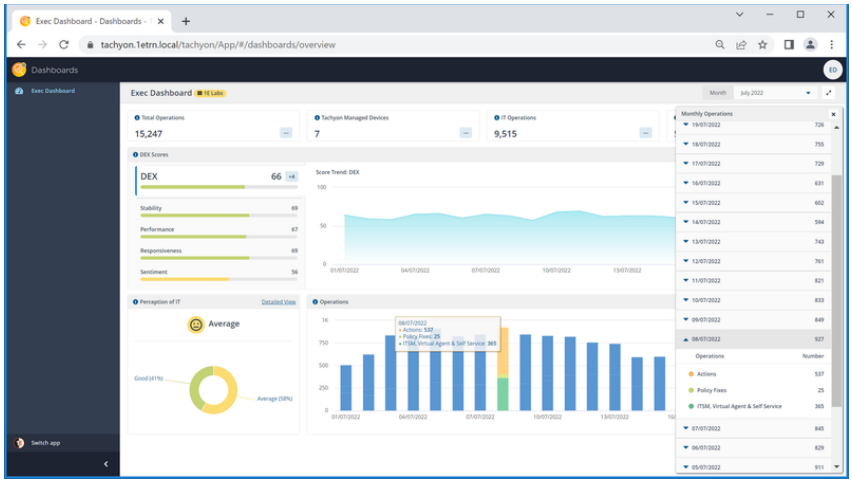
6.3.1.1.2 Checking the Operations chart for the highest number of Total Operations so far this month

The CIO can also see the breakdown of operations per day in the **Operations** tile along the bottom-right of the dashboard. Scanning across, they can see one day that stands out. Clicking on the bar for that day shows the make-up of the total:

537 actions

25 policy fixes

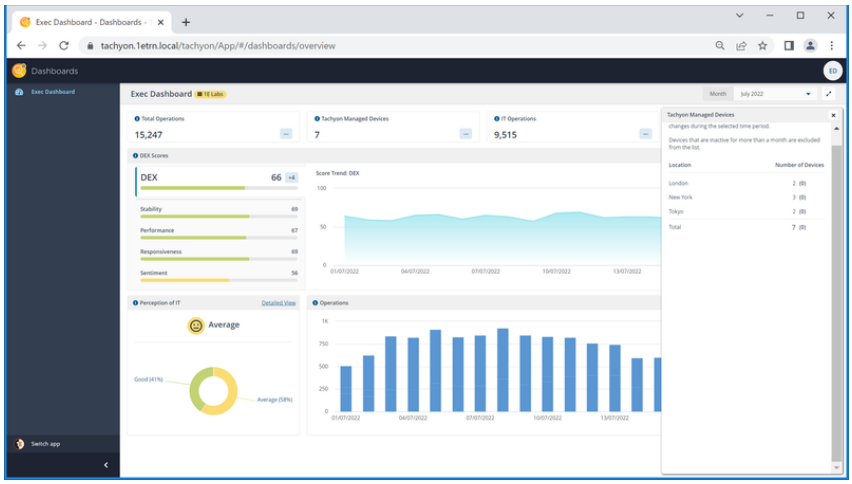
365 ITSM, Virtual Assistant & Self-service.



6.3.1.1.3 Viewing details for Tachyon Managed Devices

The CIO wants to find out more information about the devices that have connected to Tachyon during the current month. Clicking on the **Managed Devices** tile displays a breakdown of the devices organized into their locations, set using instructions.

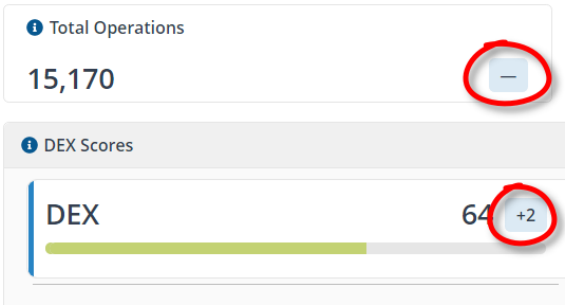
Here they can see that they've had devices reporting back from all their locations, **London**, **New York** and **Tokyo** (not in high numbers, but this is a lab example).



6.3.1.1.4 Change indicators

There is a change indicator at the bottom-right of each headline tile and at the top-right of the DEX score display. When the current month is displayed, the only indicator that shows any information is the DEX score display one, all the other ones display dashes. This is because the counted data in the headline tiles for the current month is incomplete, so comparisons with the previous month cannot be easily made.

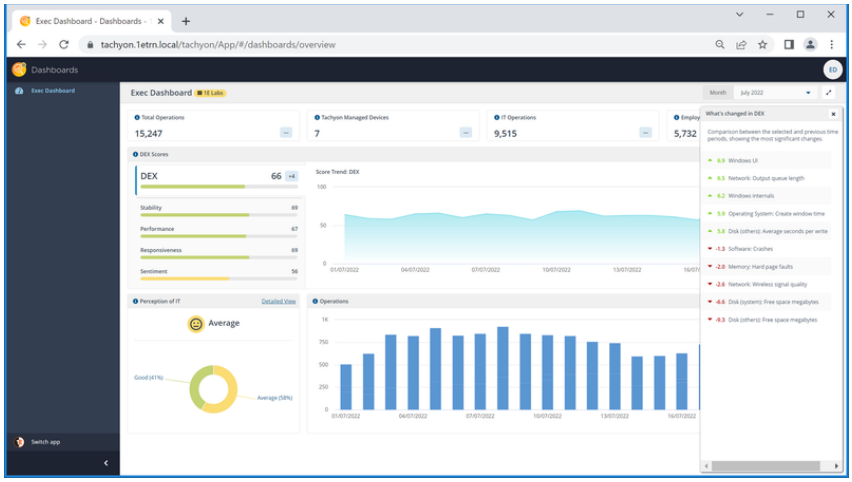
The DEX score, is calculated as an average and displayed as a change in the score, not a percentage.



6.3.1.1.5 Looking at What's changed in DEX

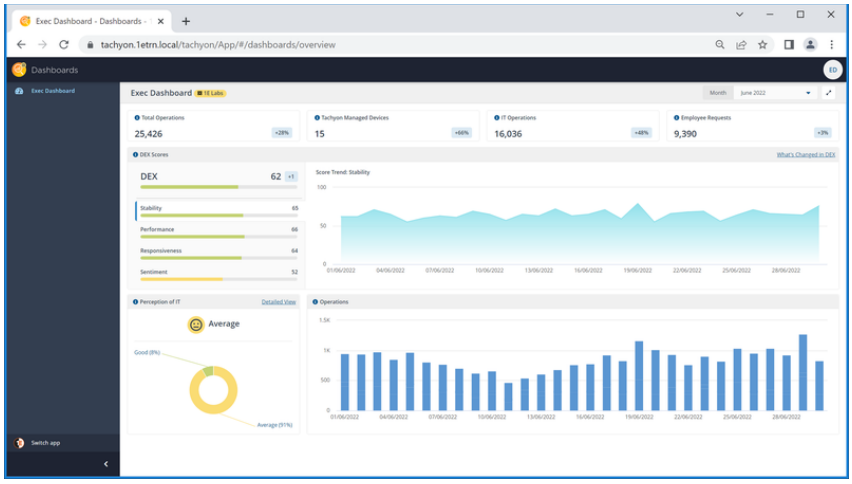
The dashboard shows information from Experience that highlights how the company is doing from a DEX perspective. The **DEX Scores** tile presents the CIO with an overall view of their DEX score and shows how it has changed since the previous month. This overall averaged score consists of the distinct **Stability**, **Performance**, **Responsiveness** and **Sentiment** scores (also averaged). Clicking on the **What's changed in DEX** link displays details on the metrics that are reported on by Experience have gone up or down in terms of their largest impact on DEX.

The **Sentiment** score is related to all the sentiment surveys that have been sent out and responded to by end-users. The **Perception of IT** tile is related to the responses of just the **Perception of IT** sentiment survey.



6.3.1.2 Comparing Operations with the Stability score

Scanning along the **Operations** chart, the CIO can see there's a peak of operations on the 19th of June, they can check through the DEX data to see if there are any correlations with this peak. Clicking on the **Stability** score shows the **Score Trend: Stability** chart. Here they can see that there's a corresponding peak in device stability, it might be that some remediation or actions that took place on that day were having a positive effect on system stability - and perhaps checking with their IT manager to see what the additional operations were related to.



6.3.1.3 How is my IT department doing?

The CIO can get a feel for how their IT department is perceived by their employees, by checking the **Perception of IT** tile. The values that are shown are the averages of each user's responses, which are then counted and placed into one of five buckets:

Very Good

Good

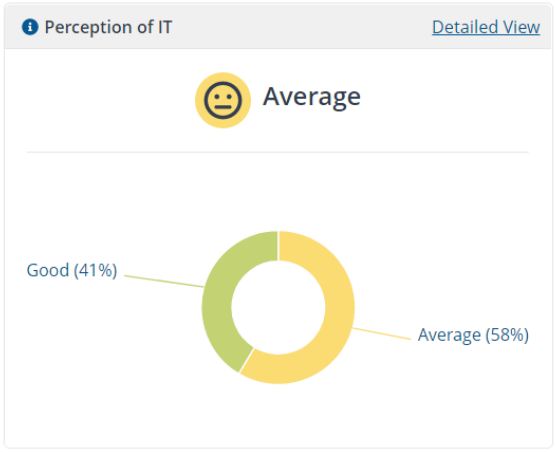
Average

Poor

Very Poor.

Each bucket with values is then plotted using a donut chart, and the largest segment is then displayed as the overall rating.

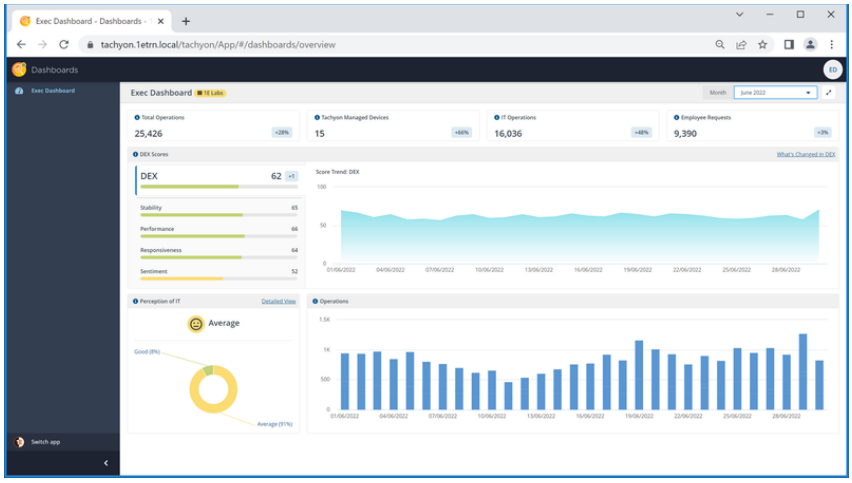
For example, in our example in July the largest segment with values is **Average**, which is used as the overall rating - with 58% of the respondents averages falling into that. All the other respondents averages fall into the **Good** rating - the percentage values displayed are rounded down. This tells the CIO that overall the responses are average, but with a large chunk tending towards good. So how does this compare with the previous month?



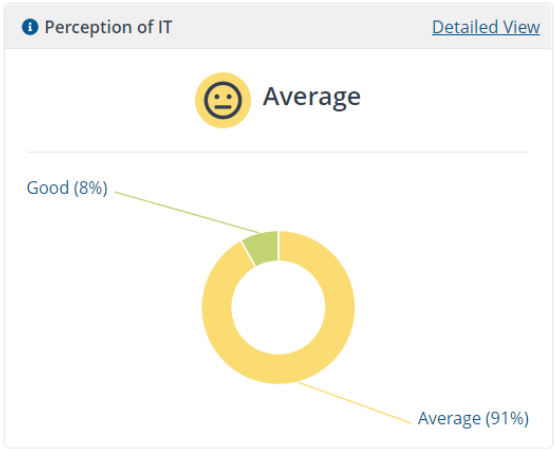
6.3.1.3.1 Looking at the data for previous months

Clicking on the **Month** selector, at the top-right of the **Exec Dashboard** page, lets the CIO change which calendar month of data is displayed on the screen. There are only three months covered, the partial data for the current month, the full aggregated data for the preceding two months.

For the months before the current one, the change indicator at the bottom-right of each headline tile displays the deltas between the selected month and the one before. For the month of June 2022, the CIO can see that the **Total Operations** for that month are up **28%** when compared with May 2022.

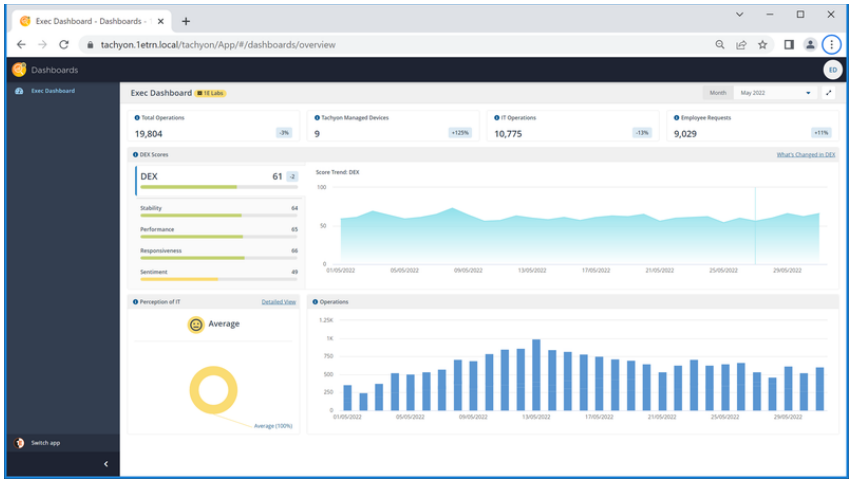


Focusing on the **Perception of IT** tile, the CIO sees that in the previous month there was a smaller percentage of respondents, just **8%**, where they averaged out to **Good**. So things have improved in July so far, where the number of **Good** respondents is up to **41%**.



6.3.1.3.2 Looking at the earliest month

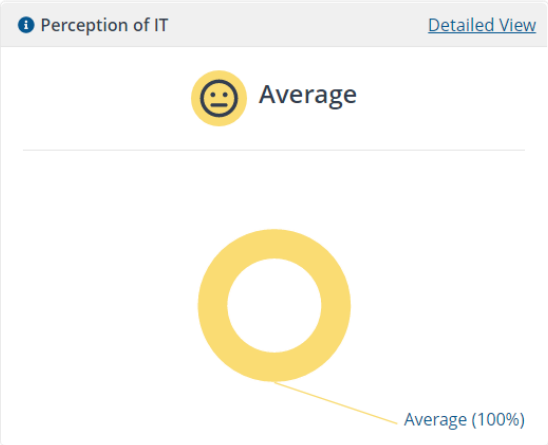
The CIO now uses the month selector to look at the data for the earliest available month.



Here they can see that their **Perception of IT** score has a completely average set of results. Indicating that the average for each user that replied to the survey is coming out as **Average**.

So in May the **Good** percentage was **0**, that is it didn't appear in the chart at all, in June it was up to **8%** and currently in July it's at **41%**.

So that's two months in a row where the **Perception of IT** responses have been improving. Even in the latest month they are still with the overall rating of **Average**, but the number of **Good** responses are increasing, and that may be a sign of a good trend for the CIO's IT department.



6.4 Troubleshooting

A general methodology for investigating issues with Dashboards, as well as identifying key issues and their resolutions.

6.4.1 1E Support contact details

6.4.1.1 Support Web portal

Maintenance support customers can log onto the 1E Support Web Portal at https://support.1e.com/ using the login details provided with their maintenance contract. This provides issue tracking, product hotfixes, and knowledge base articles related to each product.

6.4.1.2 Telephone support

Maintenance support customers can contact the technical support department at 1E through the following support numbers. Just phone the relevant number for your area, so your call can be routed quickly and efficiently to the correct support group:

US/Canada:	1-866-349-4032 (Toll-Free)
	1-917-339-2360 (Standard)
UK/Europe:	+44 (0)208 326 3499
India:	+91 120 402 4002

Australia: +61 739 111 118

6.4.1.3 Email support

Maintenance customers can use the following email for additional support. Evaluation customers can also use this email with the temporary access code that is provided through customercare@1e.com as part of their evaluation.

support@1e.com

6.4.1.4 Maintenance

You are recommended to review and apply hotfixes on a monthly basis. Hotfixes are provided in **Hotfix Bundles** and in **Monthly Updates**, which are installed using Tachyon Setup. Please refer to Maintenance.

6.4.1.5 Creating a technical report

If possible, please obtain the following details and log files before contacting 1E, to include in your technical report.

6.4.1.5.1 Version details

The OS, version number, and patch level for:

Tachyon Servers

1E Client

Configuration Manager - if used

Other 1E Server software, for example, Shopping, Nightwatchman, and WakeUp.

For Nomad and Shopping, please provide OS, version number, and patch level for:

Configuration Manager DPs

Nomad extensions used on Configuration Manager Consoles

ActiveEfficiency Server.

6.4.1.5.2 Environmental details

If there were any recent changes made to your configuration

The name of the machines, Configuration Manager Application and/or Package IDs for when the issue occurred

6.4.1.5.3 Problem details

When did the issue occur, ensure log files cover this period

The scope of the issue – did it affect a particular geographical location, group of users, or client machines

Details of any self-help troubleshooting steps you carried out

In the event of a service crash or if you are experiencing high CPU or memory usage, provide us with the dump file, event viewer logs, and traces. We will provide you with FTP details to upload these files.

6.4.1.6 Log files

Below is a summary, please refer to the Log files page for more details.

6.4.1.6.1 Tachyon Setup log files

Tachyon Setup creates a Setup log file for itself and an Install log for each of the components (if used) in the same folder as itself:

BIInstall.log

CatalogInstall.log

ContentDistribution.log

SLAInstall.log

Tachyon.Setup.log

TachyonInstall.log

6.4.1.6.2 Tachyon Server log files

For any issue, please provide a zip containing log files from the following locations:

%ALLUSERSPROFILE%\1E\Catalog*.log

%ALLUSERSPROFILE%\1E\ContentDistribution*.log

%ALLUSERSPROFILE%\1E\Platform Consumers*.log

%ALLUSERSPROFILE%\1E\SLA Platform*.log

%ALLUSERSPROFILE%\1E\Tachyon*.log

If you are having licensing issues, please include:

%ALLUSERSPROFILE%\1E\Licensing*

6.4.1.6.3 1E Client log files

1E Client logs on Windows

1E Client logs on macOS

1E Client logs on other non-Windows platforms

Nomad client log

PXE Everywhere Agent log

Shopping WSA client log

WakeUp client log

> **Note**
>
> By default, Windows resolves %ALLUSERSPROFILE% as C:\ProgramData\

6.4.2 Known issues

Lists of the current known issues for implementing, configuring and using Dashboards.

Issue	Description	Workaround
After initially installing the Hotfix bundle, when navigating to the **Exec Dashboard** page and then selecting to view earlier months, an error is displayed in the **Tachyon Managed Devices** tile.	This is because some of the data that is used for the **Tachyon Managed Devices** tile has not yet been generated.	You will need to wait for the first scheduled aggregated data sync to run at 23:59 UTC to happen. After this sync has run, the error will not be displayed.
If the **Tachyon Managed Devices** drawer is open on the **Exec Dashboard** page, and the month selector is used to change to another month, the data in the drawer is not updated to reflect the change.	The update is not being handled in the drawer correctly, so the information displayed is not updated when the month changes.	To view the correct data, close and then re-open the **Tachyon Managed Devices** drawer by clicking on the **Tachyon Managed Devices** tile.
An error occurred message appears when clicking on the **Detailed View** link on the **Perception of IT** tile to display the **Perception of IT** details drawer.	This occurs when the selected month doesn't have any data for the **Perception of IT** sentiment survey.	Refresh the page and the **Detailed View** option to display information on the **Perception of IT** survey results is no longer displayed.

Issue	Description	Workaround
The tooltips used to provide information on the screen refer to **manual actions**.	This text should refer to **manual or scheduled actions**.	n/a
The text **An error occurred** appears on the **Perception of IT** tile.	This text appears when the **Perception of IT** survey has not yet been created in Tachyon Experience.	An Experience administrator should create and save the **Perception of IT** survey.

6.4.3 Implementation Issues

Troubleshooting common issues that you may be having with implementing the Tachyon Hotfix bundle.

6.4.3.1 Post-application of the Hotfix bundle

6.4.3.1.1 Dashboards - 1E Labs not displayed

If the **Dashboards - 1E Labs** tile is not displayed on the Tachyon home page, check that you have a valid Tachyon license that includes the **Dashboards** app. You ask your 1E Account Team to get your license updated.

In a rare cases, if the **Dashboards - 1E Labs** tile is still not visible after the Hotfix bundle has been applied, an IIS reset might be required.

6.4.3.1.2 Issues with the 1E ExecutiveDashboard instruction set

If the instruction set is not visible on the **Instructions→Instruction sets** page in the **Settings** app, check that you have a valid Tachyon license that includes the Dashboards app.

If the instruction set is visible but does not contain any instructions, check the **Tachyon.Setup.log**, located in the same directory as **Tachyon.Setup.exe**,to see if there was an attempt to upload the instructions that failed due to licensing issues.

Search for entries that contain the following text (time and date stamps have been left out of the text):

```
ERROR Tachyon.ProductPackDeploymentTool - The server reported an error while uploading ... ... [{"ErrorCode":"ProductPack.SsiIsNot1ESigned"
```

This may indicate that your license is not configured correctly to license the Dashboards app.

6.4.3.1.3 Issues with the Dashboards User custom role

If the role has not been created, there were probably errors during the installation of the **Hotfix bundle**, please check the **Tachyon.Setup.log** file, located in the same directory as **Tachyon.Setup.exe**.

6.5 Reference

All the Dashboards related tables of information, such as supported platforms, communications ports etc.

6.5.1 Log files

Names and locations of log files created by Tachyon Server, 1E Client, and Tachyon tools.

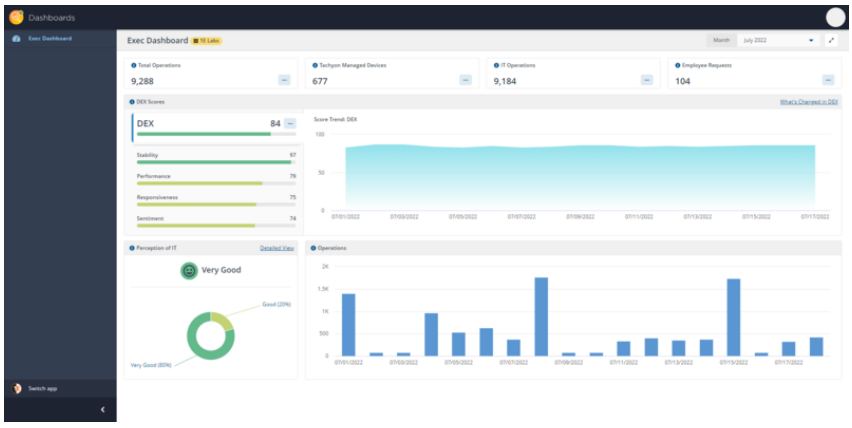
For full details, refer to Log files.

6.5.2 Page reference

A reference for the fields and tables on the pages in Dashboards.

6.5.2.1 Exec Dashboard page

The **Exec Dashboard** is an overview page in the Tachyon Portal, mainly aimed at CIO executives, showing the benefits that Tachyon is providing and highlighting how the company has been performing in terms of DEX over the past few months.



6.5.2.1.1 Time Period

Using the **Time period** filter at the top of the page, you can narrow down the results by date. You can choose from the current month's DEX score report, or one of the previous two months.

For the current month, the graph will show data from the 1st date of the calendar month to yesterday's date, for example:

July 2022 (current month until yesterday, so data doesn't change every second)

June 2022

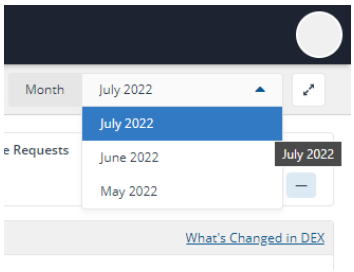
May 2022

When the **Time Period** is set to a period, the setting you choose is retained when you:

Manually refresh the page

Switch between Tachyon Platform apps

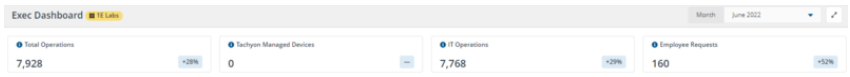
Close and reopen the app.



6.5.2.1.2 Exec Dashboard tiles

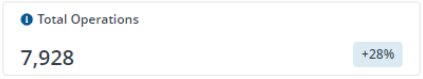
Thetilesat the top of the **Exec Dashboard**page. Each sectionallows you to quickly and easily view statistics based on the following categories.

> **Tip**
>
> The Delta for your DEX scores are only displayed once a month is complete. The examples shown are from **June 2022** in our environment. The Delta scores show the changes in the total category carried out in the selected calendar month.



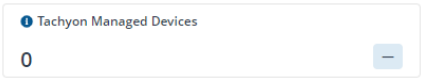
6.5.2.1.2.1 Total Operations

Total number of issues resolved by manual actions, automated policy fixes, ITSM actions, Virtual Assistant actions, and other self-service requests. In our example, the total is 160 (Employee Requests) + 7,768 (IT Operations) = 7,928 (Total Operations).



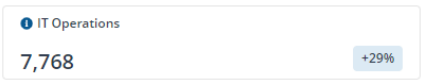
6.5.2.1.2.2 Tachyon Managed Devices

Number of devices managed by Tachyon. These are the devices where the installed 1E Client has contacted Tachyon.



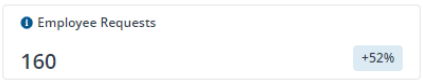
6.5.2.1.2.3 IT Operations

Number of issues resolved by manual actions, and automated policy fixes.



6.5.2.1.2.4 Employee Requests

Number of issues resolved by ITSM actions, Virtual Assistant actions, and other self-service requests.



6.5.2.1.2.5 Monthly Operations drawer

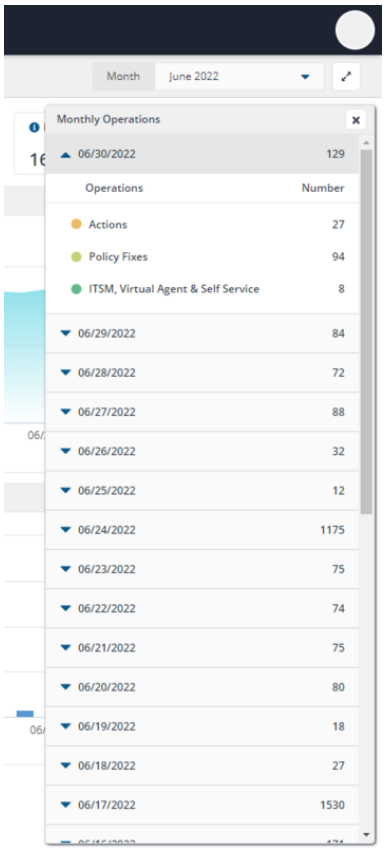
The **Monthly Operations** drawer is displayed when you click on the following tiles:

Total Operations

IT Operations

Employee Requests.

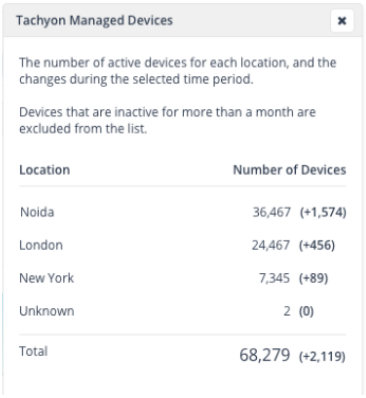
The Monthly Operations drawer displays the number of **Actions**, **Policy Fixes** and **ITSM, Virtual Agent & Self Service** per day for the currently selected month.



6.5.2.1.2.6 Tachyon Managed Devices

Displays the number of active devices for each location, and the changes during the selected time period.

Devices that are inactive for more than a month are excluded from the list.



6.5.2.1.3 DEX Scores

6.5.2.1.3.1 Score Trend

Displays the DEX score trends for the currently selected month:

DEX

Stability

Performance

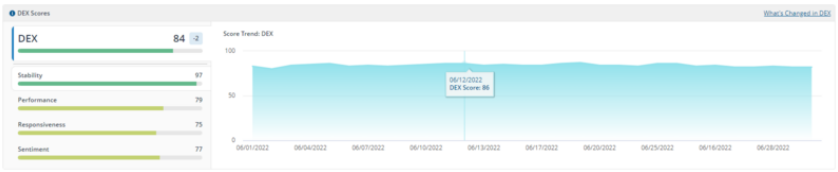
Responsiveness

Sentiment.

The DEX score includes a delta for changes in the average DEX score in the selected calendar month compared to the previous one.

The data shown is sourced from Tachyon Experience database and is aggregated for the selected time period. The DEX, Stability, Performance, Responsiveness, and Sentiment is not based on the latest score but is an average of the selected period. The DEX delta is taken from the difference between the selected time period and the previous time period.

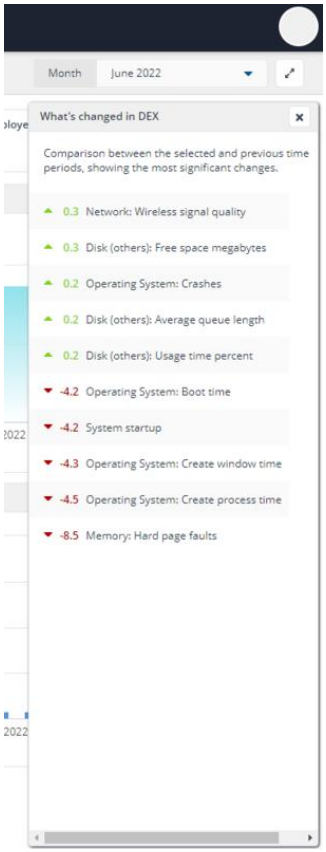
> **Note**
>
> The Tachyon Instruction **1E-Experience-DexScores** provides the data populating the DEX Scores tile.



6.5.2.1.3.2 What's changed in DEX

Shows the comparison between the selected and previous time periods, showing the most significant changes that increased and decreased.

For details of all the different metrics and scores you may see here, please review The Scores.

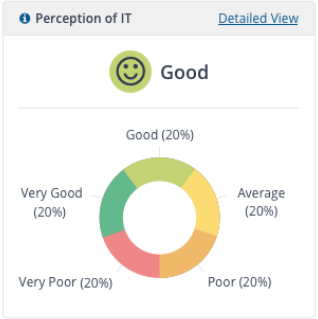


6.5.2.1.4 Perception of IT

The **Perception of IT** tile displays feedback given by end users about their experience of IT services.

Data is sourced from the Tachyon Experience database and is aggregated for your selected time period. The **Perception of IT** metric is not based on the latest score, but is based on an average of your selected period. To prevent bias in the results, multiple answers from the same user are averaged before the total scores are averaged. This ensures no single answer contributes more to the final **Perception of IT** scores than any other.

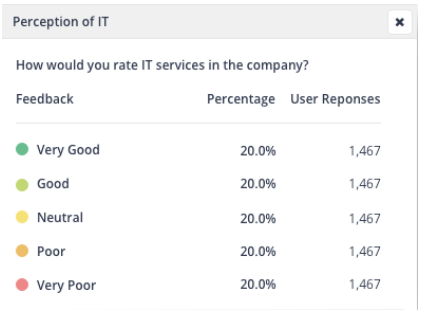
> **Note**
>
> The Tachyon Instruction **1E-Experience-SurveyResponses** provides the data populating the **Perception of IT** tile.



You can see a breakdown of the percentages by clicking on **Detailed View**.

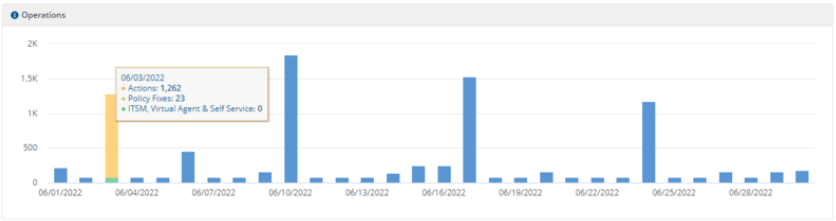
Note

The numbers show individual user responses, which can be more than one response from the same user, across multiple devices. The responses from each user are averaged.



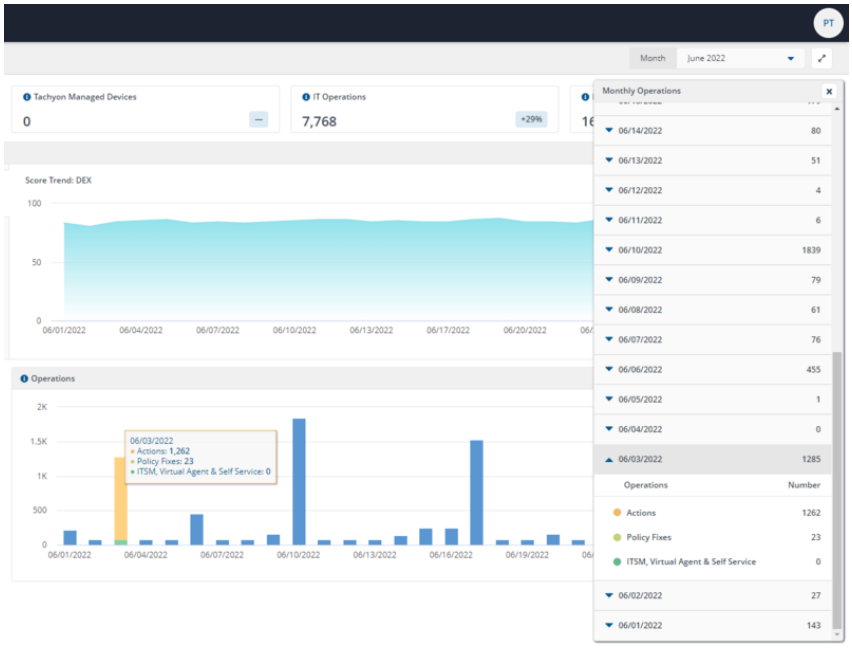
6.5.2.1.5 Operations

Number of issues resolved by manual actions, automated policy fixes, ITSM actions, Virtual Assistant actions, and other self-service requests. Hovering your mouse pointer over chart columns displays details for that time period.

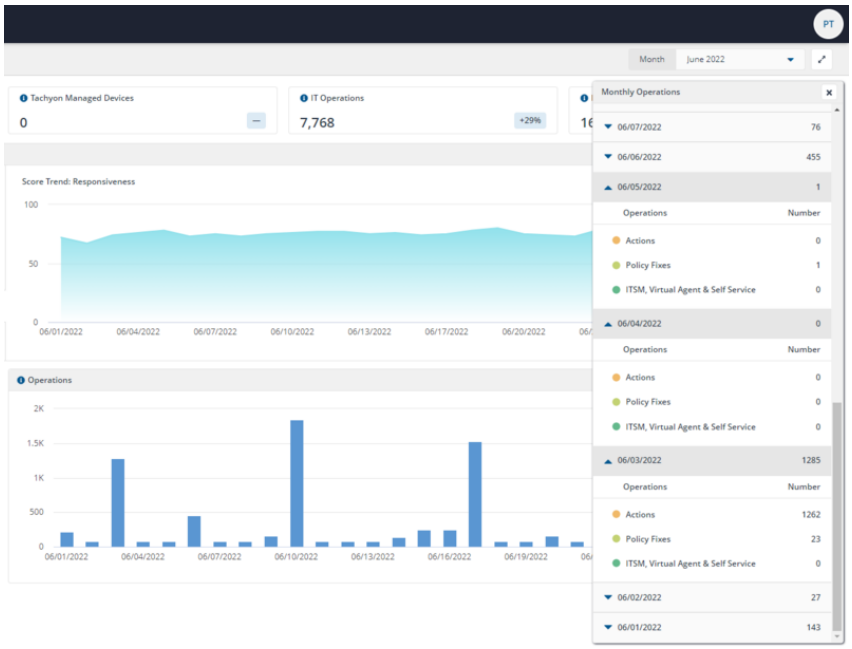


6.5.2.1.5.1 Monthly Operations drawer

Clicking on a chart column displays a drawer showing the Monthly Operations for the selected period.



You can expand the Monthly Operations chart by day to compare specific days in your chosen time period.



6.5.3 Dashboards Product Packs reference

Reference information for Tachyon feature-related Product Pack included in the **Hotfix bundle**.

Classic Product Packs contain instructions, for use in Explorer and other Tachyon applications.

Integrated Product Packs contain policies, rules and fragments for use by Guaranteed State, and may also include instructions.

6.5.3.1 1E ExecutiveDashboard product pack

Classic product pack used to create the **1E ExecutiveDashboard** instruction set, and supports retrieving data for Tachyon Dashboards.

The **1E ExecutiveDashboard** instructions are all used internally to retrieve information for the tiles on the **Exec Dashboard** page. They cannot be found or run from Explorer and do not appear in the Instructions History. If you have the right permissions, you can view the **1E ExecutiveDashboard** instruction set on the **Settings→Instructions→Instruction sets** page and see that it contains the following **Server question** instructions:

1E ExecutiveDashboard instruction payload
Get dex scores and delta for time period between <startDate> and <endDate>
Get impacted metric scores using the average scores from period <startDate> to <endDate> compared against the previous period of the same length
Get band distribution of responses to <survey> between <startDate> and <endDate>
Get band distribution of responses to <survey> and details between <startDate> and <endDate>
Get employee requests for <startDate> to <endDate>.
Get 1E managed device for <startDate> to <endDate>.
Aggregated 1E managed device count by location for <startDate> to <endDate>.
Get 1E operations for <startDate> to <endDate>.
Get 1E total IT operations for <startDate> to <endDate>.
Get 1E total operations for <startDate> to <endDate>.

Server questions are a specific type of instruction used internally to retrieve information from Tachyon platform.

6.5.4 Glossary

A glossary of Tachyon Dashboards terminology.

1E Labs | Actions | DEX | DEX Score | Employee Requests | Exec Dashboard | IT Operations | ITSM actions | ITSM, Virtual Agent & Self Service | Operations | Perception of IT | Performance | Policy Fixes | Responsiveness | Score Trend: DEX | Self Service actions | Sentiment | Stability | Tachyon Managed Devices | Total Operations | Virtual Agent actions | What's Changed in DEX

6.5.4.1 Tachyon Dashboards alphabetical glossary

Term	Definition
1E Labs	1E Labs highlights preview applications of features that are cutting edge in this version, giving you the opportunity to experience the benefits they offer and shape their development for future releases.
Actions	Part of the **Total Operations** counted by the Exec Dashboard and also plotted on its Operations chart. These relate to issues that have been resolved by running an Action. **Actions** are issues identified and resolved manually or scheduled. These are action instructions that have been run through Explorer, or any other app, but exclude actions run by ServiceNow ITSM and Virtual Assistant, and 1E Shopping. **Note** The statistics reported by Exec Dashboard include the number of action instructions that have been run. They do not include the number of questions. Although questions can be used to confirm an issue has been resolved, or used to identify an issue, it is an action that usually resolves the issue. This means the dashboard does not report on issues that were resolved outside of Tachyon, even if a Tachyon question was used to identify the issue.
DEX	DEX, or Digital Experience, provides a way of measuring the wellbeing of an organization's employees regarding their experience of the devices they use and their contact with their IT department.
DEX Score	The DEX score in Exec Dashboard is a combination of these Stability, Performance, Responsiveness, and Sentiment scores, obtained from **1E Experience**. The Score Trend chart shows data for selected score over the selected month. The above scores are a weighted combination of Experience metrics. The What's Changed popup shows the top and bottom 5 metrics that most significantly affected the selected month's DEX score.
Employee Requests	The number of issues fixed by ITSM, Virtual Agent, and Self Service. These are sum of actions instructions that have been run by ServiceNow and/or Shopping. **ITSM actions** are action instructions run by the 1E ServiceNow app **1E ITSM Connect**

Term	Definition
	Virtual Agent actions are action instructions run by chatbots, for example the 1E ServiceNow app **1E Virtual Assistant** **Self Service actions** are self-service requests made by end-users of: **1E Shopping**, where a requested item causes an action instruction to be run on the end-user's device **1E Service Catalog Connect**, where a service request is submitted that causes an action instruction to be run. The current version of Exec Dashboard does not differentiate between actions run by the three ServiceNow apps (ITSM Connect, Virtual Agent and Service Catalog Connect) because they all use the same ServiceNow consumer. For more information about ingrating these self-service products with Tachyon, please refer to:Shopping 6.1 - Enabling Tachyon integration and 1E Service Catalog Connect 2.0.
Exec Dashboard	The Exec Dashboard is an overview page in the Tachyon Portal, mainly aimed at CIO executives, showing the benefits that Tachyon is providing and highlighting how the company has been performing in terms of DEX over the past few months.
IT Operations	The number of issues fixed, either manually or by automation, and is the sum of the following: **Actions** are issues identified and resolved manually or scheduled. These are action instructions that have been run through Explorer, or any other app, but exclude actions run by ServiceNow ITSM and Virtual Assistant, and 1E Shopping. **Policy Fixes** are issues resolved automatically by **Guaranteed State** policies
ITSM actions	**ITSM actions** are action instructions run by the 1E ServiceNow app **1E ITSM Connect**
ITSM, Virtual Agent & Self Service	ITSM, Virtual Agent & Self Service is a combined number of the following: **ITSM actions** are action instructions run by the 1E ServiceNow app **1E ITSM Connect** **Virtual Agent actions** are action instructions run by chatbots, for example the 1E ServiceNow app **1E Virtual Assistant**

Term	Definition
	Self Service actions are self-service requests made by end-users of: **1E Shopping**, where a requested item causes an action instruction to be run on the end-user's device **1E Service Catalog Connect**, where a service request is submitted that causes an action instruction to be run. The current version of Exec Dashboard does not differentiate between actions run by the three ServiceNow apps (ITSM Connect, Virtual Agent and Service Catalog Connect) because they all use the same ServiceNow consumer. For more information about ingrating these self-service products with Tachyon, please refer to:Shopping 6.1 - Enabling Tachyon integration and 1E Service Catalog Connect 2.0.
Operations	The stacked bar chart shows the following detail for the selected month. **Actions** are issues identified and resolved manually or scheduled. These are action instructions that have been run through Explorer, or any other app, but exclude actions run by ServiceNow ITSM and Virtual Assistant, and 1E Shopping. **Policy Fixes** are issues resolved automatically by **Guaranteed State** policies **ITSM actions** are action instructions run by the 1E ServiceNow app **1E ITSM Connect** **Virtual Agent actions** are action instructions run by chatbots, for example the 1E ServiceNow app **1E Virtual Assistant** **Self Service actions** are self-service requests made by end-users of: **1E Shopping**, where a requested item causes an action instruction to be run on the end-user's device **1E Service Catalog Connect**, where a service request is submitted that causes an action instruction to be run. The current version of Exec Dashboard does not differentiate between actions run by the three ServiceNow apps (ITSM Connect, Virtual Agent and Service Catalog Connect) because they all use the same ServiceNow consumer. For more information about ingrating these self-service products with Tachyon, please refer to:Shopping

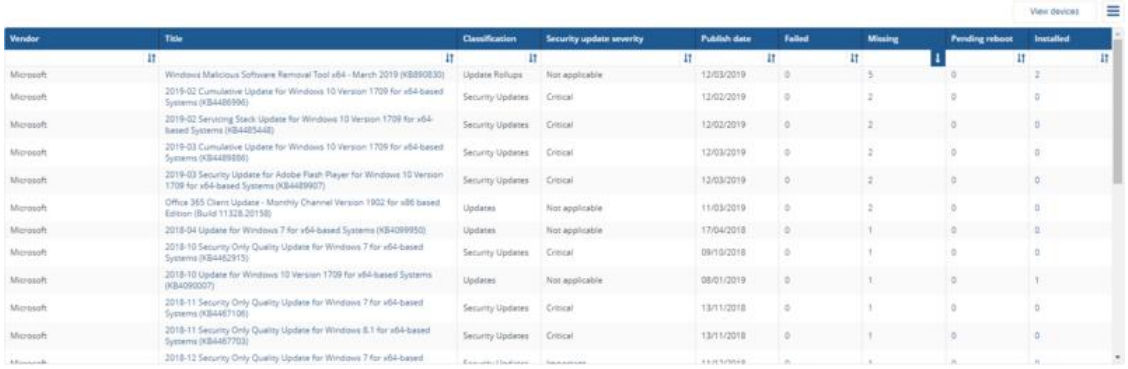
Term	Definition
	6.1 - Enabling Tachyon integration and 1E Service Catalog Connect 2.0.
Perception of IT	A sentiment survey that is optionally deployed using the sentiment feature of **1E Experience**.
Performance	Performance is a score provided by the Tachyon Experience app. Please refer to Score reference. The Performance score is derived from the scores of disk performance, CPU performance, and memory performance.
Policy Fixes	Part of the Total Operations counted by Exec Dashboard and also plotted on the Operations chart. **Policy Fixes** are issues resolved automatically by **Guaranteed State** policies
Responsiveness	Responsiveness is a score provided by the Tachyon Experience app. Please refer to Score reference. The Responsiveness score is derived from the scores of Windows internals, system startup, and Windows UI.
Score Trend: DEX	The Score Trend chart shows a trend for the selected score over the selected month, showing how the company is doing from a DEX perspective. You can hover over the chart, to see the score for a specific day of the month. Clicking on the What's Changed in DEX link displays details on the metrics that are reported on by Tachyon Experience have gone up or down in terms of their largest impact on DEX.
Self Service actions	**Self Service actions** are self-service requests made by end-users of: **1E Shopping**, where a requested item causes an action instruction to be run on the end-user's device **1E Service Catalog Connect**, where a service request is submitted that causes an action instruction to be run. The current version of Exec Dashboard does not differentiate between actions run by the three ServiceNow apps (ITSM Connect, Virtual Agent and Service Catalog Connect) because they all use the same ServiceNow consumer. For more information about integrating these self-service

Term	Definition
	products with Tachyon, please refer to: Shopping 6.1 - Enabling Tachyon integration and 1E Service Catalog Connect 2.0.
Sentiment	Sentiment is a score provided by the Tachyon Experience app. Please refer to Score reference. The User sentiment score is derived from the responses to user and metric surveys. The score for the Perception of IT survey is included in the Sentiment score.
Stability	Stability is a score provided by the Tachyon Experience app. Please refer to Score reference. The Stability score is derived from four scores based on the number of crashes and hangs for software and for the Operating System itself.
Tachyon Managed Devices	The number of devices managed by Tachyon. These are the devices where the installed 1E Client has contacted Tachyon. The number on the dashboard is cached, but the cache is updated in real-time. It increases when new clients come online, and decreases when inactive clients are purged from the Tachyon Master database.
Total Operations	The sum of IT Operations and Employee Requests for the selected month. That is, the number of issues fixed either manually, by automation, ITSM actions, Virtual Agent actions, and Self Service actions. **Actions** are issues identified and resolved manually or scheduled. These are action instructions that have been run through Explorer, or any other app, but exclude actions run by ServiceNow ITSM and Virtual Assistant, and 1E Shopping. **Policy Fixes** are issues resolved automatically by **Guaranteed State** policies **ITSM actions** are action instructions run by the 1E ServiceNow app **1E ITSM Connect** **Virtual Agent actions** are action instructions run by chatbots, for example the 1E ServiceNow app **1E Virtual Assistant** **Self Service actions** are self-service requests made by end-users of:

Term	Definition
	1E Shopping, where a requested item causes an action instruction to be run on the end-user's device **1E Service Catalog Connect**, where a service request is submitted that causes an action instruction to be run. The current version of Exec Dashboard does not differentiate between actions run by the three ServiceNow apps (ITSM Connect, Virtual Agent and Service Catalog Connect) because they all use the same ServiceNow consumer. For more information about ingrating these self-service products with Tachyon, please refer to:Shopping 6.1 - Enabling Tachyon integration and 1E Service Catalog Connect 2.0.
Virtual Agent actions	**Virtual Agent actions** are action instructions run by chatbots, for example the 1E ServiceNow app **1E Virtual Assistant**
What's Changed in DEX	The Score Trend: DEX chart includes a link **What's Changed in DEX**. The link displays details on the metrics that are reported on by Tachyon Experience, showing 5 that have gone up, and 5 that have gone down, in terms of their largest impact on DEX.

7 1E Patch Success

1E Patch Success lets you maximize success of enterprise-wide patch deployment. It provides a view of patch state of your estate, as well as supplementing your existing patch deployment methods.



7.1 Introducing Patch Success

Patch Success is a Tachyon application that lets you maximize success of enterprise-wide patch deployment. It provides a view of patch state of your estate, as well as supplementing your existing patch deployment methods.

For more information please refer to the Using Patch Success section of this documentation. Here's an overview of the features available in the Patch Success application.

7.1.1 Patch Success features

7.1.1.1 Overview page

The overview page contains three charts that show the current device patch status, the security updates by severity level and patch performance across all the devices connected to Tachyon.

The charts are interactive letting you easily drill-down into details on specific items in the display. The table can toggle between the status of devices or status of patches.

> **Note**
>
> For more information on the **Overview** page please refer to:

Patch Success Overview page.

7.1.1.2 Patches page

The **Patches** page shows a full list of patches that are applicable to devices within your estate and you can select an individual patch to view its details. From this page you can also launch the Explorer application with the coverage set to the selected devices.

> **Note**
>
> For more information on the **Patches**, **Patch installations** and **Patch details** page please refer to:

Patch pages.

7.1.1.3 Devices page

The **Devices** page shows a full list of devices within your estate and you can select an individual device to view its details.

> **Note**
>
> For more information on the **Devices**, **Device patches** and **Device details** page please refer to:

Device pages.

7.1.1.4 Monitoring

The Monitoring pages show a full list of instruction history created by Patch Success and you can select individual instruction to view its details.

> **Note**
>
> For more information on the **History**, **Instruction details** and **Responses** page please refer to:

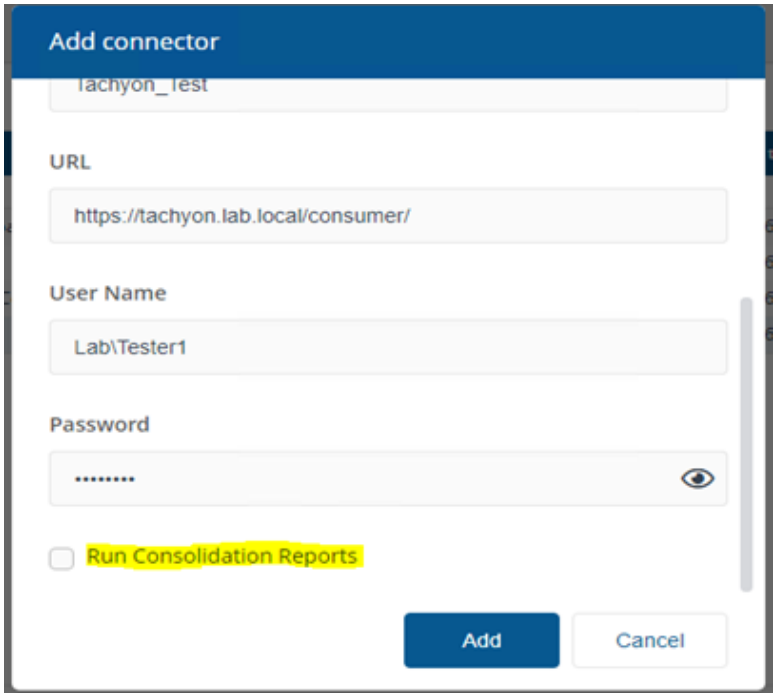
Monitoring pages.

7.2 Quick Start

7.2.1 Connector Usage Recommendations for Patch success customers

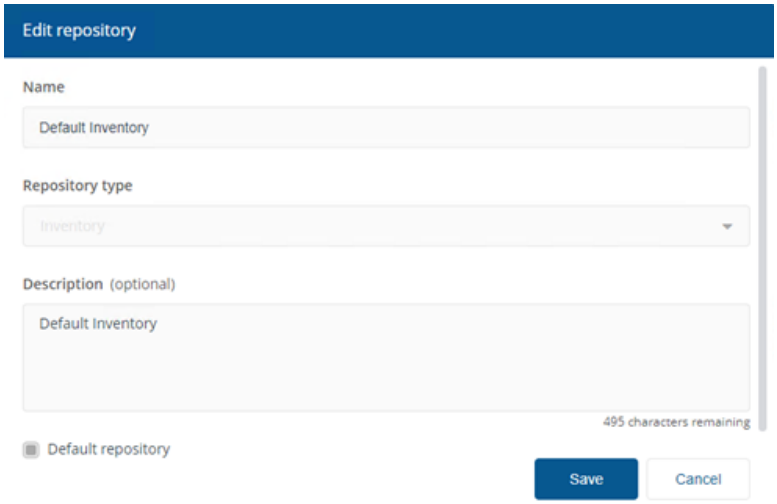
1. Create a connector :-

Create a tachyon connector and while adding connector uncheck the “Run Consolidation Reports” option so that BIC does not get triggered as a part of Sync



2. Select a repository :-

Choose default repository for performing action and If in case user wants to sync it with a different repository then create an inventory type Repository.



3. Execute sync :-

On execute action screen , select the following entities in “Data to sync” category before running the sync.

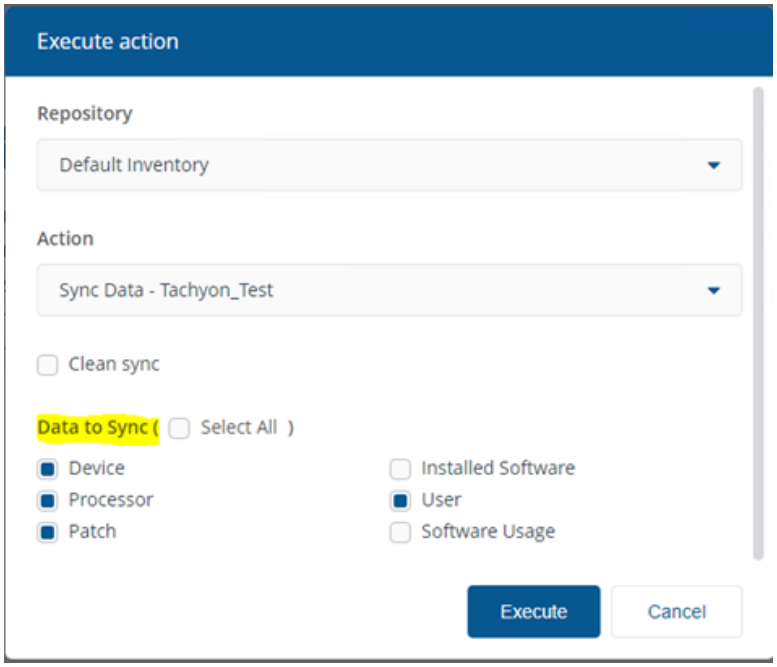
Device

Processor

User

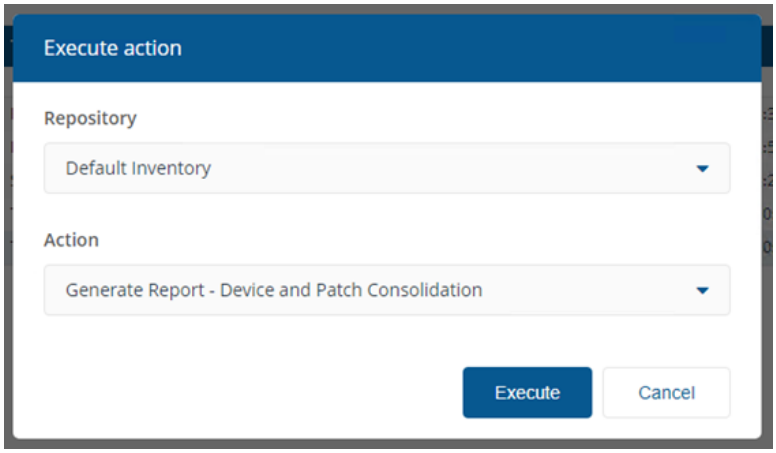
Patch

Sync category will help patch success users to only sync with selected data as they might not be interested for importing the Software Inventory Data.

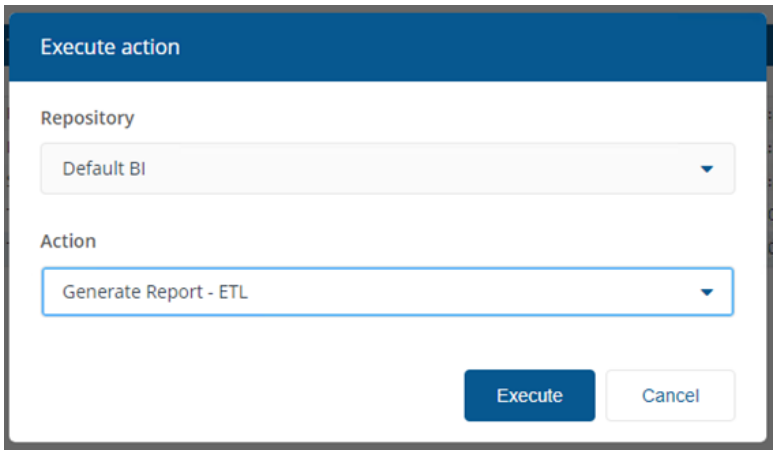


4. Execute consolidation and ETL Report :-

Run only “Device and Patch Consolidation” on execute action screen.



Now again go to execute action screen and Run ETL Report after selecting repository as Default BI.



Note :- In case user has upgraded tachyon from previous version , then run clear data for the repository so that Output record types gets cleared and then execute a fresh sync.

7.3 Implementing Patch Success

Everything you need to know about getting Patch Success installed and running in your network. This section is structured in a way that leads you through the three phases of a typical implementation project.

Design, including requirements

Install

Verify.

7.3.1 Requirements

What you will need to prepare in advance of implementing a Tachyon Server in your network. Typically these are tasks that may take some time to organize, depending on how your organization works.

7.3.1.1 Prerequisites

You will already have installed Patch Success using Tachyon Setup. To do this, you required the following:

A full installation of Tachyon Platform including deployments of clients

A SQL Server Analysis Services (SSAS) instance, preferably on the same server as the SLA databases.

Business Intelligence (BI) selected for installation using Tachyon Setup.

An appropriate Tachyon License to permit using Patch Success and Tachyon connector inventory instructions.

This is normally included in a standard Tachyon license

See Tachyon License details below.

7.3.1.2 Configuration overview

Create an instruction set called **1E Patch Success**, and upload its instructions

Create a custom role called **1E Patch Success Actioners**, assign permissions, assign to All Devices

Configure the **Tachyon connector**, its instruction set **1E Inventory** and custom role **1E Inventory Questioners**

Configure the inventory connector for Configuration Manager (SCCM) or WSUS

Create schedules for the above connectors

7.3.1.3 Configuration requirements

A **domain security group** representing Patch Administrators who will use the Tachyon Patch Success application.

The steps below describe how a Tachyon user will be created for this group, and a role which grants access to the Patch Success pages and instructions.

In our examples this role is called **1E Patch Success Actioners**.

A **domain user account** for use by the Tachyon connector to keep track of the inventory instructions.

The steps below describe how a Tachyon user will be created for this account and used in the configuration of the connector.

In our examples this user is **ACME\SLATACHYON**.

A **domain user account** for you to use, with:

SQL permissions to allow you to run SQL queries which modify the TachyonMaster database. This is required for:

Configuring the source for Patch downloads

Enabling Download only feature

Changing the maximum number of targeted devices

Tachyon roles assigned:

Connector Administrators to configure and test the Tachyon connector

Instruction Set Administrators role to upload the Tachyon Inventory Product Pack instructions and assign them to a new instruction set.

Inventory Administrators role to populate an inventory repository.

Log Viewers role to aid troubleshooting (optional).

Permissions Administrators role to create the **1E Patch Success Actioners** role.

WSUS or **Configuration Manager** (with Software Updates installed) is already implemented. One or both of these are required for:

Adding a connector for Patch meta-data

Configuring the source for Patch downloads

7.3.1.4 Tachyon License details

Ensure your Tachyon License file has the Inventory and PatchSuccess consumers enabled and includes the patterns for **1E-Inventory-*** and **1E-PatchSuccess-***

You can view your Tachyon license details using either of the following methods:

in the Tachyon Portal, navigate to **Settings→Configuration→License information**, look in the **Products** section and expand **Features** and instructions items

in the license file **Tachyon.LIC** found in **C:\ProgramData\1E\Licensing**

If either pattern does not exist, then the corresponding instructions will not run. You may have an old version of Tachyon, or your license needs to be updated.

```
   <Features>
      <Feature name="TachyonPlatform">
        <Consumer name="Inventory" enable="on"> </Consumer>
        <Instructions signersha="F08386A5318A8187D79B0A58253C65CB4E442570" patt
ern="1E-Inventory-*"> </Instructions>
        ...
      </Feature>
      ...
      ...
      <Feature name="PatchSuccess">
        <Consumer name="PatchSuccess" enable="on"> </Consumer>
        <Instructions signersha="F08386A5318A8187D79B0A58253C65CB4E442570" patt
ern="1E-PatchSuccess-*"> </Instructions>
        ...
      </Feature>
      ...
    </Features>
```

7.3.2 Configuring Patch Success

Configuring Patch Success after installation. The procedure below assumes that all users of Patch Success are permitted to see and use the buttons in the Patch Success application. Some guidance is provided for making buttons only available to specific users.

The steps for configuring Patch Success are:

Create an instruction set called **1E Patch Success**, and upload its instructions

Create a custom role called **1E Patch Success Actioners**, assign permissions, assign to All Devices

Configure the **Tachyon connector**, its instruction set **1E Inventory** and custom role **1E Inventory Questioners**

Configure the inventory connector for Configuration Manager (SCCM) or WSUS

Create schedules for the above connectors

7.3.2.1 Creating the 1E Patch Success instruction set and Actioners role

7.3.2.1.1 Creating the 1E Patch Success instruction set

The steps below create an instruction set called **1E Patch Success** and a custom role called **1E Patch Success Actioners.** Users who need to use Patch Success must be assigned to this custom role. The role allows the following:

Access to the Patch Success application and all its pages

Visibility and use of one or more of **Deploy**, **Download only**, **Explore** and **Check Status** buttons in the Patch Success pages, according to the permissions assigned to the role.

The **1E Patch Success** instruction set will contain 3 instructions from the **Patch Success Product Pack** described in the table below.

Instruction text (ReadablePayload)	Type	Description	Instruction file name	Version
<action> patch(es) specified by <patchSpec> identifier(s) from <source> source to targeted device(s) Where: **<action>** is either **Deploy** or **Download only**	Action	Deploys a specific patch or patches to targeted devices. **Note** Unlike the other instructions, the **<patchSpec>** parameter in this instruction does not support **all**. You must be specific which KBs you want to deploy.	**1E-PatchSuccess-Deploy**	5

Instruction text (ReadablePayload)	Type	Description	Instruction file name	Version
<patchSpec> is a list of comma separated GUIDs and/or KB numbers (without KB prefix) of patches to be installed **<source>** is the patch download source: **WSUSR** - Microsoft Update via the Internet **WSUSL** - WSUS **SCCM** - Configuration Manager **Default** - the value of **PatchSuccessSource** in the **GlobalSettings** table of the **TachyonMaster** database, as described in Configuring Patch Success: Configuring the source for Patch downloads.		This instruction is used by the **Deploy** and **Download only** buttons, which allow users to deploy selected patches to devices. The **1E Patch Success Actioners** role requires **Actioner** permissions to see the **Deploy** and the **Download only** buttons. See Patch.Deploy in the Tachyon SDK.		
Returns patch status from <source> for <patchSpec> identifier(s) Where : **<source>** is the patch download source, as above **<patchSpec>** is either **all**, or a list of comma separated GUIDs and/or	Question	Returns patch status for given KB article numbers on targeted devices. The instruction is used by the **Check Status** button, which allow users to check the patch status of the selected patches and represent the results in Explorer for further investigations. The **1E Patch Success Actioners** role requires **Questioner**	**1E-PatchSuccess-Explore**	5

Instruction text (ReadablePayload)	Type	Description	Instruction file name	Version
KB numbers (without KB prefix) of patches to be reported.		permissions to see the **Check Status** button. See Patch.List in the Tachyon SDK.		
Returns patch status from <source> of given<patchSpec> identifier(s) for PatchSuccess consumption Where: **<source>** is the patch download source, as above **<patchSpec>** is either **all**, or a list of comma separated GUIDs and/or KB numbers (without KB prefix) of patches to be reported.	Question	Returns patch status for all known patches on targeted devices. Information is based on offline cache. When run, its response data is offloaded direct to the SLA-BI cube. The instruction is used by the **Update Status** button, which allows users to update the dashboard with the status of selected patches, to see for example **Pending reboot** and **Installed** states. The **1E Patch Success Actioners** role requires **Questioner** permissions to see the **Update status** button. See Patch.List in the Tachyon SDK.	**1E-PatchSuccess-Refresh**	5

Note

Patch Success also requires a further 5 instructions which are included in the **1E Inventory** instruction set created when setting up a Tachyon Connector. You can add a Tachyon Connector later when you get to Configuring connectors and schedules below. If you already have a Tachyon Connector then you need to ensure the **1E-PatchSuccess-PatchStatus** instruction has been added to the **1E Inventory** instruction set.

Click here for more details about 1E Inventory instructions...

The following is an extract from Tachyon connector.

Creating the 1E Inventory instruction set

These steps are only required if:

you have not already loaded the **1E Inventory** Product Pack using the Product Pack Deployment tool as part of the Tachyon Setup process

you will be using **Tachyon Powered Inventory**

The steps show how to create an instruction set called **1E Inventory**.

The **1E Inventory** instruction set will contain the 5 instructions listed in the following table:

Instruction (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
Whic	Ques	Processor details Uses Device.GetProcessors method. **Note**	Proc	**1E-I**	3

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategoryEssor	InstructionfilenameVersion
hprocessors	tion	Click here to expand details of data collected... Method **GetProcessors** Library Core Action Retrieves information about the CPUs plugged in to the	e	**nventory-De**

InstructionContext(ReadablePayload)	Type	Description		DataToSyncCategory	InstructionFilenameVersion
areinthedev			motherboard of the device.		**vice-GetPro**
		Parameters	(None)		
		Return values	*Vendor* (string): The vendor of the processor		
			Name (string): The vendor-defined name of		

InstructionContext(ReadablePayload)	Type	Description		DataToSyncCategory	InstructionfilenameVersion
ice?With			this processor package *CoreCount* (int): The number of cores inside this package *SpeedMhz*(int): The clock speed of the processor		**cessors**

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFilename	Version
aggregator of <lim		in its current operating mode From v5.1 onwards these columns also appear : *LogicalCoreCount* (int) : The number of logical cores			

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFileName	Version
itSecs>seco		inside this package *Hyperthreading* (bool): Indicates whether the cores are hyperthreaded, true for yes, false for no.			

InstructionContext (ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFileName	Version
nds.		Example `Device.GetProcessors();`			
		Platforms Windows Linux MacOS Solaris Intel Solaris Sparc			
		Notes *Name* is the immutable string			

Instruction context (Readable Payload)	Type	Description	DataToSyncCategory	Instruction filename	Version
		that the CPU reports to SMBIOS. This often contains the publicly marketed and sold average speed of the CPU, which usually differs to the actual speed			

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction filename	Version
		of the processor instance. *SpeedMhz* on Windows can change over time for one particular CPU. Modern CPU's can adjust their clock in response to heat and			

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFileName	Version
		power from moment to moment. This parameter cannot be relied upon for scoping future instruction executions unless some kind of range of			

Instruction (Readable Payload)	Type	Description	Data to Sync Category	Instruction file name	Version
		values is in the scope to cope with natural speed variance.			
Inventory	Query	Process Usage data inventory for SLA Uses the $ProcessUsage_Daily inventory table, if **Module.Inventory.ProcessUsage.Enabled** setting is true (default) in the 1E Client configuration file.	Software	**1E-Inve**	3

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFilename	Version
ry-whatisth	on	Please refer to Capture source settings. **Note** Click here to expand details of data collected... Windows only. The following table shows fields available in the **$ProcessUsage_Daily** table.	eUsage	**ntory-FileU**	

esummaryofileusagesince<startDate>?WithastageSummary

Field	Data type	Description	Sample value	Tables
CommandLine	string	This is associated with the command	C:\Program Files\Git\mingw64\libexec\git-core\git-credential-manager.exe	

InstructionontextReadablePayload)	Type	Description	DatatoSynccategory	InstructionfilenameVersion
ggerof<limi		dusedtolaun		

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction filename	Version
tSecs>seconds		chthatainsta			

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFilename	Version
ds.		nce, mostpro			

InstructionContext (ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFilename	Version

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
		stone.ltwil			

Instruction context (Readable Payload)	Type	Description	Instruction contain	Data to Sync category	Instruction filename	Version

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFileName	Version
anydifferen					

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFileName	Version
		cesifotheri			

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFileName	Version
instancesare					

Instruction context (Readable Payload)	Type	Description	Launched with	Data to Sync category	Instruction file name	Version

InstructionContext (ReadablePayload)	Type	Description	hasSlightlyd	DataToSyncCategory	InstructionfilenName	Version

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction filename	Version
		if different com			

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
		and line. Iti			

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFileName	Version
		sanindicati			

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
		onofatypica			

Instruction context (Readable Payload)	Type	Description	DataToSyncCategory	Instruction filename	Version

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction filename	Version
		effort this is ins			

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFilename	Version
Durat	integ	The enu tance.			1

Instruction context (Readable Payload)	Type	Description			Data to Sync category	Instruction filename	Version
		ion	er	mber of minut			

Instruction context (Readable Payload)	Type	Description	Discovered by	Data to Sync category	Instruction filename	Version

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction filename	Version
		the individu			

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
		alexecution			

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction filename	Version
(s) of at least as					

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFilename	Version
		toneinstanc			

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
		e of this exec			

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction filename	Version
		utable. Dura			

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
		tion can never			

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
		r b e m o r e t h a n			

InstructionontextReadablePayload)	Type	Description	DatatoSynccategory	InstructionfilenameVersion
		1440minutes		

InstructionontextReadablePayload)	Type	Description	DatatoSynccategory	InstructionfilenameVersion
		, beingthenu		

InstructionContext(ReadablePayload)	Type	Description	MemberOfMinInstructionCategory	DataToSyncCategory	InstructionFileName	Version

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version

Instruction context (Readable Payload)	Type	Description				Data to Sync category	Instruction filename	Version
executableHa	string	eMD5hashoft	0ae9e8258 2bdf6aa6fd5 811376					

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
sh		hebinarytha			

InstructionText (ReadableText)	Type	Description	DataToSyncCategory	InstructionFileName	Version
tcontainsth					

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
		entry point			

Instruction context (Readable Payload)	Type	Description (usually a name)	Data to Sync category	Instruction file name	Version

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
Executable	string	The name of the git-credential-manager.exe			

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction filename	Version
		IeName of the binary			

Instruction context (Readable Payload)	Type	Description	DataToSyncCategory	Instruction filename	Version
hat contains					

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
		the entry point			

InstructionontextReadablePayload)	Type	Description	DatatoSynccategory	InstructionfilenameVersion
		ntobtainedf		

InstructionontextReadablePayload)	Type	Description	fromstampedv	DatatoSynccategory	Instructionfilename	Version

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFilename	Version

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
		mation where			

Instruction context (Readable Payload)	Type	Description	DataToSyncCategory	Instruction filename	Version
		possible, th			

Instruction context (Readable Payload)	Type	Description	DataToSyncCategory	Instruction filename	Version

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFilename	Version
Executa	integ	Thesize not.	131168		

InstructionontextReadablePayload)	Type	Description	DatatoSynccategory	Instructionfilename	Version
bleSize	er	ofthebinary			

InstructionontextReadablePayload)	Type	Description	DatatoSynccategory	InstructionfilenameVersion
		thatishashe		

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
		db below			
Execu	stri	The ve			1.5.0.0

Instruction context (Readable Payload)	Type	Description	DataToSyncCategory	Instruction filename	Version
tableVersioning		Version information			

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction filename	Version
	on	ation stamp e			

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFilename	Version
		dintothheexe			

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFilename	Version
		cutablewher			

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
		available.			

InstructionContext (ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFileName	Version
ExecutionCo	integer	The number of			2

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction filename	Version
	unt	instancesob			

InstructionContext(ReadablePayload)	Type	Description	DataToSynccategory	InstructionfilenameVersion
servedduri n				

InstructionontextReadablePayload)	Type	Description	gtheDuratio	DatatoSynccategory	InstructionfilenameVersion

Instruction context (Readable Payload)	Type	Description				Data to Sync category	Instruction file name	Version

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
		Process ger ueof1indica			

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFileName	Version
		test that this			

Instruction context (Readable Payload)	Type	Description	isCategoris	DataToSyncCategory	InstructionfileName	Version

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFileName	Version
		easanopera			

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFilename	Version
		tingsystemb			

InstructionontextReadablePayload)	Type	Description	DatatoSynccategory	InstructionfilenameVersion
		ytherulesin		

InstructionContext(ReadableParyload)	Type	Description	DatatoSyncccategory	InstructionfilenameVersion
		placee.Avalu		

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFileName	Version
eof0indicat					

InstructionContext(ReadablePayload)	Type	Description	DataToSynccategory	InstructionfilenameVersion
estthatitisn				

Instruction context (Readable Payload)	Type	Description	DataToSyncCategory	Instruction filename	Version

InstructionContext (ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFileName	Version
		en mestampofwh			

InstructionontextReadablePayload)	Type	Description	DatatoSynccategory	InstructionfilenameVersion
		entheelastin		

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
		stance of the e			

Instruction context (Readable Payload)	Type	Description	DataToSyncCategory	Instruction filename	Version
executable(					

InstructionontextReadablePayload)	Type	Description	DatatoSynccategory	InstructionfilenameVersion
		ofallltheacc		

InstructionContext (ReadablePayload)	Type	Description	DataToSynccategumulatedsub	DataToSynccategory	InstructionfilenameVersion

InstructionontextReadablePayload)	Type	Description	DatatoSynccategory	InstructionfilenameVersion
		jectsofthis		

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFileName	Version
		record) was l			

Instruction context (Readable Payload)	Type	Description	Last seen (pol	Data to Sync category	Instruction file name	Version

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFilename	Version
		ling)oractu			

InstructionontextReadablePayload)	Type	Description	allyexited(	DatatoSynccategory	Instructionfilename	Version

InstructionContext(ReadableParyload)	Type	Description	DatatoSyncCategory	InstructionfilenameVersion
		events). Whi		

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction filename	Version
		Install any insta			

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFilename	Version
nceisrunnin					

InstructionontextReadablePayload)	Type	Description	DatatoSynccategory	InstructionfilenameVersion
		g, forthecur		

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFilename	Version
		rentdayreco			

Instruction context (Readable Payload)	Type	Description	DataToSyncCategory	Instruction filename	Version
		rds, LastSee			

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction filename	Version
		new will create a pa			

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
		cross the day			

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
		and duration			

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
		will increas			

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFileName	Version
estimepass					

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFilename	Version
		esifthepproc			

Instruction context (Readable Payload)	Type	Description	DataToSyncCategory	InstructionFilename	Version
esstremainsr					

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFilename	Version
		running. Once			

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFileName	Version

InstructionContext(ReadableParyload)	Type	Description	DatatoSynccategory	InstructionfilenameVersion
		rossedthent		

Instruction context (Readable Payload)	Type	Description	DataToSyncCategory	Instruction file name	Version
		hedailyreco			

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
rds forryeste					

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
rdayare' clo					

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
		sed off-by se			

Instruction context (Readable Payload)	Type	Description	tting Last Se	Data to Sync category	Instruction file name	Version

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
		en=TS+86400			

InstructionontextReadablePayload)	Type	Description	(thenumbero	DatatoSynccategory	InstructionfilenameVersion

Instruction context (Readable Payload)	Type	Description	DatatoSynccategory	Instruction filename	Version
		fseconds in a			

InstructionontextReadablePayload)	Type	Description	DatatoSynccategory	Instructionfilename	Version
		day), whichi			

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
		smidnight of			

InstructionontextReadablePayload)	Type	Description	DatatoSynccategory	InstructionfilenameVersion
		thenextday.		

Instruction context (Readable Payload)	Type	Description	DataToSyncCategory	Instruction filename	Version
If all instan					

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
		cesofonebin			

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFilename	Version
array are excite					

InstructionContext (ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFileName	Version
		dandneverru			

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFilename	Version
managainthatd					

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction filename	Version
		ay, the entheL			

InstructionContext(ReadablePayload)	Type	Description	lastSeenfiel	DatatoSynccategory	Instructionfilename	Version

InstructionontextReadablePayload)	Type	Description	DatatoSynccategory	InstructionfilenameVersion
dforthatdai				

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFilename	Version
		lyrecordsho			

Instruction context (Readable Payload)	Type	Description	DataToSyncCategory	Instruction filename	Version
uld'stick'a					

InstructionontextReadablePayload)	Type	Description	DatatoSynccategory	InstructionfilenameVersion
		tonevaluean		

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version

InstructionontextReadablePayload)	Type	Description	DatatoSynccategory	InstructionfilenameVersion
		hangeagain.		

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction filename	Version
In other word					

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFilename	Version
		sthemaximum			

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFileName	Version
		differenceb			

InstructionContext(ReadableParyload)	Type	Description	DatatoSyncccategory	InstructionfilenameVersion
		etweenTSand		

InstructionContext(ReadablePayload)	Type	Description	LastSeenIna	DataToSyncCategory	InstructionFilename	Version

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFilename	Version
		singlerowis			

InstructionContext(ReadableParyload)	Type	Description	DatatoSyncccategory	InstructionfilenameVersion
		atmost8640000		

InstructionContext (ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFilename	Version
		, being the menu			

InstructionontextReadablePayload)	Type	Description	mberoffseconn	DatatoSynccategory	Instructionfilename	Version

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
		dsinaday. Tr			

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
		acking of ane			

InstructionContext(ReadablePayload)	Type	Description	ExecutionSum	DataToSyncCategory	InstructionFileName	Version

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version

InstructionontextReadablePayload)	Type	Description	DatatoSynccategory	InstructionfilenameVersion
		daytoanothe		

Instruction context (Readable Payload)	Type	Description	DataToSyncCategory	Instruction filename	Version
r("carry-ov					

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFileName	Version
		er") can be ac			

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
		hieved by loo			

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFilename	Version
		kingforarec			

InstructionontextReadablePayload)	Type	Description	DatatoSynccategory	InstructionfilenameVersion
ordbasedonT				

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFilename	Version
Stomorrow=L					

InstructionContext(ReadablePayload)	Type	Description	lastSeentoda	DatatoSynccategory	Instructionfilename	Version

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
y with all the					

InstructionontextReadablePayload)	Type	Description	otherkeyinf	DatatoSynccategory	Instructionfilename	Version

InstructionontextReadablePayload)	Type	Description	DatatoSynccategory	InstructionfilenameVersion
		ormationthe		

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFilename	Version
		same. If that			

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFilename	Version
exactkeyrec					

InstructionontextReadablePayload)	Type	Description	DatatoSynccategory	InstructionfilenameVersion
		ordwiththhe'		

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFilename	Version
		carryover' c			

InstructionContext(ReadablePayload)	Type	Description	Conditions	DataToSyncCategory	InstructionFilename	Version

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
not found the					

InstructionontextReadablePayload)	Type	Description	DatatoSynccategory	InstructionfilenameVersion
		ntheprocess		

InstructionontextReadablePayload)	Type	Description	DatatoSynccategory	InstructionfilenameVersion
		didnottheor		

Instruction context (Readable Payload)	Type	Description	Data to Synchronically	Data Category	Instruction filename	Version

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFilename	Version
		tinueacross			

InstructionontextReadablePayload)	Type	Description	midnight.No	DatatoSynccategory	InstructionfilenameVersion

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFilename	Version
		tethatapproc			

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
		estsdies			

InstructionontextReadablePayload)	Type	Description	DatatoSynccategory	InstructionfilenameVersion
after23:59:				

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction filename	Version
00 and starts					

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
before001					

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFilename	Version
:00thenext d					

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
		rt to be a conti			

InstructionontextReadablePayload)	Type	Description	DatatoSynccategory	Instructionfilename	Version
		nuousproces			

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFilename	Version
		sinthesumma			

Instruction context (Readable Payload)	Type	Description	DataToSyncCategory	Instruction filename	Version
		rytables.Ev			

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
		enthoughtic			

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFilename	Version
		ouldthisoret			

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
		ically always			

Instruction context (Readable Payload)	Type	Description	DataToSyncCategory	Instruction filename	Version
		topped for ne			

InstructionontextReadablePayload)	Type	Description	DatatoSynccategory	InstructionfilenameVersion
		arlytwominu		

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFilename	Version
		test.Thisisb			

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFilename	Version
		ecausethere			

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
		solution of t			

InstructionContext(ReadableStepsPayload)	Type	Description	DataToSyncCategory	InstructionFileName	Version

InstructionontextReadablePayload)	Type	Description	DatatoSynccategory	InstructionfilenameVersion
		thestartoft		

InstructionontextReadablePayload)	Type	Description	DatatoSynccategory	InstructionfilenameVersion
		hemiinutethe		

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
		event to occurr			

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction filename	Version
TS	integ	When edin.	1526947200		

Instruction context (Readable Payload)	Type	Description	DataToSyncCategory	Instruction filename	Version
er	er	recordwasa			

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
		added to the eta			

InstructionontextReadablePayload)	Type	Description	DatatoSynccategory	Instructionfilename	Version
ble.SeeTime					

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFilename	Version
		stamps.Midn			

InstructionontextReadablePayload)	Type	Description	DatatoSynccategory	Instructionfilename	Version
		ightUTCthat			

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFileName	Version
isthestartd					

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction filename	Version
ayofthe24ho					

Instruction context (Readable Payload)	Type	Description	urscovered by	Data to Sync category	Instruction filename	Version

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction filename	Version
		y this is record			

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFileName	Version
		d. The Tachyon client captures executable usage; this is from the moment the executable is turned into a process, hence the process usage. The Process Usage data presented is grouped by executable binary, and parallel runs are accumulated in the ExecutionCount, but			

Instruction	Type	Description	Data to Sync Category	Instruction filename	Version
		not in the Duration, where coverage time period is desired instead.			
Inventory	Question	Software inventory for SLA Uses a combination of: Software.GetInstallations method Software.GetUserInstallations method SQL Server registry values **Note**	Installed	**1E-Inventent**	3

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction filename	Version
-whatsoftwa		Click here to expand details of data collected... Method: **GetInstallations** Module: Software Library: Core Action: Gets a list of the installed software	Software	**ory-Softwa**	

InstructionContext(ReadableRequestPayload)	Type	Description		DataToSyncCategory	InstructionFilename	Version
reisinstall			available to all users, optionally filtered by product and/or publisher. *Product* (string; optional): If specified, search for just this product.		**re**	
		Parameters				

InstructionContext (ReadablePayload)	Type	Description		DataToSyncCategory	InstructionFilename	Version
edWithasta			*Publisher* (string; optional): If specified, get just this publisher's software.			
		Return values	A table of:			
			Product (string): The product name.			

InstructionContext (ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFilename	Version
ggerof<limi		*Publisher* (string): The publisher of the product. *Version* (string): The version of the product. *InstallDate* (string): If available, when the product was installed. *Architecture* (string): Platform architecture of			

Instruction	Context (Readable Payload)	Type	Description		Data to Sync category	Instruction filename	Version

tSecs>secon		Example	this installation (e.g. x86, x64)
			Get all software:
			`Software.GetInstallations();`
			Find and remove all installed instances of Calculator Plus:
			`Software.GetInstallations( Publisher : "Microsof`				

Instruction context (Readable Payload)	Type	Description		Data to Sync category	Instruction filename	Version
ds.			t", Product : "Microsoft Calculator Plus"); evaluate; Agent.Echo(Message: "Is installed"); Software.Uninstall(Publisher : "Microsoft", Product : "Microsoft Calculator Plus"); To select a specific version, use a SQL WHERE clause:			

InstructionContext(ReadablePayload)	Type	Description		DataToSyncCategory	InstructionFilename	Version
			@installs = Software.GetInstallations(Publisher : "Microsoft", Product : "Office Professional"); SELECT DISTINCT * FROM @installs WHERE Version LIKE "16.0%";			
		Platforms	Windows Linux			

Instruction context (Readable Payload)	Type	Description	DataToSyncCategory	Instruction filename	Version
		MacOS Solaris Intel Solaris Sparc Android			
		Notes: To find additional software installed for specific users, use Software.GetUserInstallations.			

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
Method		**GetUserInstallations**			
Li		Core			

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFilename	Version
	b r a r y				
	A c t i	Gets a list of the software installed for specific users, optionally filtered by product and/or publisher.			

InstructionContext (ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFileName	Version
	Parameter	*Product* (string; optional): If specified, search for just this product. *Publisher* (string; optional): If specified, get just this publisher's software.			

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
	Returns	A table of: *Architecture* (string): Platform architecture of this installation (e.g. x86, x64)			

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFilename	Version
	uses	*InstallDate* (string): If available, when the product was installed. *Product* (string): The product name. *Publisher* (string): The publisher of the product. *Sid* (string): The user identifier for whom this software has been installed.			

InstructionContext (ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFilename	Version
		Username (string): Friendly representation of the *Sid* - this will only be resolved locally. *Version* (string): The version of the product.			
	Example	Get all user specific software: `Software.GetUserInstallations();`			

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
	Ie Platfor	Windows			

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFilename	Version
	ms				
	Notes	*Sid* resolution may fail as this method will not go over the wire. In this case Username will be NULL.			
		The file modified and accessed time attributes of the NTUSER.dat directory entries under the %USERPROFILE%			

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFilename	Version
		folder for each user and service principal might be updated to some time during the execution of this method. This is a side effect of loading and unloading the user hive and is housekeeping performed by Windows, not the 1E Client. This can cause "unused" profiles to appear to be used if the modified times are			

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction filename	Version
		employed to determine whether a user has logged in, which is not a reliable method of establishing this fact. This method reads user uninstall registry keys from HKU, but will not load hives. Installs for this function are retrieved from *HKU:\<SID>\Software\Micro*			

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
		soft\Windows\CurrentVersion\Uninstall			
Inventory	Question	User data inventory for SLA Uses the **$UserUsage_Daily** inventory table, if **Module.Inventory.UserUsage.Enabled** setting is true (default) in the 1E Client configuration file. Top Console User is also calculated from this table. Please refer to Capture source settings.	User	**1E-Invent**	3

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFilename	Version
-summaryofw		**Note** Click here to expand details of data collected... Windows only. The following table shows fields available in the **$UserUsage_Daily** table.		**ory-UserUsa**	

hichusershavelloggedonsince<startDate>?Withasgesummary

Field	Datatype	Description	Sample value	Tables
Duration	integer	The number of minutes covered by the in	12	$User Usage_Daily

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
tagger of <li		dividual use			

Instruction context (Readable Payload)	Type	Description	DataToSyncCategory	Instruction filename	Version
mitSecs>sec		rsession(s)			

InstructionontextReadablePayload)	Type	Description	DatatoSynccategory	Instructionfilename	Version
onds.		ofatleaston			

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFilename	Version
		eInstanceof			

InstructionontextReadablePayload)	Type	Description	DatatoSynccategory	InstructionfilenameVersion
		thisloogin.		

InstructionontextReadablePayload)	Type	Description	Duration	DatatoSynccategory	InstructionfilenameVersion

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFilename	Version
neverbemore					

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction filename	Version
		than 1440 min			

Instruction context (Readable Payload)	Type	Description	Data to Sync categories, being	Instruction file name	Version

InstructionontextReadablePayload)	Type	Description	DatatoSynccategory	InstructionfilenameVersion
	henumberofm			

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
		inutes in ada			

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction filename	Version
Email	string	The email address.	$User Usage_Daily		

InstructionContext (ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFileName	Version

InstructionontextReadablePayload)	Type	Description	DatatoSynccategory	InstructionfilenameVersion
		scachedinth		

Instruction context (Readable Payload)	Type	Description	DataToSyncCategory	Instruction filename	Version
		esystemfort			

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
		his user. Thi			

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
		smaynotnece			

InstructionContext(ReadableParyload)	Type	Description	DatatoSynccategory	InstructionfilenameVersion
		ssarilybeth		

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
email address					

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
		ss to use to co			

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFilename	Version
ntactthheuse					

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
		rviacorpora			

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction filename	Version
		team mail. The			
	Fir	str	Ali	$User Us	

InstructionontextReadablePayload)	Type	Description	DatatoSynccategory	InstructionfilenameVersion
stName	ing	forenamethatce	age_Daily	

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
t t h e s y s t e m h					

InstructionontextReadablePayload)	Type	Description	DatatoSynccategory	InstructionfilenameVersion
		ascachedfor		

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction filename	Version
		the user.			
	Last	str	The	Bro	$User Us

Instruction context (Readable Payload)	Type	Description	DataToSyncCategory	Instruction filename	Version
		tName ing surnamethat wn age_Daily			

InstructionContext(ReadablePayload)	Type	Description	DataToSynccCategory	InstructionfilenameVersion
		thesystemha		

InstructionontextReadablePayload)	Type	Description	DatatoSynccategory	Instructionfilename	Version
		scachedfort			

Instruction context (Readable Payload)	Type	Description					Data to Sync category	Instruction filename	Version
			heuser						
		LastS	integ	TheUT	15269	$User Usage_			

Instruction context (Readable Payload)	Type	Description					Data to Sync category	Instruction filename	Version
		een	er	CTimestampo	90846	Daily			

InstructionContext(ReadablePayload)	Type	Description	fwhenthelas	DatatoSynccategory	Instructionfilename	Version

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFilename	Version
		instanceof			

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
		the user sess			

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFileName	Version
		ion(ofallth			

Instruction context (Readable Payload)	Type	Description	Accumulate	Data to Sync category	Instruction file name	Version

Instruction context (Readable Payload)	Type	Description	DataToSyncCategory	Instruction filename	Version
dsubjectsof					

InstructionontextReadablePayload)	Type	Description	DatatoSynccategory	InstructionfilenameVersion
		thisrecord)		

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction filename	Version
was last seen					

InstructionontextReadablePayload)	Type	Description	DatatoSynccategory	InstructionfilenameVersion
		(pollingor		

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
		actually exi			

InstructionontextReadablePayload)	Type	Description	DatatoSynccategory	InstructionfilenameVersion
		ted(events)		

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
, rounded down					

Instruction context (Readable Payload)	Type	Description	DataToSyncCategory	InstructionFilename	Version
not the start					

InstructionContext(ReadableParyload)	Type	Description	DatatoSynccategory	InstructionfilenameVersion
		oftheminute		

InstructionontextReadablePayload)	Type	Description	DatatoSynccategory	InstructionfilenameVersion
		inwhichtheee		

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction filename	Version
		vent to occurre			

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction filename	Version
		d. While stany			

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
		session ins			

InstructionontextReadablePayload)	Type	Description	DatatoSynccategory	InstructionfilenameVersion
		progress,fo		

InstructionontextReadablePayload)	Type	Description	DatatoSynccategory	Instructionfilename	Version
		rthecurrent			

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
		days records,			

InstructionontextReadablePayload)	Type	Description	LastSeenwil	DatatoSynccategory	Instructionfilename	Version

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction filename	Version
		Icreepacros			

InstructionontextReadablePayload)	Type	Description	DatatoSynccategory	InstructionfilenameVersion
		sthedayandt		

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFileName	Version
		hedurationw			

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFilename	Version

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction filename	Version

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFileName	Version
sifthheuserr					

InstructionontextReadablePayload)	Type	Description	DatatoSynccategory	InstructionfilenameVersion
		emainslogge		

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFilename	Version
		din.ThatisD			

Instruction context (Readable Payload)	Type	Description	Duration and L	Data to Sync category	Instruction filename	Version

Instruction context (Readable Payload)	Type	Description	DataToSyncCategory	InstructionFilename	Version
		lastSeenwill			

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction filename	Version
		increase eac			

InstructionontextReadablePayload)	Type	Description	DatatoSynccategory	Instructionfilename	Version
		htimeyouque			

InstructionontextReadablePayload)	Type	Description	DatatoSynccategory	InstructionfilenameVersion
rythetable(				

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction filename	Version
		with at least			

Instruction context (Readable Payload)	Type	Description	DataToSyncCategory	Instruction filename	Version
		aminutebetw			

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFilename	Version
eenqueries					

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFilename	Version
).OnceMidni					

InstructionContext(ReadablePayload)	Type	Description	DataToSynccategory	InstructionfilenameVersion
		ghtisscrosse		

InstructionontextReadablePayload)	Type	Description	DatatoSynccategory	InstructionfilenameVersion
		dtheentthedai		

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
		Iy records fo			

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
		registeredaya			

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
		're' closed of			

Instruction context (Readable Payload)	Type	Description	DataToSyncCategory	Instruction filename	Version
'bysetting					

InstructionContext(ReadablePayload)	Type	Description	LastSeen=TS	DataToSyncCategory	InstructionFilename	Version

InstructionontextReadablePayload)	Type	Description	DatatoSynccategory	InstructionfilenameVersion
		+864000(then		

Instruction context (Readable Payload)	Type	Description	Number of seco	Data to Sync category	Instruction file name	Version

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFilename	Version
ndsinaday),					

InstructionContext (ReadablePayload)	Type	Description	which is mid	DataToSyncCategory	InstructionFilename	Version

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
		right of the ene			

InstructionontextReadablePayload)	Type	Description	DatatoSynccategory	InstructionfilenameVersion
xtday.Ifall				

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
		user session			

Instruction context (Readable Payload)	Type	Description	DataToSyncCategory	Instruction filename	Version
nsforroneuse					

InstructionontextReadablePayload)	Type	Description	DatatoSynccategory	Instructionfilename	Version
		rareexitteda			

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFileName	Version
endneverrocu					

InstructionContext (ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFileName	Version
		ragaintthatd			

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
		ay, then the L			

Instruction context (Readable Payload)	Type	Description	lastSeenfiel	DatatoSyncCategory	InstructionfilenameVersion

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFileName	Version
		dfor thatdai			

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
lyrecordsho					

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction filename	Version
uld'stick'a					

Instruction context (Readable Payload)	Type	Description	DataToSyncCategory	Instruction filename	Version
		tonevaluean			

InstructionontextReadablePayload)	Type	Description	DatatoSynccategory	InstructionfilenameVersion
dneverercevercc				

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
		hangeagain.			

Instruction context (Readable Payload)	Type	Description	Inotherword	Data to Sync category	Instruction file name	Version

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFilename	Version
		sthemaximum			

InstructionontextReadablePayload)	Type	Description	DatatoSynccategory	Instructionfilename	Version
		differenceb			

InstructionontextReadablePayload)	Type	Description	DatatoSynccategory	InstructionfilenameVersion
etweenTSand				

InstructionContext(ReadablePayload)	Type	Description	LastSeenIna	DataToSyncCategory	InstructionfilenameVersion

InstructionontextReadablePayload)	Type	Description	DatatoSynccategory	Instructionfilename	Version
		singlerowis			

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction filename	Version
		atmost8640 0			

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFilename	Version
		, being the menu			

Instruction context (Readable Payload)	Type	Description	member of section	Data to Sync category	Instruction file name	Version

InstructionontextReadablePayload)	Type	Description	DatatoSynccategory	InstructionfilenameVersion
dsinaday.Tr				

InstructionontextReadablePayload)	Type	Description	DatatoSynccategory	InstructionfilenameVersion
		ackingofaus		

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
		ersessionsu			

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFilename	Version
		mmaryfromon			

InstructionontextReadablePayload)	Type	Description	DatatoSynccategory	InstructionfilenameVersion
edaytoanoth				

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction filename	Version
		er("carry-o			

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFilename	Version
		ver") can be a			

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
		chieved by lo			

InstructionontextReadablePayload)	Type	Description	DatatoSynccategory	InstructionfilenameVersion
		okingforare		

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFilename	Version
		cordbased on			

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFilename	Version
TS tomorrow=					

InstructionContext(ReadablePayload)	Type	Description	LastSeen	DataToSyncCategory	InstructionFilename	Version

InstructionontextReadablePayload)	Type	Description	DatatoSynccategory	Instructionfilename	Version
		ay with all th			

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
		other key in			

InstructionContext(ReadablePayload)	Type	Description	format	DataToSyncCategory	InstructionFilename	Version

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFileName	Version
		esame.Ifthea			

Instruction context (Readable Payload)	Type	Description	DataToSyncCategory	Instruction filename	Version
	texactkeyre				

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
		cord with the			

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFilename	Version
'carryover'					

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFilename	Version
conditionsi					

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
		snot found th			

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction filename	Version
		enthe user see			

InstructionontextReadablePayload)	Type	Description	DatatoSynccategory	InstructionfilenameVersion
		ssiondidnot		

InstructionontextReadablePayload)	Type	Description	DatatoSynccategory	Instructionfilename	Version
		theoretical			

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFileName	Version
lycontinuea					

InstructionContext(ReadablePayload)	Type	Description	DataToSynccategory	InstructionfilenameVersion
crossmidnig				

InstructionontextReadablePayload)	Type	Description	DatatoSynccategory	Instructionfilename	Version
		ht.Notethat			

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFileName	Version
		assessiontha			

InstructionontextReadablePayload)	Type	Description	DatatoSynccategory	Instructionfilename	Version
		textitsafter			

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
		23:59:00 and			

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFilename	Version
startsagain					

InstructionontextReadablePayload)	Type	Description	DatatoSynccategory	Instructionfilename	Version
before001					

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFileName	Version
:00thenextd					

InstructionontextReadablePayload)	Type	Description	DatatoSynccategory	Instructionfilename	Version
		aywillappea			

InstructionontextReadablePayload)	Type	Description	DatatoSynccategory	InstructionfilenameVersion
rtobeacontai				

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFileName	Version
		nuoususerse			

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction filename	Version
session in these					

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
		summary table			

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFilename	Version
		s. Eventhoug			

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
		hit could the			

InstructionontextReadablePayload)	Type	Description	DatatoSynccategory	InstructionfilenameVersion
		oreticallyh		

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction filename	Version
		edf or nearly			

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction filename	Version
		two minutes.			

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
		This is because			

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFilename	Version
		setheresolu			

InstructionontextReadablePayload)	Type	Description	DatatoSynccategory	InstructionfilenameVersion
		tionoftheta		

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
		bleistothes			

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFilename	Version
startoftheminute					

InstructionontextReadablePayload)	Type	Description	DatatoSynccategory	InstructionfilenameVersion
nutethheeven				

Instruction context (Readable Payload)	Type	Description	Data to Sync occurred in	Data to Sync category	Instruction filename	Version

InstructionContext(ReadableJson)	Type	Description	DataToSyncCategory	InstructionFilename	Version
n.SeeTimest					

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction filename	Version
SID	stri	The Win amps.	S-1-5-	$User Usage_	

Instruction context (Readable Payload)	Type	Description	DataToSyncCategory	Instruction filename	Version
ng	dowsNTSIDof	21-xxxx-yyyy-	Daily		

Instruction context (Readable Payload)	Type	Description					DataToSyncCategory	Instruction filename	Version
			the user.	zzz					
	TS	int	Whe	152	$User				

Instruction context (Readable Payload)	Type	Description				Data to Sync category	Instruction filename	Version
			eger	nthereco rdw	6947200	age_Daily		

InstructionontextReadablePayload)	Type	Description	DatatoSynccategory	Instructionfilename	Version
		asaddedtoth			

InstructionontextReadablePayload)	Type	Description	DatatoSynccategory	InstructionfilenameVersion
etableSeeT				

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFileName	Version
		timestamps.			

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction filename	Version
Username	string	The user account	alicebacme\	$User Usage_Daily	

InstructionContext (ReadablePayload)	Type	Description			DataToSyncCategory	InstructionFilename	Version
			untname, with	AliceBrown			

InstructionContext(ReadablePayload)	Type	Description	hadomainpre	DatatoSynccategory	Instructionfilename	Version

InstructionontextReadablePayload)	Type	Description	DatatoSynccategory	Instructionfilename	Version
		fixifapplic			

InstructionontextReadablePayload)	Type	Description	DatatoSynccategory	Instructionfilename	Version
		ableeForWin			

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction filename	Version
		dows devices			

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
		not a in a doma			

InstructionontextReadablePayload)	Type	Description	DatatoSynccategory	InstructionfilenameVersion
		in,the'doma		

InstructionontextReadablePayload)	Type	Description	DatatoSynccategory	Instructionfilename	Version
in'isthelloc					

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction filename	Version
		almachinena			

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
		me. For non-W			

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFileName	Version
		indowsdevic			

Instruction context (Readable Payload)	Type	Description	esSuchHasLin	DataToSyncCategory	InstructionFilename	Version

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFileName	Version
uxthereisno					

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFilename	Version
domainpart.					

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
		The Tachyon client captures user sessions (usage); this is from the moment the user instigates a login/logout, hence User Usage. The usage data presented is grouped by SID and Username, and parallel login durations are really the coverage of the time period, not the total time for all the individual sessions. User and administrator accounts are included, either local or remote. System			

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFileName	Version
		accounts, and accounts used to run services, are excluded.			
Returnspa	Question	Returns patch status for 1E Inventory consumption	Patch	**1E-PatchS**	5.0

InstructionontextReadablePayload)	Type	Description	DatatoSynccategory	Instructionfilename	Version
tchstatusfo				**uccesss-Patc**	

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
r1EInventor				**hStatus**	

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
yconsumptio					

Instruction, staggering	Type	Description	Data to Sync category	Instruction filename	Version

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
gfor<limits					

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
ecs>second					

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
s. Tip The **1E-**					

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
PatchSuccess					

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
s-PatchStat					

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFilename	Version
usinstructi					

InstructionontextReadablePayload)	Type	Description	DatatoSynccategory	InstructionfilenameVersion
onisnotrequ				

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
ired if you do					

InstructionontextReadablePayload)	Type	Description	DatatoSynccategory	Instructionfilename	Version
notintendto					

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
use the Patch					

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
Succes sappl					

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFilename	Version
ication, and					

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
will in not run i					

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
f you do not ha					

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
vealicensef					

InstructionontextReadablePayload)	Type	Description	DatatoSynccategory	InstructionfilenameVersion
orPatchSucc				

InstructionontextReadablePayload)	Type	Description	DatatoSynccategory	InstructionfilenameVersion
essForemore				

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
information					

InstructionontextReadablePayload)	Type	Description	DatatoSynccategory	Instructionfilename	Version
aboutconfig					

InstructionontextReadablePayload)	Type	Description	DatatoSynccategory	InstructionfilenameVersion
uringPatchS				

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
ucc ess pl eas					

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction filename	Version
[Conf](#)					

InstructionontextReadablePayload)	Type	Description	DatatoSynccategory	Instructionfilename	Version
igguringPatchS					

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFilename	Version
[uccess](). **Warni**					

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFileName	Version
ng					
This instr					

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFilename	Version
uctionispar					

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
1E I					

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction filename	Version
nventory ins					

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFilename	Version
InstructionSet					

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
used by the Ta					

InstructionontextReadablePayload)	Type	Description	DatatoSynccategory	Instructionfilename	Version
chyonConnec					

InstructionontextReadablePayload)	Type	Description	DatatoSynccategory	InstructionfilenameVersion
tor.Donotmo				

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
vei to the **1E**					

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
Patch					
Succ					

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
ess instruct					

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
ions set used b					

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFilename	Version
ythebuttons					

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFilename	Version
visibleinth					

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFilename	Version
ePatchSuccess					

InstructionContext(ReadablePayload)	Type	Description	DataToSyncCategory	InstructionFileName	Version
ssapplicati					

Instruction context (Readable Payload)	Type	Description	Data to Sync category	Instruction file name	Version
on.					

Tip

You can use the Product Pack Deployment tool to simultaneously Upload the instructions and Create the Instruction set, or use the manual steps below.

These instructions are included in the **1E Inventory** product pack, available in the **TachyonPlatform.v5.x.x.x.zip** file downloaded from the 1E Support Portal.

First upload the Patch Success instructions:

Download the **TachyonPlatform.v5.x.x.x.zip** file from the 1E Support Portal

Extract the **1E-PatchSuccess.zip** from the Classic folder

Logon to the Tachyon Portal using a Tachyon user account with the **Permissions Administrators** and **Instructions Administrators** roles

Open the **Settings** application

Navigate to the **Settings**→**Instructions**→**Instruction sets** page

Click on the **Upload** button

In the Open dialog navigate to the location of the **1E-PatchSuccess.zip** file

Select **1E-PatchSuccess.zip** and click **Open**.

All the instructions contained in the zip file will initially be added to the default **Unassigned** instruction set. Instructions in the **Unassigned** instruction set cannot be used, so you will need to add the instructions to a new instruction set:

Select the **3** instructions you want to add to the new set, by clicking the checkbox at the start of each instruction row in the list

Click the **Add new set** button in the button panel to the right of the page

In the **Add new instruction set** popup subsequently displayed, type **1E Patch Success** as the name

Optionally select a **custom icon** file

Ensure that the **Include 3 selected instructions** checkbox is checked

Click the **Add** button to add the new instruction set, with the selected instructions.

7.3.2.1.2 Creating the 1E Patch Success Actioners role

You must create the **1E Patch Success Actioners** role so that its member users can use all features of Patch Success, including buttons which cause instructions to run in Explorer. Instructions are configured in Creating the 1E Patch Success instruction set above.

> **Tip**
>
> Some **1E Patch Success** instructions are actions which require approval. Users cannot approve their own actions, but members of this role can approve each others actions. If you prefer other users or security groups to have **Approver** permissions, they would need an additional custom role, for example called **1E Patch Success Approvers**. Or you may use an existing approvers role and assign the **1E Patch Success** instruction set to it. Ensure the selected role has the **All Devices** management group assigned to it.
>
> The built-in (system) role **Patch Success Viewers** can be used for users who only need to view the Patch Success screens and dashboard with no access to any buttons.

To create a new user:

Navigate to the **Settings→Permissions→Users** page.

Click the **Add** button to start the add user process.

In the **Add user** popup subsequently displayed in the **Select user** field, type the name of the AD security group representing Patch Administrators who will use the Tachyon Patch Success application.

Select a name from the search list, and click the **Add** button.

The new user will be added to the **Users** table.

> **Tip**
>
> You may have already created a Tachyon user for this custom role. You can change or add other users later.

To create the custom role:

Navigate to the **Settings→Permissions→Roles** page.

Click the **Add** button to start the add role process.

In the **Add role** popup subsequently displayed set the name as **1E Patch Success Actioners**

Optionally enter a description

Click the **Add** button.

The new role will be added to the **Roles** table. Locate its entry and click on the link in the **Name** column for that row.

Select the **Members** tab and click the **Add** button.

In the **Add role member** popup subsequently displayed, search for the Tachyon user that you added in the earlier steps.

Click the **Add** button.

Select the **Permissions** tab and click the **Add** button.

In the **Add permission** popup subsequently displayed, scroll down the Type list and select **Repository:patch**

Select the **Read** checkbox.

Click the **Add** button.

In the **Add permission** popup subsequently displayed, scroll down the Type list and select **Instruction set**.

Scroll down the Name list and select the **1E Patch Success** instruction set.

Select checkboxes for each of the following from the list of permissions, and then click the **Add** button:

Questioner permission - allows users to see and use the **Explore** and **Check Status** buttons

Actioner permission - allows users to see and use the **Deploy** button

Approver permission - allows users to approve each other's use of the **Deploy** button instruction (see the note at the start of this section about alternative Approver roles).

Select the **Management groups** tab and click the **Add** button.

In the **Add management group** popup subsequently displayed, scroll down the list and select **All Devices**.

Click the **Add** button.

> **Warning**
>
> Only select **All Devices**. This is the same as the **All Devices** management group as seen in Patch Success Title and filter bars.

To verify:

Logon to the Tachyon Portal using a Tachyon user account with the new **1E Patch Success Actioners** role.

Navigate to the **Patch Success - Overview** page.

7.3.2.2 Configuring connectors and schedules

You must create the following connectors and schedules:

Tachyon connector and its **Sync Data** schedule - to import inventory and patch data into an inventory repository - this is normally the **Default inventory** repository

Configuration Manager or **WSUS** connector and its **Sync Data** schedule - to import meta-data for patches into the inventory repository

Generate Report - ETL schedule - for reprocessing of cube data in a **BI** repository - this is normally the **Default BI** repository

Patch data from all inventory repositories is reprocessed by an ETL (extract, transform, load) and stored in the BI cube to support dynamically updating interactive dashboards. The Patch Success application allows its users to view one inventory repository at any time.

7.3.2.2.1 Adding the Tachyon connector

You must add the Tachyon Connector in order to support **Tachyon Powered Inventory** which uses the **1E Inventory** instructions.

Please refer to Tachyon connector for detailed configuration steps. In summary these steps do the following:

Creates a user. In our example this is **ACME\SLATACHYON**

Configures the Tachyon connector. A by-product of this step means Management Group synchronization is enabled to support the use of Management groups

Creates the **1E Inventory** instruction set and **1E Inventory Questioners** role.

> **Note**
>
> The **1E Inventory** instruction set contains 4 instructions for inventory and 1 instruction for **Patch Success**. All of these instructions are necessary for Patch Success, but the

inventory instructions are also used for other purposes. If you have already created the Tachyon Connector using only the inventory instructions, then you will need to add the instruction for **Patch Success** to the same instruction set. For more details about these instructions please refer to Tachyon connector: Creating the 1E Inventory Instruction Set.

7.3.2.2.2 Adding a connector for Patch meta-data

Patch Success needs to get meta-data for patches. Ensure you add a connector for whichever one of the following sources that you use to approve patches:

Configuration Manager (SCCM) if it is configured to manage WSUS

Windows Server Update Services (WSUS)

If you are using Configuration Manager then you must add a System Center Configuration Manager connector.

If you are using WSUS then you must add a Windows Server Update Services connector.

7.3.2.2.3 Creating schedules for Patch processing

The following Patch Success schedule process is designed to reduce the data that is retrieved when performing Tachyon, Configuration Manager and WSUS connector syncs and to provide a separate Device and Patch consolidation that can be run without running the Basic Inventory Consolidation. This saves time and processing when using Patch Success on its own. We suggest configuring the following daily schedules, set to run on the same inventory repository in the order presented - leave enough time between the steps to allow the previous step to complete. You can test how long that takes by running the steps manually.

	Action	Frequency	Notes
1	**Sync Data - Configuration Manager** or **Sync Data - WSUS**	**Daily**	Pick a suitable time when there is the least amount of activity. If using the Configuration Manager sync be aware it may take a long time to run because as well as patch meta-data, it is also importing a lot of inventory, and usage data for processes and users. To work around this, when using the Configuration Manager connector only with Patch Success, you can configure the sync to

	Action	Frequency	Notes
			fetch just the **Device** and **Patch** data.
2	**Sync Data - Tachyon**	**Daily**	When configuring the Tachyon connector sync for use with Patch Success only, configure the sync to fetch just the **Device**, **Patch** and **User** data. You can schedule the **Sync Data** action to run at any time of day. Pick a suitable time when there is the least amount of processing activity. You must select the frequency that prevents the Sync Data actions for the Tachyon connector overlapping. In Tachyon Platform 5.2 and 8.x the duration that the Inventory instructions run for is a default of 24 hours, therefore select **Daily** or **Weekly**. In Tachyon Platform 5.1 the duration that the Inventory instructions run for is a default of 15 minutes, therefore select **Daily** or **Weekly**, or at least 20 minutes apart.
3	**Generate Report - Device and Patch consolidation**	**Daily**	This action can be run when using Patch Success on its own. If you are using AppClarity as well these reports are also included

	Action	Frequency	Notes
			as part of the Basic Inventory Consolidation.
4	**Generate Report - ETL**	**Daily**	This report reprocesses the cube data.

Steps for adding a schedule can be found on the Settings→Configuration→Schedules page.

For the **Sync Data** actions, the actual name of the action depends on the connector name. Also ensure you select the correct inventory repository, the default is **Default Inventory**.

7.3.2.3 Configuring the source for Patch downloads

Patch Success needs to be configured with the download source from which client devices will download and install patches. By default the download source is configured as **SCCM** (Configuration Manager) but you will need to change this to **WSUSL** (local WSUS) if you are using WSUS instead of Configuration Manager.

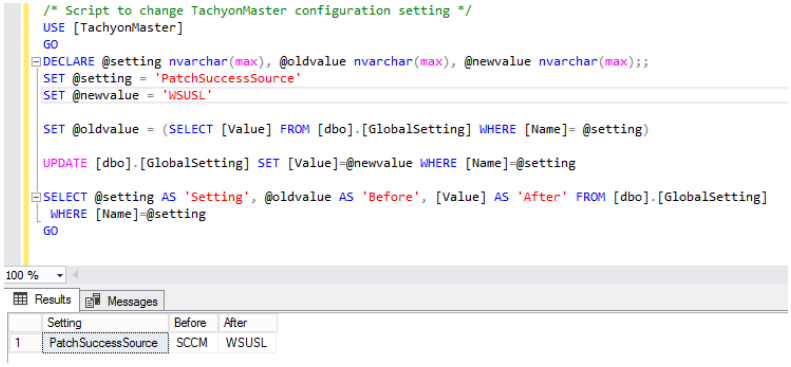
To change the download source, you must manually update the value of **PatchSuccessSource** in the **GlobalSettings** table of the **TachyonMaster** database:

If your client devices are using **Configuration Manager** to download and install patches then leave **PatchSuccessSource** as **SCCM** - this is the default

If your client devices are using **WSUS** to download and install your patches then change **PatchSuccessSource** as **WSUSL** using the following SQL script:

SQL script to configure PatchSuccessSource setting

```
/* Script to change TachyonMaster configuration setting */
USE [TachyonMaster]
GO
DECLARE @setting nvarchar(max), @oldvalue nvarchar(max), @newvalue nvarchar(max
);;
SET @setting = 'PatchSuccessSource'
SET @newvalue = 'WSUSL'

SET @oldvalue = (SELECT [Value] FROM [dbo].[GlobalSetting] WHERE [Name]= @setti
ng)

UPDATE [dbo].[GlobalSetting] SET [Value]=@newvalue WHERE [Name]=@setting

SELECT @setting AS 'Setting', @oldvalue AS 'Before', [Value] AS 'After' FROM [d
bo].[GlobalSetting]
 WHERE [Name]=@setting
GO
```



Note

Configuration of the **PatchSuccessSource** global setting (**SCCM** or **WSUSL**) is important to ensure that client devices use the correct source when instructed to download patches by the Tachyon Patch Success application. Patch Success administrators can expedite the patching process by using either **Download only** or **Deploy** (download and install) buttons. These buttons cause Tachyon to send the **1E-PatchSuccess-Deploy** instruction to multiple clients with details of which patches to download only or to also install. In addition, if the PatchSuccessSource global setting is configured as WSUSL then the buttons provide the option to download from Microsoft Update via the Internet instead of from WSUS. The buttons do this by overriding the gobal Setting **WSUSL** with **WSUSR** (in the database Patch Success refers to Microsoft Update as WSUS remote). If you want to know more about the methods used by the **1E-PatchSuccess-Deploy** instruction please refer to the Tachyon SDK - Patch.Deploy method documentation.

Note

If you set either WSUSR or SCCM (and intend allowing Windows Update to download the patches if they're not available on the Distribution Point) then the Windows Updates service must be allowed to download content from the internet and deploy the updates.

7.3.2.4 Additional configuration options

Following additional configuration options are available and can be changed if required.

7.3.2.4.1 Enabling Download only feature

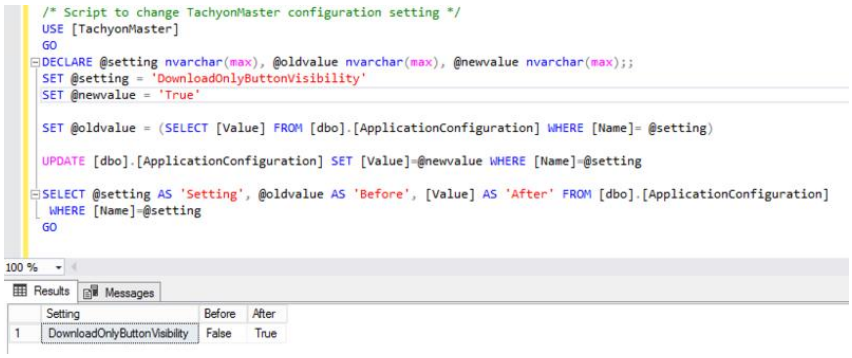
Download only is a button to download only without deploying the patch. This is only available for **WSUSL** and **WSUSR** patch source.

To enable **Download only** feature for the patch source **WSUSL** and **WSUSR**, run the following SQL script.

SQL script to configure DownloadOnlyButtonVisibility setting

```
/* Script to change TachyonMaster configuration setting */
USE [TachyonMaster]
GO
DECLARE @setting nvarchar(max), @oldvalue nvarchar(max), @newvalue nvarchar(max
);;
SET @setting = 'DownloadOnlyButtonVisibility'
```

```
SET @newvalue = 'True'

SET @oldvalue = (SELECT [Value] FROM [dbo].[ApplicationConfiguration] WHERE [Na
me]= @setting)

UPDATE [dbo].[ApplicationConfiguration] SET [Value]=@newvalue WHERE [Name]=@set
ting

SELECT @setting AS 'Setting', @oldvalue AS 'Before', [Value] AS 'After' FROM [d
bo].[ApplicationConfiguration]
 WHERE [Name]=@setting
GO
```



7.3.2.4.2 Changing the maximum number of targeted devices

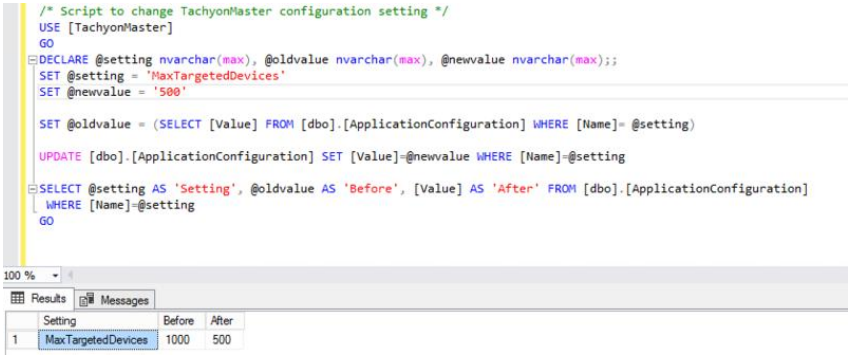
For the patch source **WSUSL** and **WSUSR** the UI will limit the number of devices that can be targeted for Downloads and Deployments to the maximum number. This limit is put in place to warn of the possible impact of deploying and downloading patches at scale, to the network infrastructure.

To change the maximum number of targeted devices run the following SQL script.

SQL script to configure MaxTargetedDevices setting

```
/* Script to change TachyonMaster configuration setting */
USE [TachyonMaster]
GO
DECLARE @setting nvarchar(max), @oldvalue nvarchar(max), @newvalue nvarchar(max
);;
SET @setting = 'MaxTargetedDevices'
SET @newvalue = '500'

SET @oldvalue = (SELECT [Value] FROM [dbo].[ApplicationConfiguration] WHERE [Na
me]= @setting)

UPDATE [dbo].[ApplicationConfiguration] SET [Value]=@newvalue WHERE [Name]=@set
ting

SELECT @setting AS 'Setting', @oldvalue AS 'Before', [Value] AS 'After' FROM [d
bo].[ApplicationConfiguration]
```

```
 WHERE [Name]=@setting
GO
```



7.3.2.5 Tachyon Platform zip

The Tachyon Platform zip file can be downloaded from the 1E Support Portal https://support.1e.com/.

Refer to Tachyon platform zip file for details.

7.3.3 Verifying

7.3.3.1 Verify Patch Success installation

To run the following tests you need:

Tachyon Server installed.

The name and password for the **server installation account**, the account must also be enabled.

Ref	Test	Expected	Remediation
TCNI01	Logon to the Tachyon Server using the **server installation account** Confirm 1E Tachyon Server is listed in Apps/Programs and Features	Programs and Features (appwiz.cpl) displays **1E Tachyon Server** with correct version number. If an MSP update has been installed, the Installed Updates displays **1E Tachyon Server Update (Qnnnnn)**. The following Windows services exist and are running. **1E Catalog Update Service** (Automatic) (Service account) **1E SLA Platform Engine** (Automatic Delayed start) (Network Service) **1E SLA Platform Integrate Agent** (Automatic Delayed start) (Network Service)	If any of the services are not running, then check the corresponding log(s). The **Switch Host** service will stop after several seconds if it is unable to

Ref	Test	Expected	Remediation
	Confirm Tachyon's Windows services are running.	**1E SLA Platform Integrate Manager** (Automatic Delayed start) (Network Service) **1E Tachyon Coordinator** (Automatic Delayed start) (Network Service) **1E Tachyon Switch Host**(Automatic Delayed start) (Local System) If you did not install Nomad, you may also have **1E ActiveEfficiency** (Automatic) (Network Service) remaining after an upgrade.	start any Switches. The **ConsumerAPI** log is not created until a user (the **server installation account**) successfully connects to the Tachyon Portal. The **Background API** log is not created until a 1E Client attempts to download content. The **1E-TachyonPlatform** product pack can be used to trigger this.
TCNI02	Check the Tachyon Server logs.	Click here to expand... The default location for all Tachyon logs is the folder *%ALLUSERSPROFILE%\1E* Subsystem / Component / 1E\Tachyon\ / *Tachyon.Portal.log* **Tachyon Master** / Tachyon Portal	

Ref	Test	Expected				Remediation
			UI and applications (Tachyon)			
		Consumer API	1E\Tachyon\	*Tachyon.ConsumerAPI.log*		
		Coordinator service	1E\Tachyon\	*Tachyon.Coordinator.log* *Tachyon.Instrumentation.log*		
		Experience web application	1E\Tachyon\	*Tachyon.Experience.log*		
		Catalog	Catalog UI (CatalogWeb - Admin sync)	1E\Catalog\	*Catalog.Integration.UI.log*	
		Catalog API				
		Catalog Update Service	1E\Catalog\	*Catalog.UpdateService.log*		
		Content Distribution	Content Distributio	1E\ContentDistribution	*ContentDistribution.log*	

Ref	Test	Expected				Remediation
			n web application			
		SLA	SLA/Platform APIs (Admin, Core External)	1E\Tachyon\	*Tachyon.AdminAPI.log*	
		SLA Platform UI (Platform)	1E\SLA Platform\	*Web.log*		
		SLA Engine	1E\SLA Platform\	*Engine.log*		
		SLA Integrate Services (Connector Manager)	1E\SLA Platform\	*1E.SLAPlatformIntegrateAgent.log* *1E.SLAPlatformIntegrateManager.log* *1E.SLAConnector.<type>_sync.log*		
		SLA Inventory	n/a	*n/a*		
		SLA Operations Provider (not	1E\Platform	*n/a*		

Ref	Test	Expected				Remediation
		currently used)	Consumer\			
		SLA databases (Data, Integrate, Shared)	n/a	*n/a*		
		BI	MDX API	SQL database	*[SLA-BI].[BI].[Event Log]*	
		Tachyon Response	Core	1E\Tachyon\	*Tachyon.CoreAPI.log*	
		Background Channel (Background)	1E\Tachyon\	*Tachyon.BackgroundAPI.log*		
		Switch(es) (also includes a single Switch Host service)	1E\Tachyon\	*Tachyon.Switch.4000.SW1.log* *Tachyon.Switch.Host.log*		

Please refer to Services and NTFS Security if changing the location of log files.

In this version of Tachyon Server, some installers do not support the LOGPATH property and the logs folder is not configurable during installation.

Each component has a configuration file in the Tachyon Server installation folder structure, which contains log configuration details. Defaults are:

Ref	Test	Expected	Remediation
		Filepath *%ALLUSERSPROFILE%\1E\<product>* where product is Tachyon, SLA Platform, and Catalog Filename as shown in the table above. Maximum size 10MB (2MB for Switch logs). 2 rollover files numbered 1 to 2 with the rollover number included as n.log (5 rollover files for Switch logs). Date and timestamps are UTC to help troubleshooters synchronize logs on systems in different timezones. Switch logs have the following names: The first Switch installed will typically have a log filename **Tachyon.Switch.4000.SW1.log** (where 4000 is the port it is listening on and SW1 is the **config name** in the SwitchConfiguration table in the TachyonMaster database). Other Switches on the same server will have different config names appended. The log filename will be unique on a server, but there may be the same named log on a different server. A Switch will continue to use the same log, unless the SwitchConfiguration table is modified so that a different ID is used. If you see a Tachyon.Switch.log without a config name appended, this is a special case where a Switch cannot find its correct configuration, and has fallen back to using the template * row which has ID=1. In which case you will need to troubleshoot how that happened. Rollover logs have numbers appended, for example Tachyon.Switch_A.1.log, up to a default maximum of 5. Tachyon server components use the **log4net RollingFileAppender** class. Details can be found in http://logging.apache.org/log4net.	

Ref	Test	Expected	Remediation
PSC01	Check the configuration of the Tachyon connector		

7.4 Using Patch Success

How to use the Patch Success application to report on and ensure successful patching of your enterprise.

Note

Patch Success can be reached directly using the following URL:

`https://<tachyon DNS Name FQDN>/Tachyon/App/#/patchsuccess/`

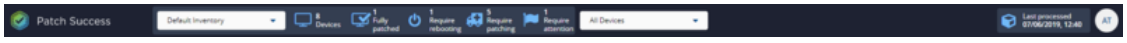
where <tachyon DNS Name FQDN> is the one set up during the preparation phase, as described under the heading DNS Names

7.4.1 Title and filter bars

Information about the title and filter bars that appear at the top of all Patch Success pages.

7.4.1.1 Patch Success title bar

The title bar shows information about the total number of devices and the patch status. The totals on the title bar are not affected by filters. The following table describes the function of each heading in the title bar.



Heading	Description
Inventory repository	A selected inventory repository. Changing the selection in this drop down will update the data on the Patch Success dashboards. Only one inventory repository can be selected at any one time.
Devices	The total number of devices in the selected inventory repository. If two numbers are shown, the first number is the total number of

Heading	Description	
	devices that reported patch data. A single number is shown if all devices reported patch data. The image above shows 8 devices have reported patch data.	
Fully patched	The number of fully patched devices.	**Note** The numbers shown are for the selected inventory repository. A device is counted only once under under each of these headings. The sum of these four numbers equals the total number of devices in the selected inventory repository. The totals shown on the title bar are only affected by the Repository filter, no other filter will affect these numbers. See below for more information about how 'Device Patch Status' is determined.
Require rebooting	The number of devices that require rebooting to complete installations.	
Require patching	The number of devices with missing patches.	
Require attention	The number of devices with failed patches.	
Management group	A management group filter. Changing the selection in this drop down will change the filter to the selected management group and update the data on the Patch Success dashboards.	

Heading	Description
	To filter multiple management groups you must use the Filter popup, and the title bar will show the first one in the filter list.
Last processed	This shows the last time the ETL and cube was last processed.
Avatar	The initials of the logged on user.

7.4.1.2 Page title bar

Each Patch Success page has refresh and expand buttons.

The refresh button is used to refresh the contents of the page.

The expand button toggles the size of the page inside the browser by hiding or showing the menu and main title bar.

7.4.1.3 Filter bar

The filter bar shows all currently selected filters. The **Filter** button open the **Filter** popup to allow filters to be managed, and **Clear Filters** removes all the currently selected filters.

You can add filters by using the Filters button, or cicking on headings in the Overview

7.4.1.3.1 Using the Filter popup to add and remove filters

Click the **Filter** button to display the **Filter** popup

Select a Filter type from the first column

Select or enter all the required filter options for the selected filter and click **Add**

Add multiple filters if required

Click **Apply** to close the **Filter** popup and apply the selected filters

You can add multiple filters of the same type if needed, the exception being range filters where only one filter per type can be added. The range filters are time to install and publish date. All filters of the same type are combined with **OR**, filters of different types are combined with **AND**. The **Filter** popup is divided into 3 columns as shown in the picture opposite and the table below:

Filter type	Filter options	Filter summary
Displays a list of Filter types. Select a Filter type by scrolling through the list and selecting one.	Displays options for the currently selected filter type. Click **Add** to add the filter with its selected options. Click **Clear** to reset the currently selected options. This will not affect filters that have already been added to the filter summary column.	Displays all the currently selected filters. Click the icon to remove a filter from the summary. Click **Apply** to apply the new filters and close the **Filter** dialog. Click **Cancel** to ignore any changes and close the **Filter** dialog.

7.4.1.3.2 Interacting with Overview page charts to add and remove filters

You can click on chart slices and labels to add filters. Clicking on a slice or label once adds its filter, and clicking on it again removes its filter. Clicking with the CTRL key down allows you to add and remove multiple filters. For range charts clicking with the SHIFT key down allows you to select a range of filters.

7.4.1.3.3 To remove a filter

click on the

icon to remove an invidual filter from the **Filter summary** or from the filter bar

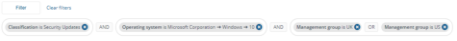
click on **Clear filters** to remove all filters from the filter bar

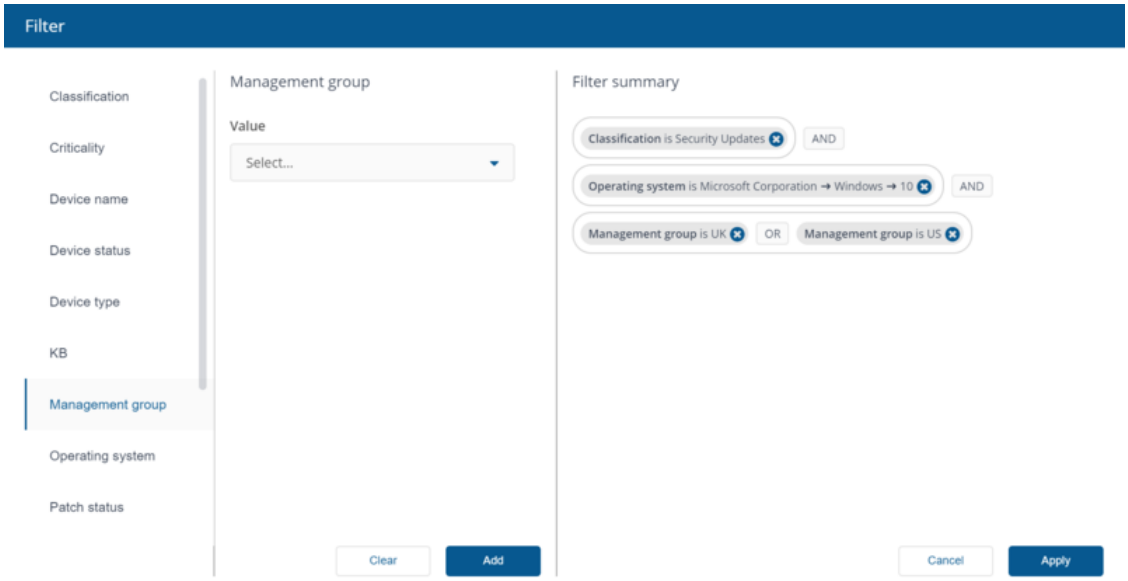
click on a

icon to remove an invidual filter from teh filter bar

open the Filter popup and use the the **Filter summary** or from the filter bar

The pictures below show an example of filters that have been added to show **Security Updates** on **Windows 10** devices in the **UK or US management groups**.





7.4.1.3.4 Filter types

The following table lists filter types and their avilable values. You can add multiple filters of the same type if needed, the exception being range filters where only one filter per type can be added. The range filters are time to install and publish date. All filters of the same type are combined with **OR**, filters of different types are combined with **AND**.

Type	Available values
Classification	Select a patch classification from the list of available values. The available values depend on which products and classifications have been specified in WSUS, as shown in the picture opposite. Critical Updates Definition Updates Drivers Feature Packs Security Updates Service Packs Tools Update Rollups Updates

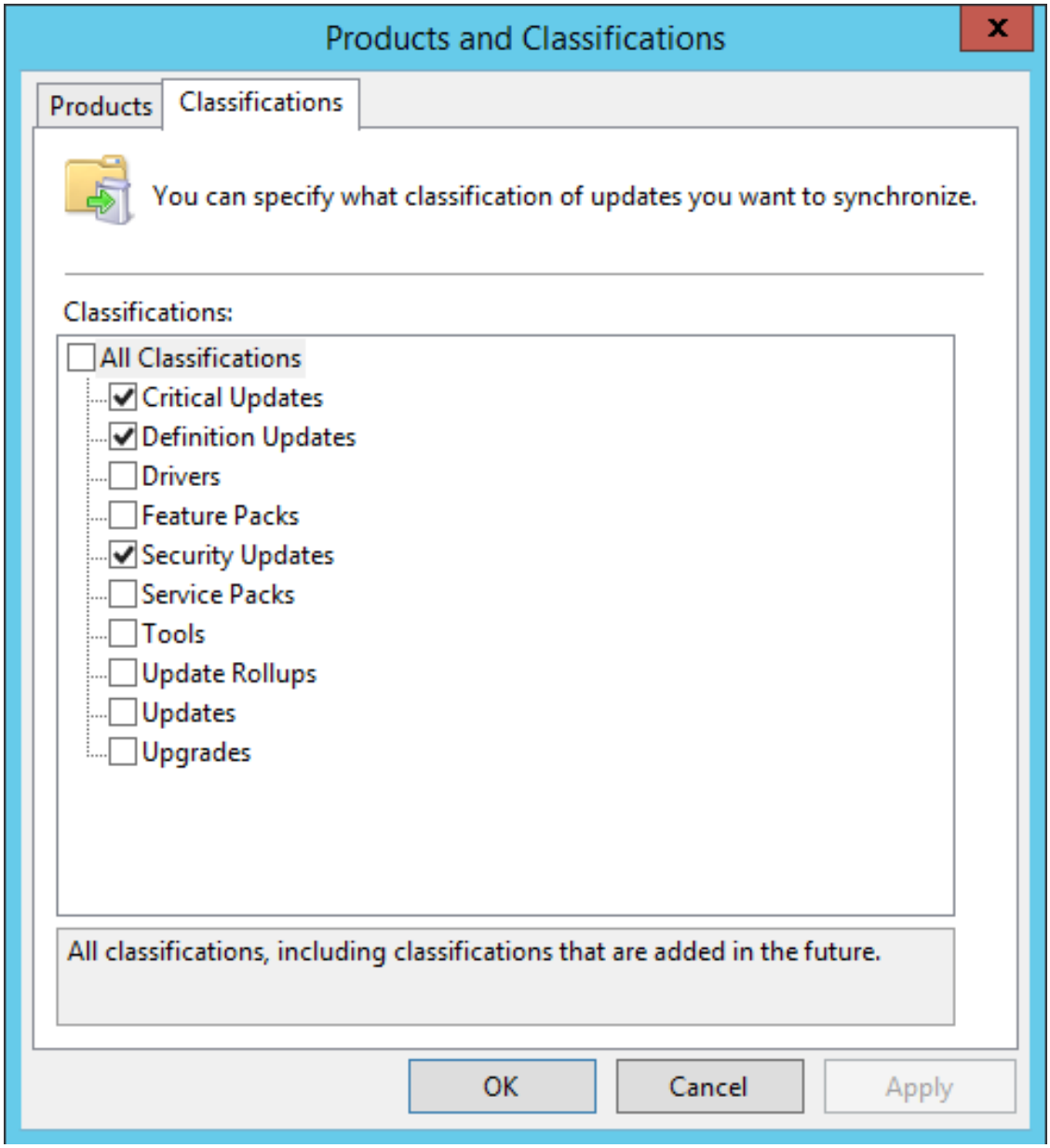
Type	Available values
	Upgrades And also: Unidentified - none of the above
Criticality	Select a device criticality from the list of available values. The available values shown opposite are default values provided by Tachyon and configurable in a lookup list in the **GlobalSettings** table in **TachyonMaster** database. 5: Critical 4: High 3: Medium 2: Low 1: Non-critical 0: Unidentified (not set) Device criticality is set on devices by the using the Device.SetCriticality method, as used for example by the instruction **1E-Explorer-TachyonAgent-SetCriticality**. The instruction sets the criticality number on the Tachyon client, which is returned as part of the Device details. If not set then the client returns 0. The system translates this number into a criticality value using a lookup table (in the TachyonMaster database). The criticality value is used in various dashboard tiles and tables, as well as Device details, and can be filtered using these values.
Device name	Select a specific device by name. Search by typing at least three characters and select a device from the search results. The filter itself cannot contain a wildcard, you must select a device and use its full name.
Device status	Select a device status from the list of available values: Fully patched - all patches are *succesfully installed* No patches - no patches are reported Requires attention - some patches *failed* to install or have an *error* Requires patching some patches are *missing* Requires rebooting - some patches are *pending a reboot*

Type	Available values
Device type	Select a device type category and sub-category: Physical Desktop Laptop Server Tablet Workstation Unidentified Virtual Virtualisation technology, for example: ESX, POWER, Solaris Zone, Solaris Container, Hyper-V, Oracle VM, RedHat VM Virtual Machine - if the virtualisation technology is unidentified, which typically occurs if the virtual host cannot be identified or is not included in the inventory repository
KB	Select a specific KB number. Search by typing at least three digits and select a KB from the search results. The search is based on KB meta-data available in your inventory repository as reported by Configuration Manager or WSUS. The list includes all KBs not just the ones that are actually installed, and may therefore return zero devices.
Management group	Select a management group from the available list. If the list is not up-to-date after creating a new management group then you may need to reprocess the cube data.
Operating system	Select an operating system by selecting **Vendor**, **Title** and **Colloquial version** from the available lists. The values available will depend on data in your selected inventory repository.
Patch status	Select a patch status from the available list: Failed Installed

Type	Available values
	Missing Pending reboot
Publish date	Select **from** and/or **to** dates for when patches were published. Dates are inclusive. **Note** Only one range filter is allowed when filtering.
Severity	Select a patch severity from the available list: Critical Important Low Moderate Unidentified
Time take to install	Specify **from** and/or **to** for the number of days a patch was installed after it was published. Days are inclusive. **Note** Only one range filter is allowed when filtering.
User	Select a specific user by name or enter **Unidentified**. Search by typing at least three characters and select a user from the search results. The filter itself cannot contain a wildcard, you must select a user and use their full name.

7.4.1.3.5 WSUS Products and Classifications

Please refer to https://docs.microsoft.com/en-us/sccm/sum/get-started/configure-classifications-and-products for a description of each classification.



7.4.2 Patch Success Overview page

The overview page shows a dashboard with three charts and a pivot table, that are dynamically recalculated based on applied filters.

Without filters the dashboard shows the status of all devices in the selected inventory repository and all patches affecting them. When filters are added, the dashboard is recalculated according to the applied filtered. For an explanation of filters, please refer to Title and filter bars.

The totals on the title bar are not affected by filters. For more details about the title bar please refer to Title and filter bars.

7.4.2.1 Dashboard charts

7.4.2.1.1 Patch status per device

Shows the overall patch status, after applying filters, by organizing devices into the following states ordered by priority:

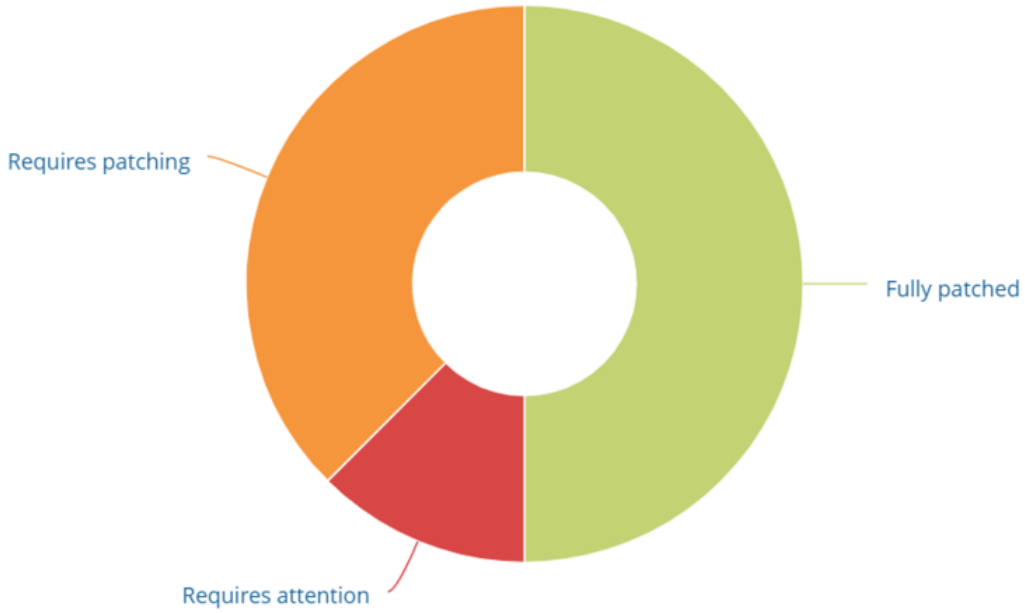
Requires attention: some required patches failed to install

Requires patching: some required patches are missing

Requires rebooting: some applied patches are pending a reboot

Fully patched: all required patches have been applied successfully

Selecting a chart slice or label will apply a **Patch status** filter to the whole dashboard, but not to the title bar. For details of this and other filter types please refer to Title and filter bars: Filter types.



7.4.2.1.2 Security updates by severity level

Shows the security update spread, after applying filters, by organizing the security updates into their Microsoft security bulletin severities:

Critical

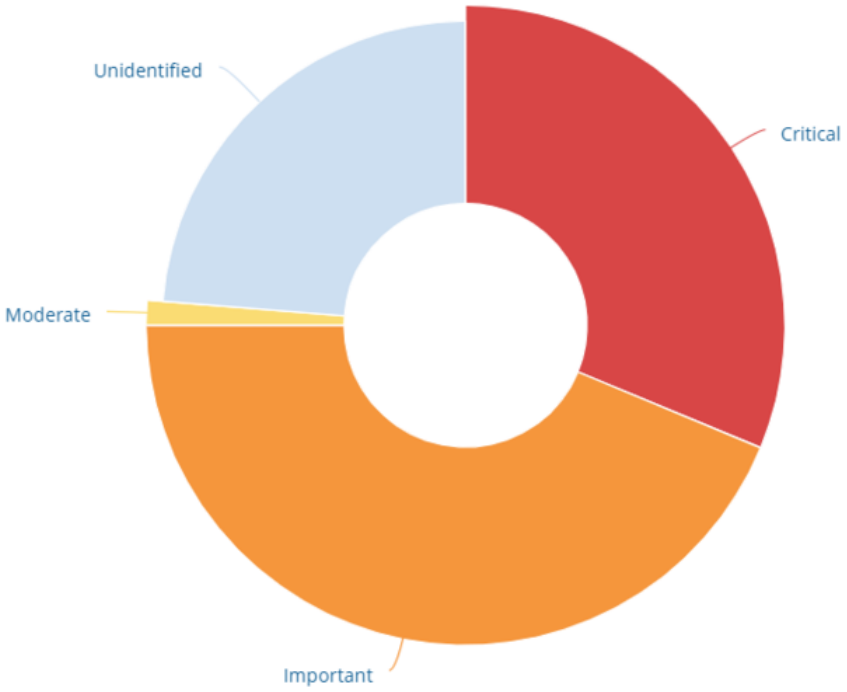
Important

Moderate

Low

Unidentified: no assigned severity.

Selecting a chart slice or label will apply a **Severity** filter to the whole dashboard, but not to the title bar. For details of this and other filter types please refer to Title and filter bars: Filter types.

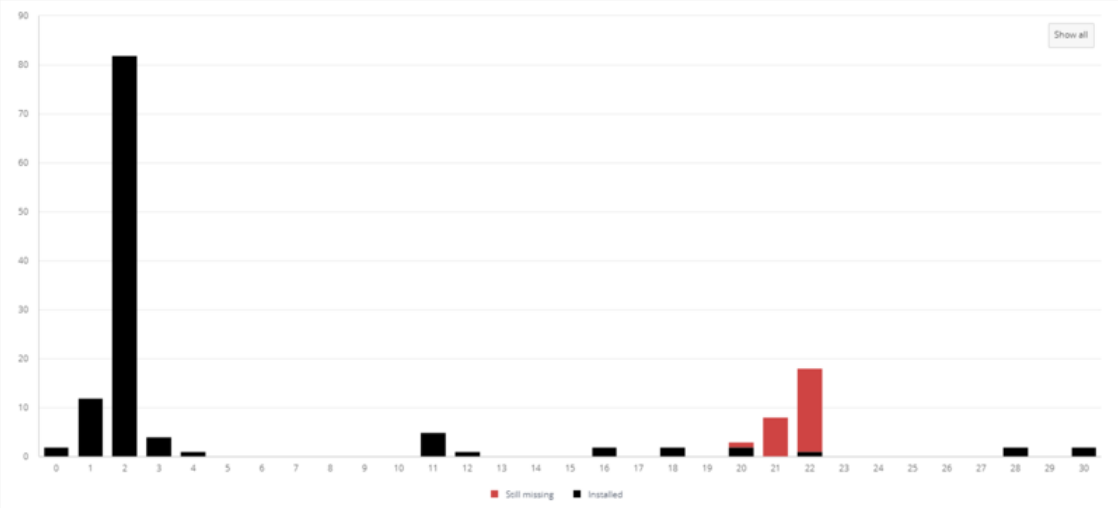


7.4.2.1.3 Patch performance

Shows the number of updates installed per day. The black column shows the days elapsed between the patch installation date and the publish date or the device's OS installation date (whichever is more recent). It also shows, as a red column, the required number of patches that are missing.

You can zoom in and out to highlight details of patches across time.

Selecting a chart bar or label will apply a **Time taken to install** range filter to the whole dashboard, but not to the title bar. For details of this and other filter types please refer to Title and filter bars: Filter types.



7.4.2.2 Interacting with the charts

You can click on chart slices and labels to add filters. Clicking on a slice or label once adds its filter, and clicking on it again removes its filter. Clicking with the CTRL key down allows you to add and remove multiple filters. For range charts clicking with the SHIFT key down allows you to select a range of filters.

The example picture opposite shows the dashboard with a filter for a single device. It has 10 patches, 5 are **Missing** and 5 are **Installed**.

As the device has 5 missing patches the device patch status is **Requires patching**.

When you hover a chart label you will see the number of devices and the percentage of the total for that label.

The device patch status chart shows:

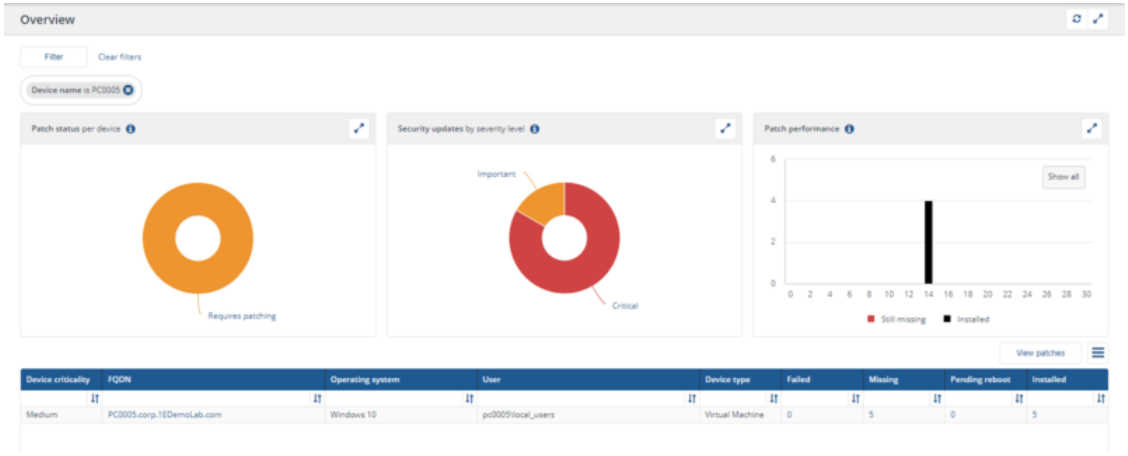
Requires patching 100% (1 device)

The security updates by severity level chart shows:

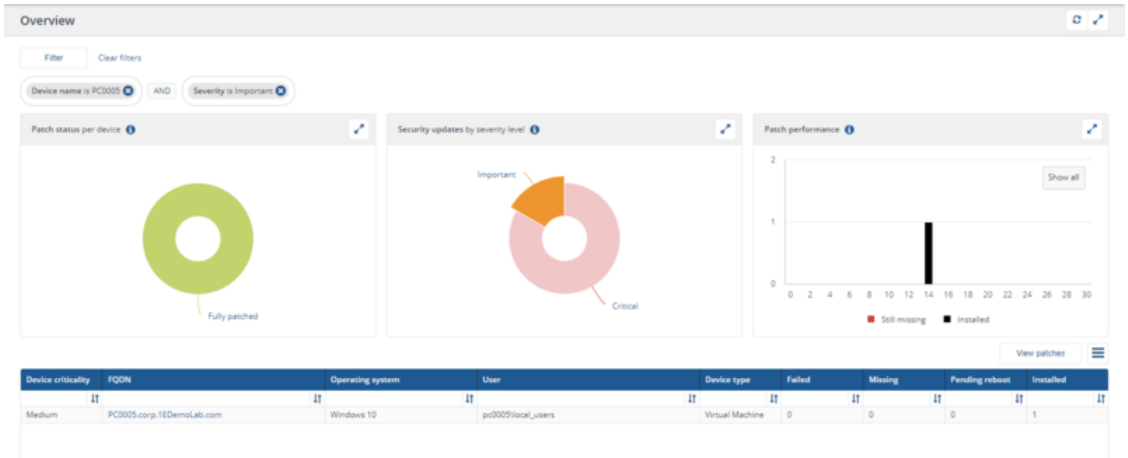
Important 17% (1 updates)

Critical 83% (5 updates)

> **Note**
>
> Patches that are not security updates do not have a severity and therefore appear as **Not applicable** and do not affect the severity chart.



Adding a filter to show only **Security Updates** that are important causes the set of patches for this device to be reduced to 1 patch in total, with 1 patch showing as installed. The device patch status now shows **Fully Patched**.



7.4.2.3 Pivot table

Clicking on the **View patches** button causes the table to pivot from a list of devices to a list of patches and the button changes to **View devices**. Clicking on the button again pivots the table back to a list of devices.

With the table in **View devices** mode, the list shows:

Device criticality

Device FQDN

Operating system

Primary user

Device type

Patch numbers according to their status:

Failed

Missing

Pending reboot

Installed

Clicking on a device **FQDN** takes you to the Device pages: Device View.

Clicking on one of the **Patch numbers** takes you to the Device patches page.

The example picture opposite shows a filtered view of devices in a specific management group.

With the table in **View patches** mode, the list shows:

Vendor

Title

Classification

Security update severity

Publish date

Patch numbers according to their status:

Failed

Missing

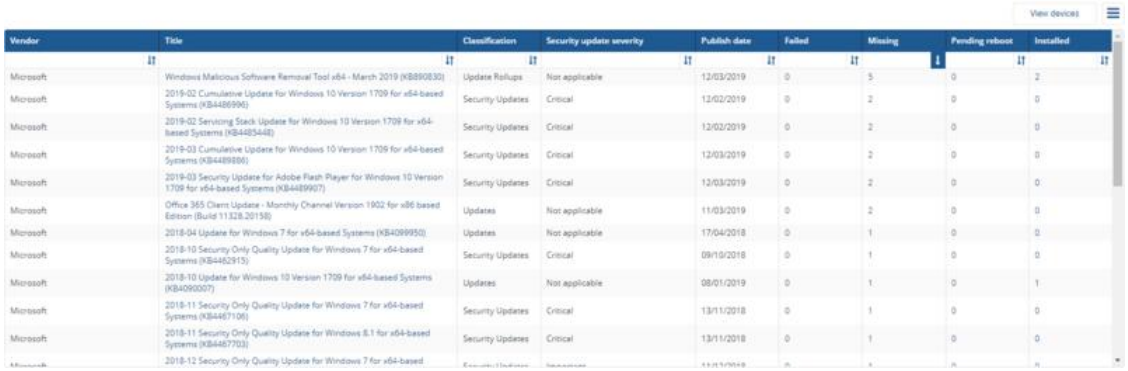
Pending reboot

Installed

Clicking on a patch title will take you to the Patch details page.

Clicking on one of the **Patch numbers** takes you to the Patch installations page.

The example picture opposite shows the previously filtered device and its 6 patches.



7.4.3 Patch pages

Information about the patch pages:

Patches page

Patch installations page

Patch details page

7.4.3.1 Patches page

This page is accessed from the Patch Success menu.

The page shows a full list of patches applicable to devices within your estate.

KB - is a patch knowledge base number.

Vendor - is a patch vendor name.

Title - is a patch title.

Classification - is classification of a patch.

Security update severity - is severity of security updates.

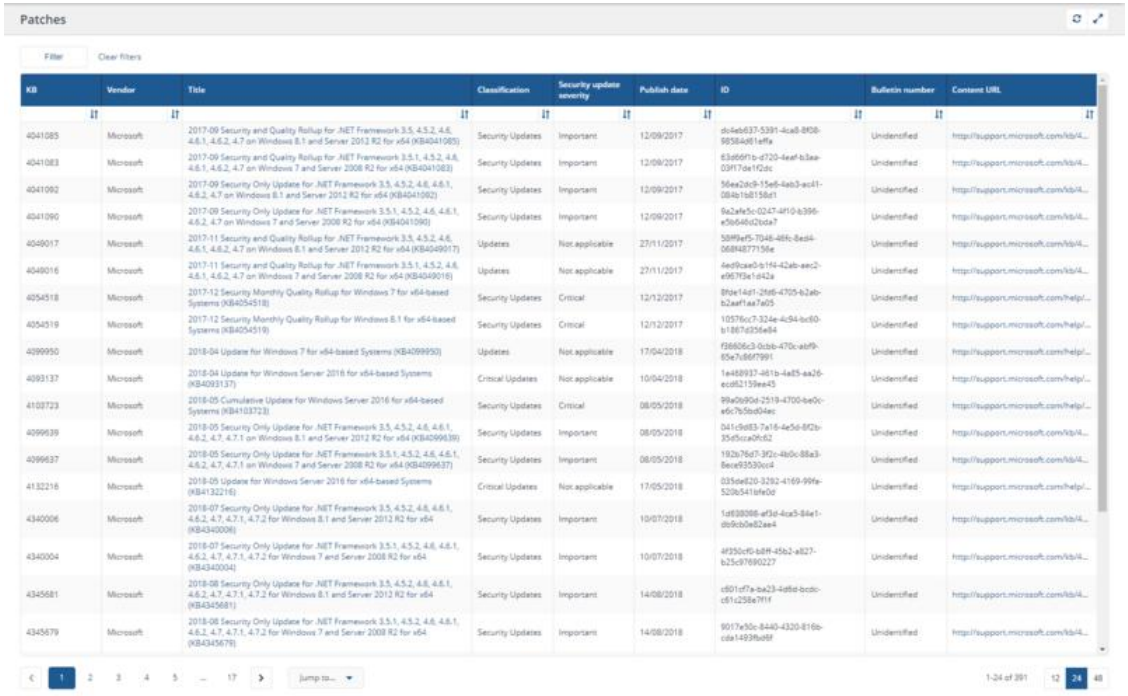
Publish date - is a date on which the patch was published.

ID - is a patch identifier.

Bulletin number - bulletin number for the patch.

Content URL - external content URL which provides more details about the patch.

Clicking on a patch title takes you to the Patch details page.



7.4.3.2 Patch installations page

This page is accessed by clicking on one of the **Patch numbers** on the Patch Success Overview page table in **View patches** mode.

The page shows details of the selected patch and all the respective devices where the patch is applicable.

Clicking the **Explore** button takes you to the **Home** page of the **Explorer** application, with coverage scope predefined for the selected devices. There you use any instructions (questions and actions) that you have permission to use.

Clicking the **Check Status** button runs the **1E-PatchSuccess-Explore** instruction:
Returns patch status for <patchSpec> identifier(s) for the current patch on the selected devices, and takes you to the **Explorer** application to monitor progress of the status instruction.

Clicking the **Update status** button will run the **1E-PatchSuccess-Refresh** instruction:
Returns patch status of given <patchSpec> identifier(s) for PatchSuccess consumption for the current patch on the selected devices and the response will be used to update the dashboards. This can be used to refresh the status of a patch within the dashboard without running the full reprocessing ETL.

Clicking the **Download only** button will run the **1E-PatchSuccess-Deploy** instruction:
Download only patch(es) specified by <patchSpec> identifier(s) from <source> source to targeted device to trigger a download without a deployment of the current patch to the selected devices, and takes you to the History page to monitor progress of the download instruction.

> **Note**
>
> Download only functionality is not available for SCCM based deployments. Download only functionality is disabled by default and can be enabled in configuration.

Clicking the **Deploy** button will run the **1E-PatchSuccess-Deploy** instruction:
Deploy patch(es) specified by <patchSpec> identifier(s) from <source> source to targeted device

to trigger deployment of the current patch to the selected devices, and takes you to the History page application to monitor progress of the deploy instruction.

For more details about Patch Success instructions, please refer to Configuring Patch Success: Create the 1E Patch Success Instruction Set.

Patch details:

Vendor and respective products of the patch

Publish date and Knowledge Base number of the patch

Patch classification and security update severity

The table shows a list of devices with the following details:

Device criticality - is criticality of a device

FQDN - is the fully qualified domain name of a device

Operating system - is the operating system of a device

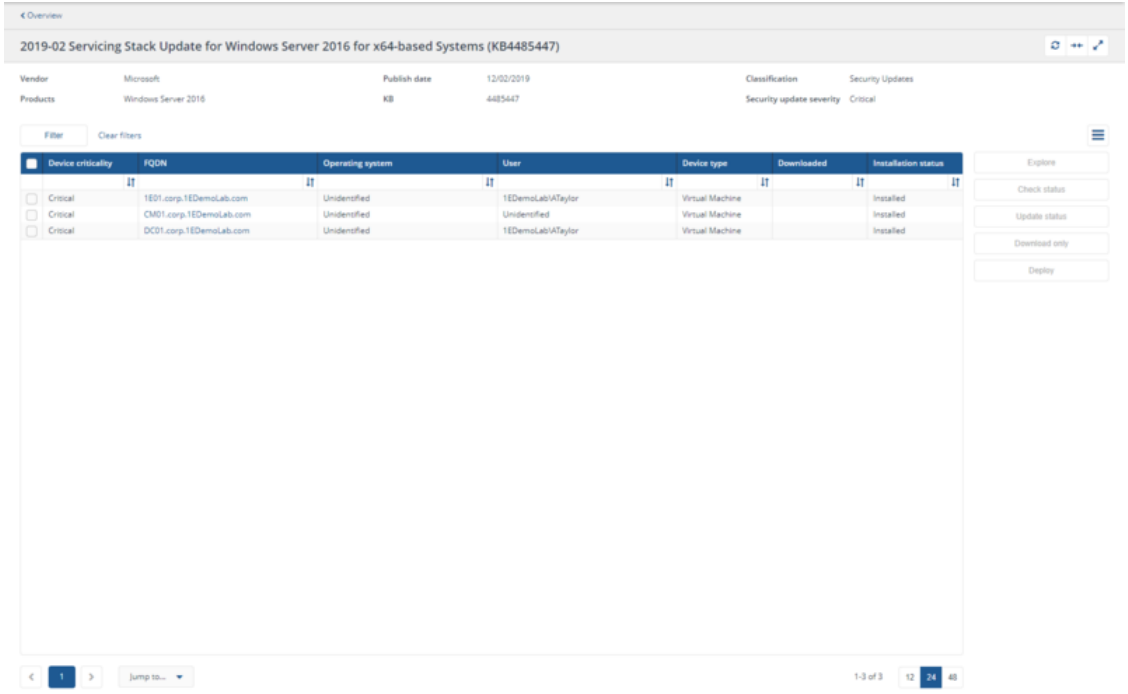
User - is primary device user

Device type - is type of device

Downloaded - is a flag to indicating if the patch downloaded on the device

Installation status - is the status of the patch on the device

Clicking on a device **FQDN** will take you to the Device details page.



7.4.3.3 Patch details page

This page is accessed by clicking a patch title on:

Patches page

Patch Success Overview page table in view patches mode.

The page shows details for the selected patch:

Description of the selected patch

Vendor

Related products

Publish date

ID guid

Knowledge Base number

Bulletin number

Classification

Security update severity

Reboot behaviour

If the patch is uninstallable

Supercedence

Source of patch information

Content URL

Also shows total numbers of device where the patch is:

Failed

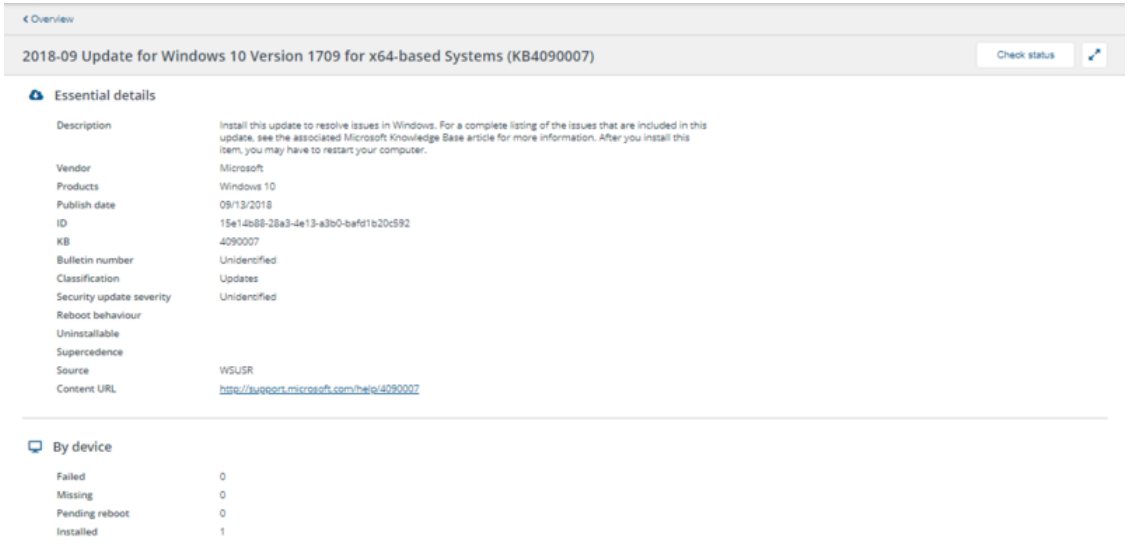
Missing

Pending reboot

Installed

The **Check Status** button runs the **1E-PatchSuccess-Explore** instruction:
Returns patch status for <patchSpec> identifier(s) for all devices, and takes you to the **Explorer** application to monitor progress of the instruction.

For more details about Patch Success instructions, please refer to Configuring Patch Success: Create the 1E Patch Success Instruction Set.



7.4.4 Device pages

Information about the device pages:

Devices page

Device patches page

7.4.4.1 Devices page

This page is accessed from the Patch Success menu.

Shows all the devices and their current patch status.

FQDN - is the fully qualified domain name of a device

User - is the primary user of a device

Device criticality - is the criticality of a device - please refer to Using Device Criticality

Device type - is the type of device, physical or virtual

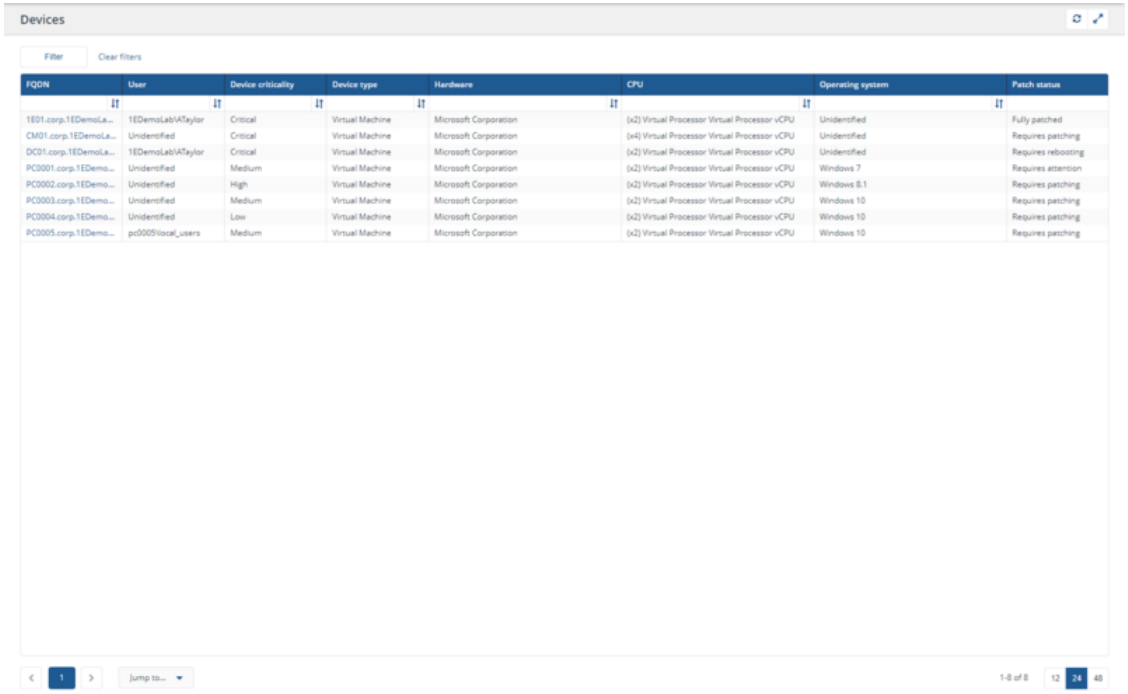
Hardware - the device make and model

CPU - the device CPU

Operating system - the device operating system

Patch status - the patch status of the device

Clicking on a device **FQDN** will take you to the Device View.



7.4.4.2 Device patches page

Shows details of the selected device and all the patches related to the device.

This page is accessed by clicking on one of the **Patch numbers** on the Patch Success Overview page table in **View devices** mode.

Clicking the **Explore** button takes you to the **Home** page of the **Explorer** application, with coverage scope predefined for the selected device. There you use any instructions (questions and actions) that you have permission to use.

Clicking the **Check Status** button runs the **1E-PatchSuccess-Explore** instruction:
Returns patch status for <patchSpec> identifier(s) for the selected patches on the current device, and takes you to the **Explorer** application to monitor progress of the status instruction.

Clicking the **Update status** button will run the **1E-PatchSuccess-Refresh** instruction:
Returns patch status of given <patchSpec> identifier (s) for PatchSuccess consumption for the selected patches on the current device and the response will be used to update the dashboards. This can be used to refresh the status of a patch within the dashboard without running the full ETL.

Clicking the **Download only** button will run the **1E-PatchSuccess-Deploy** instruction:
Download only patch(es) specified by <patchSpec> identifier(s) from <source> source to targeted device to trigger a download without a deployment of the current patch to the selected devices, and takes you to the History page to monitor progress of the download instruction.

> **Note**
>
> Download only functionality is not available for SCCM based deployments. Download only functionality is disabled by default and can be enabled in configuration.

For more details about Patch Success instructions, please refer to Configuring Patch Success: Creating the 1E Patch Success instruction set and Actioners role. Clicking the **Deploy** button will run the **1E-**

PatchSuccess-Deploy instruction:
Deploy patch(es) specified by <patchSpec> identifier(s) from <source> source to targeted device to trigger deployment of selected patches to the current selected device, and takes you to the History page to monitor progress of the deploy instruction.

Device details :

Operating system title and edition

Device make, model and type

CPU make, model and speed

Online status of the device

Device criticality

The table shows a list of patches with the following details:

Vendor - is a patch vendor name

Title - is a patch title

Classification - is classification of a patch

Security update severity - is severity of security updates

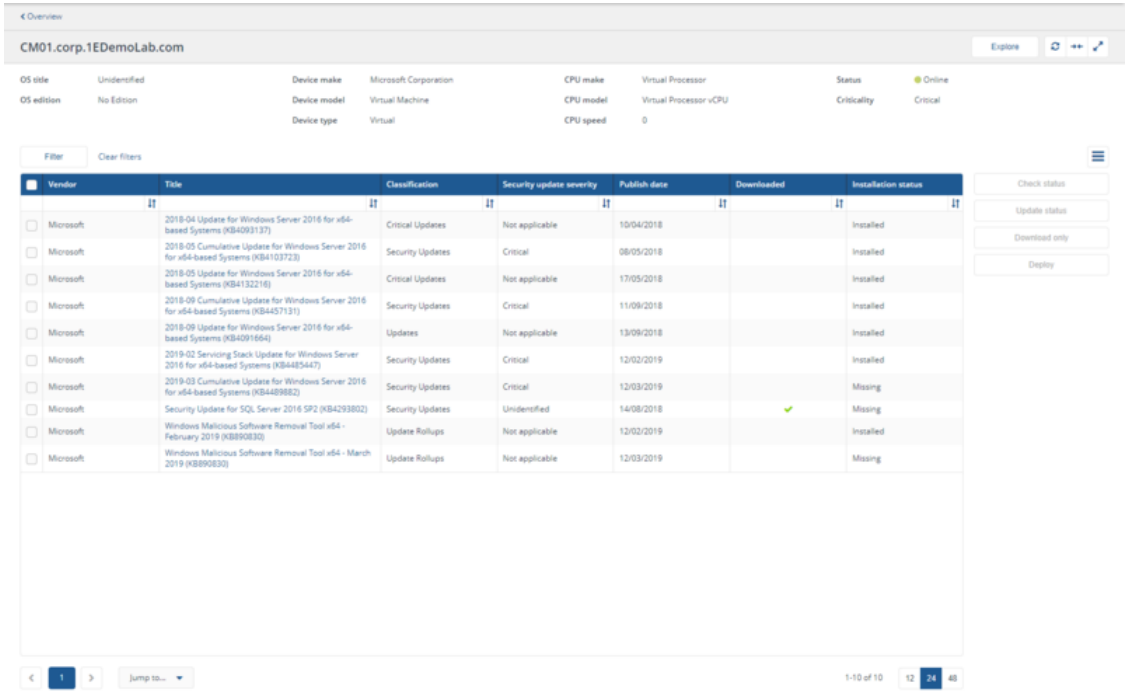
> **Tip**
>
> The severity classification is provided by the vendor, for example Microsoft.
> **Not Applicable** is not related to the device, it simply means the vendor has not given a severity classification for the patch.

Publish date - is a date on which the patch was published

Downloaded - is a flag to indicating if the patch downloaded on the device

Installation status - is the current status of the patch

Clicking on a device **FQDN** will take you to the Patch details page.



7.4.5 Monitoring pages

Information about the device pages:

History page

Responses tab

Targeted Devices tab

Patches tab

Responses page

7.4.5.1 History page

This page is accessed from the Patch Success menu.

Shows all the Patch Success instructions and their current status.

Instruction performed - is a user friendly description of the instruction showing targeted patches and devices covered by the issued instruction.

Creator- is the user that has created the instruction.

Creation - is the time at which the instruction was created.

Start - is the time at which the instruction has started.

Deletion - is the the time at which the instruction has ended.

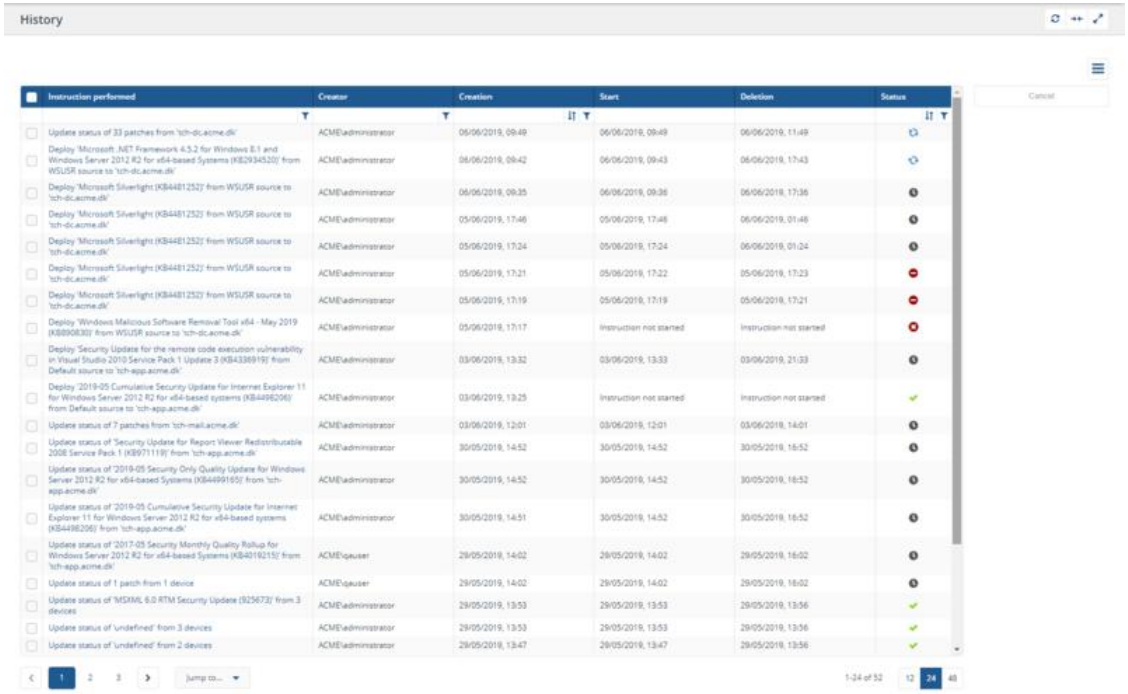
Status - is the device status of the instruction.

Icon	Description
	This instruction has been created
	This instruction is awaiting approval
	This action has been rejected by an approver
	This instruction is in progress and still gathering responses
	This instruction has responses that can be viewed
	This instruction's responses have expired
	This instruction is being cancelled
	This instruction has been cancelled
	This instruction has failed
	This instruction is awaiting authentication

Clicking on a device **Instruction performed** will take you to the Responses tab.

Clicking the **Cancel** button cancels the selected instructions.

> **Note**
>
> Cancelling instructions will not undo already completed actions and will simply stop any outstanding actions from completing. To determine which actions have been completed, navigate to responses tab by clicking the**Instruction performed**name in the instruction row.



7.4.5.2 Responses tab

Shows all the responses returned from an instruction.

Response time - is the time at which the response was received.

FQDN - is the fully qualified domain name of the device from which the response was received from.

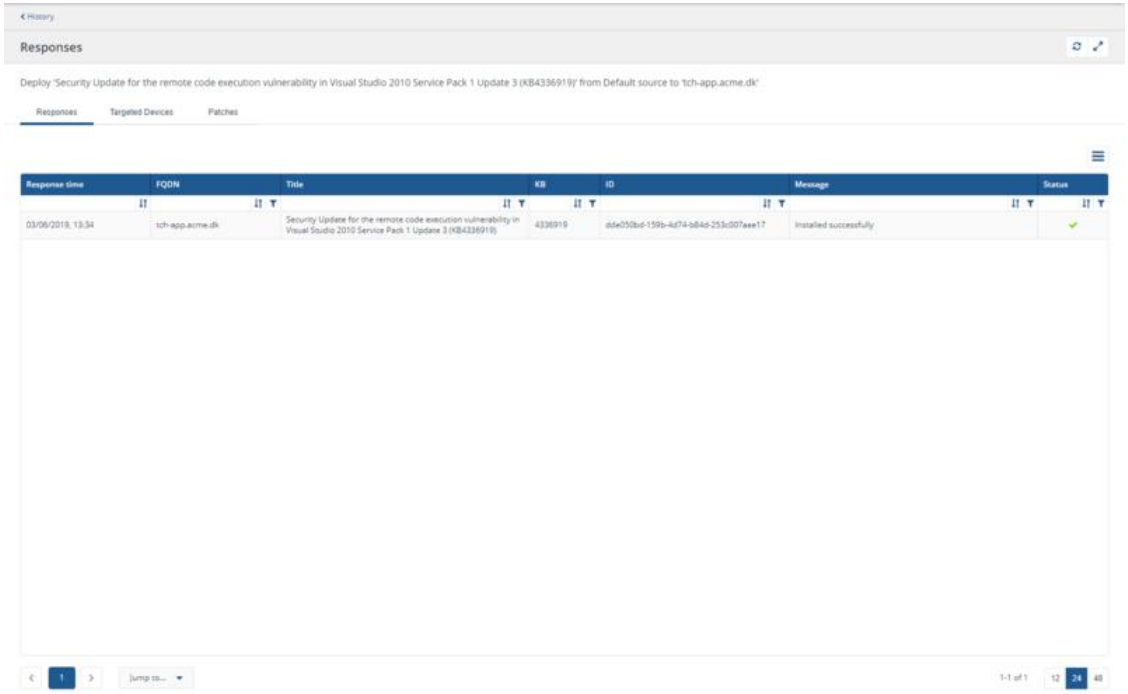
Title - is the title of the patch targeted by the instruction.

KB - is the Knowledge Base number of the patch targeted by the instruction.

ID - is the identified of the patch targeted by the instruction.

Message - is the result of the update or deployment.

Status - is the status of the update or deployment.



7.4.5.3 Targeted Devices tab

Shows all the target devices for an instruction.

FQDN - is the fully qualified domain name of a device from which the response was received from.

User - is the primary user of a device.

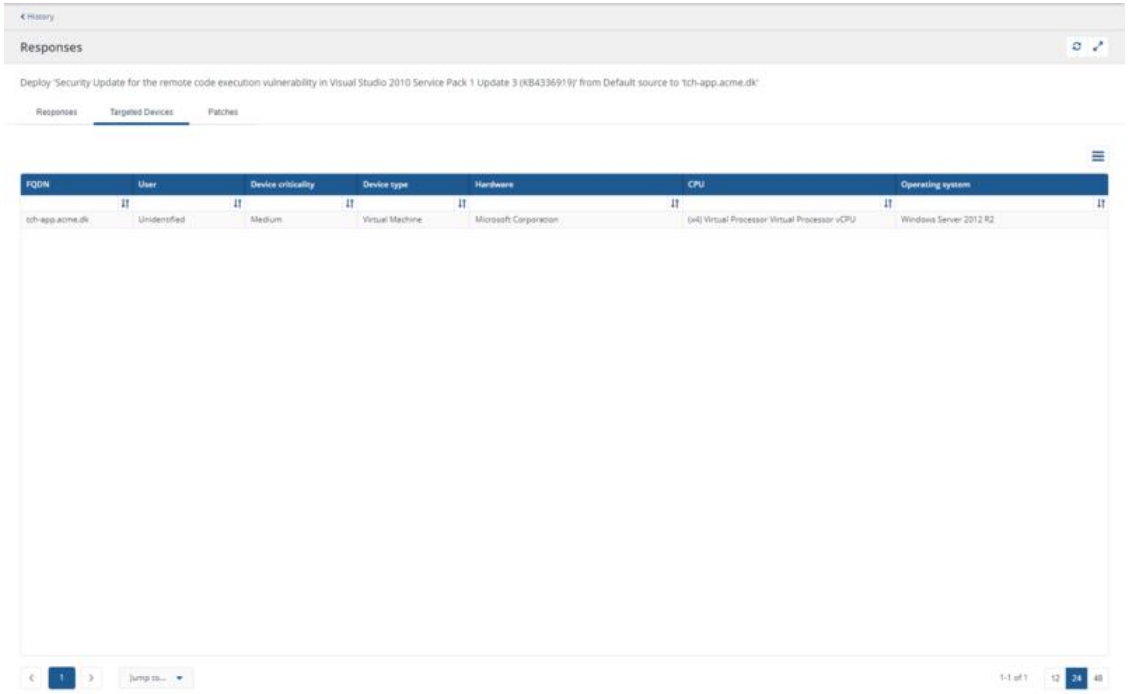
Device criticality - is the criticality of a device.

Device type - is the type of device, physical or virtual.

Hardware - the device make and model.

CPU - the device CPU.

Operating system - the device operating system.



7.4.5.4 Patches tab

Shows all the patches for an instruction.

KB - is a patch knowledge base number.

Vendor - is a patch vendor name.

Title - is a patch title.

Classification - is classification of a patch.

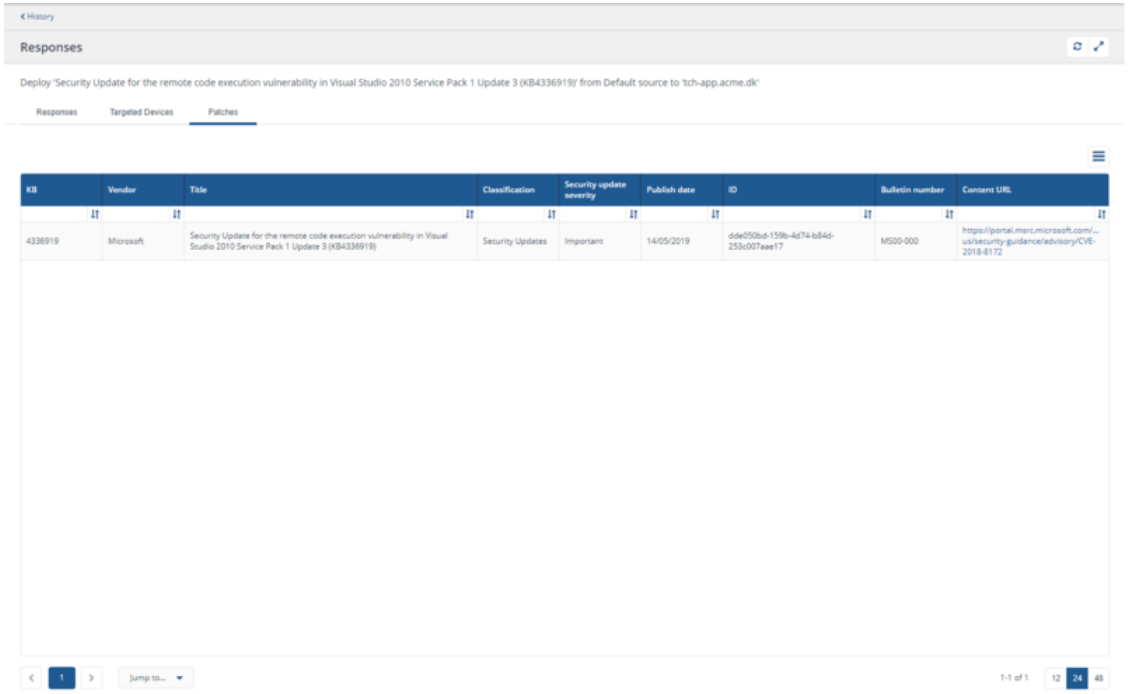
Security update severity - is severity of security updates.

Publish date - is a date on which the patch was published.

ID - is a patch identifier.

Bulletin number - bulletin number for the patch.

Content URL - external content URL which provides more details about the patch.



7.4.5.5 Responses page

Shows all the responses returned from all Patch Success instructions.

Response time - is the time at which the response was received.

FQDN - is the fully qualified domain name of the device from which the response was received from.

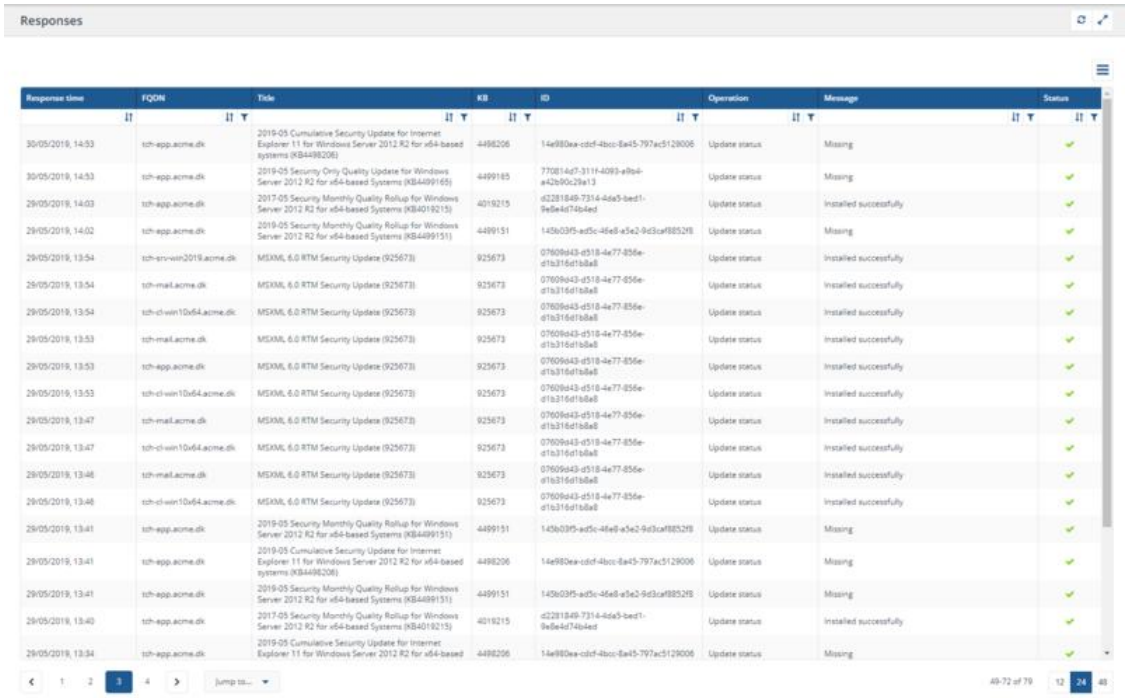
Title - is the title of the patch targeted by the instruction.

KB - is the Knowledge Base number of the patch targeted by the instruction.

ID - is the identified of the patch targeted by the instruction.

Message - is the result of the update or deployment.

Status - is the status of the update or deployment.



7.4.6 Reporting and successfully patching a management group for a single KB - tutorial

A worked example of using Patch Success.

In this tutorial

In this tutorial an emergency patch has been deployed using Configuration Manager, but the Security team have concerns that some devices have not received that patch and could become vulnerable to an exploit.

In this tutorial we will demonstrate:

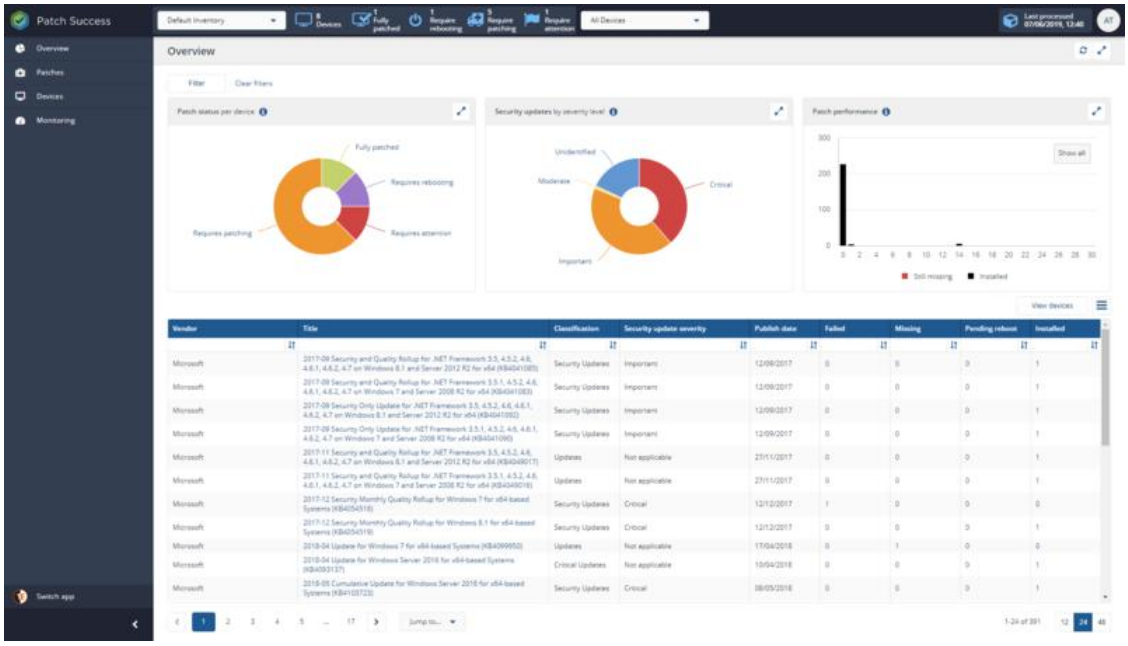
Checking the performance of the specific KB against a management group

Patching immediately any device or devices in the management group which haven't received it

7.4.6.1 Checking the performance of the specific KB against a management group

Navigate to **Patch Success→Overview**

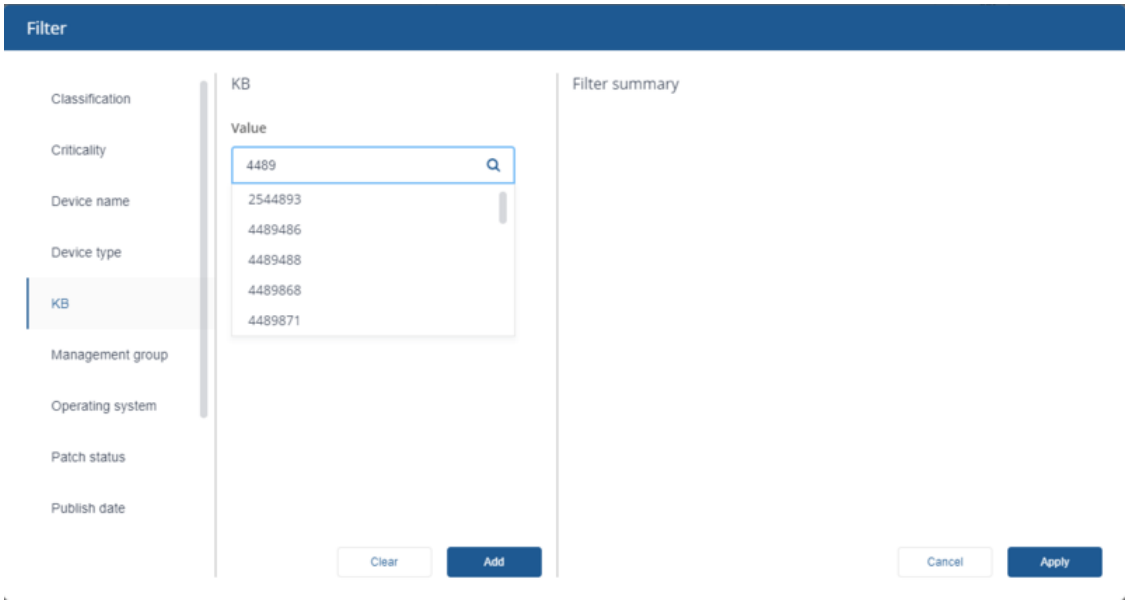
In the title bar, click on the management group drop-down list. By default this will show **All Devices**. If you change the selection, notice the name of the selected management group is added to the filter bar. You can select only one management group using this method. In our example we will select the **All Devices** management group.



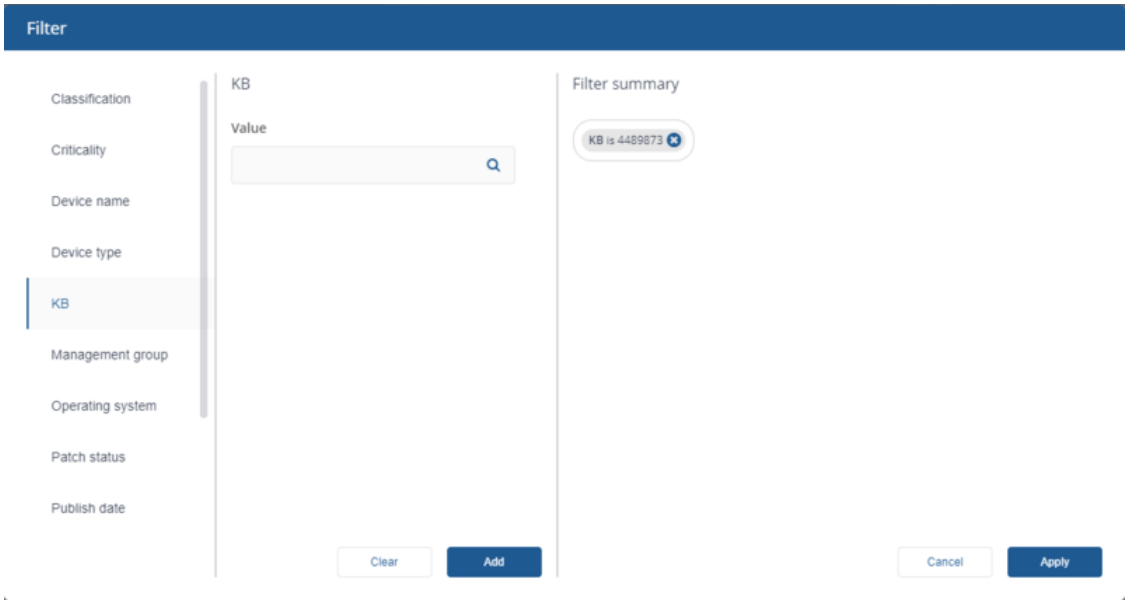
Click on the **Filter** button and the **Filter** popup appears.

Select the **KB** filter and enter a value for the KB and a drop-down auto-fills a list of KBs, select the chosen KB, and click **Add**.

Select the **Management group** filter and select a management group from the value drop-down list, and click **Add**. You can select more than one Management group using this method. Remove all selected groups, because we are using **All Devices** in this tutorial.



In the **Filter** popup, click the **Apply** button.



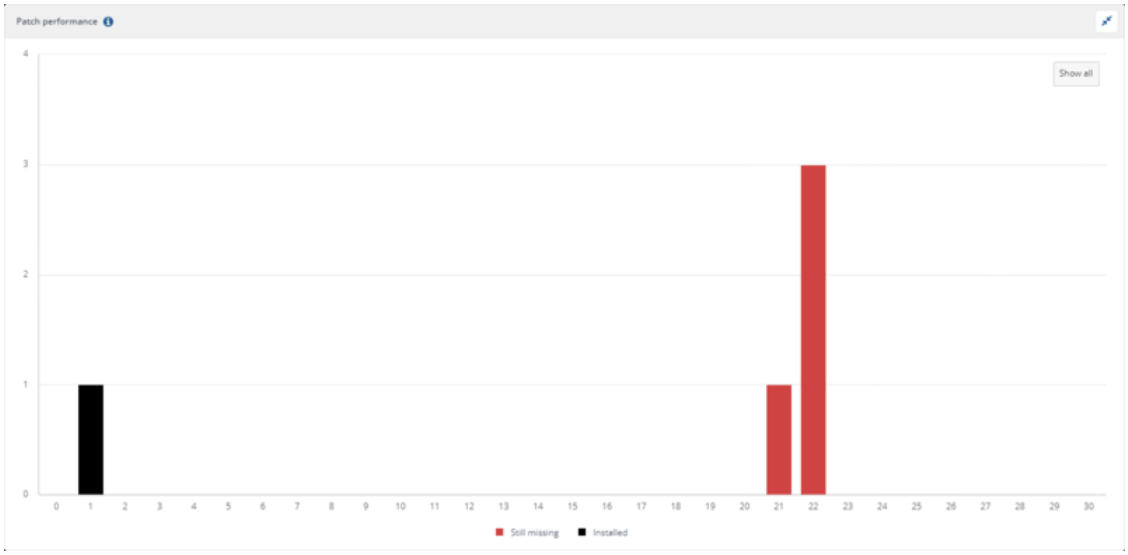
This chart displays the Performance in the last 30 Days by default, but by clicking "Show all" will show the period where the patch is missing.

The black column shows the Installed trend over time for that patch in the management group

The red column indicates the number of devices missing patches and when the patches should have been installed.

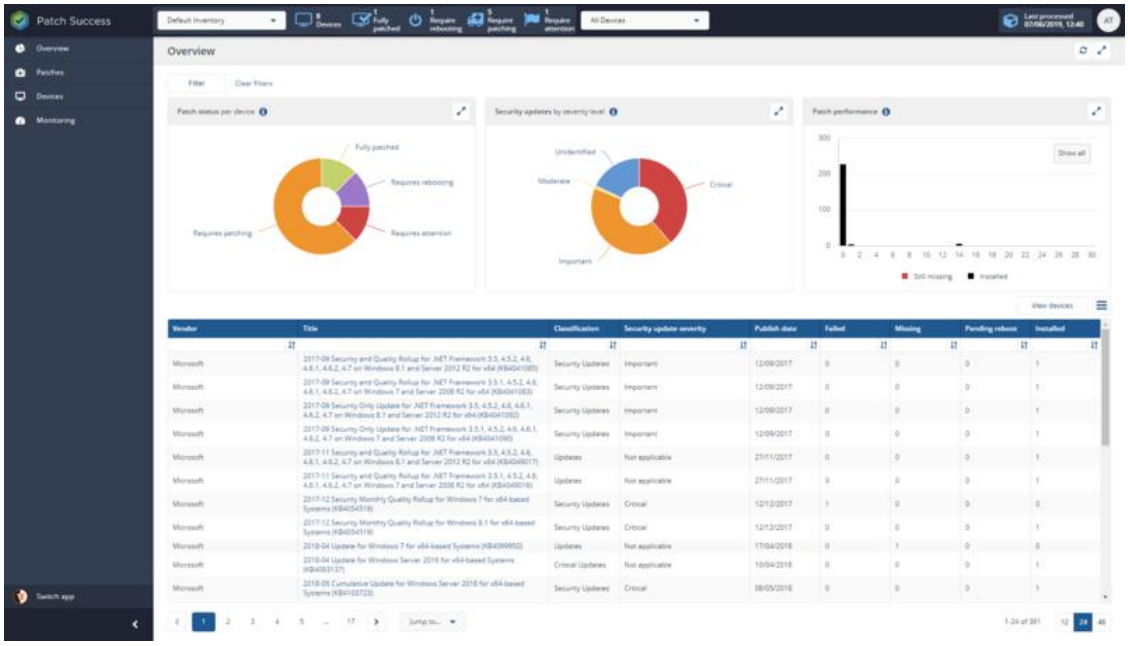
The diagram shows that the patch is still missing on 1 device in the last 21 days and 3 devices in the last 22 days in the management group. It also shows that 1 device had the patch installed 1 day after the release date.

In the **Overview** page, expand the **Patch performance** chart which has been filtered based on the selected KB.



7.4.6.2 Patching immediately any device or devices in the management group which haven't received it

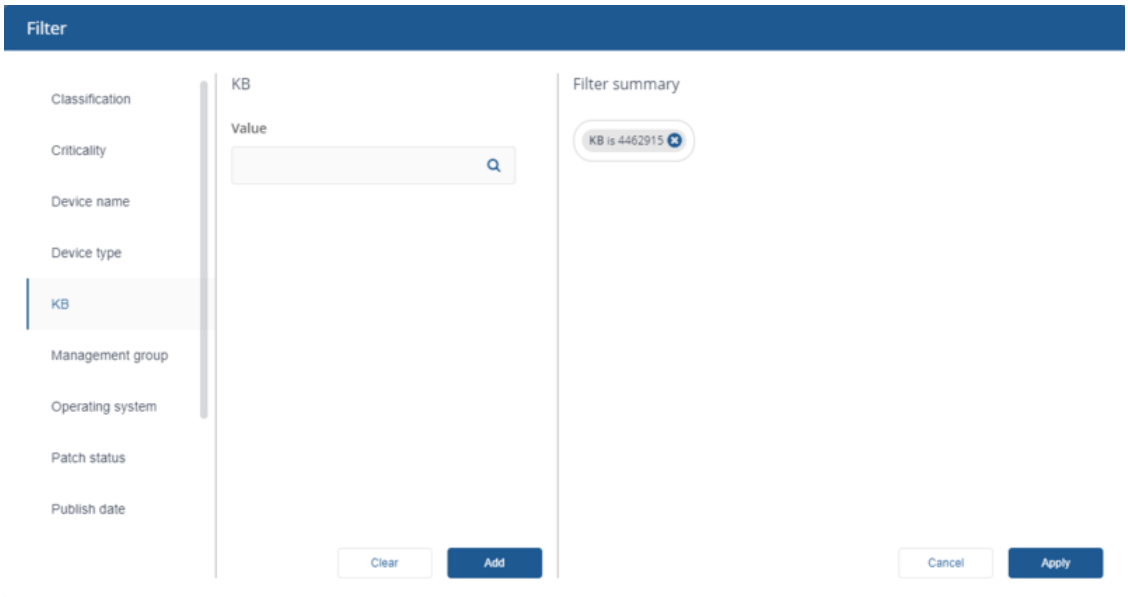
Navigate to **Patch Success→Overview**



Click on the **Filter** button and the **Filter** popup appears.

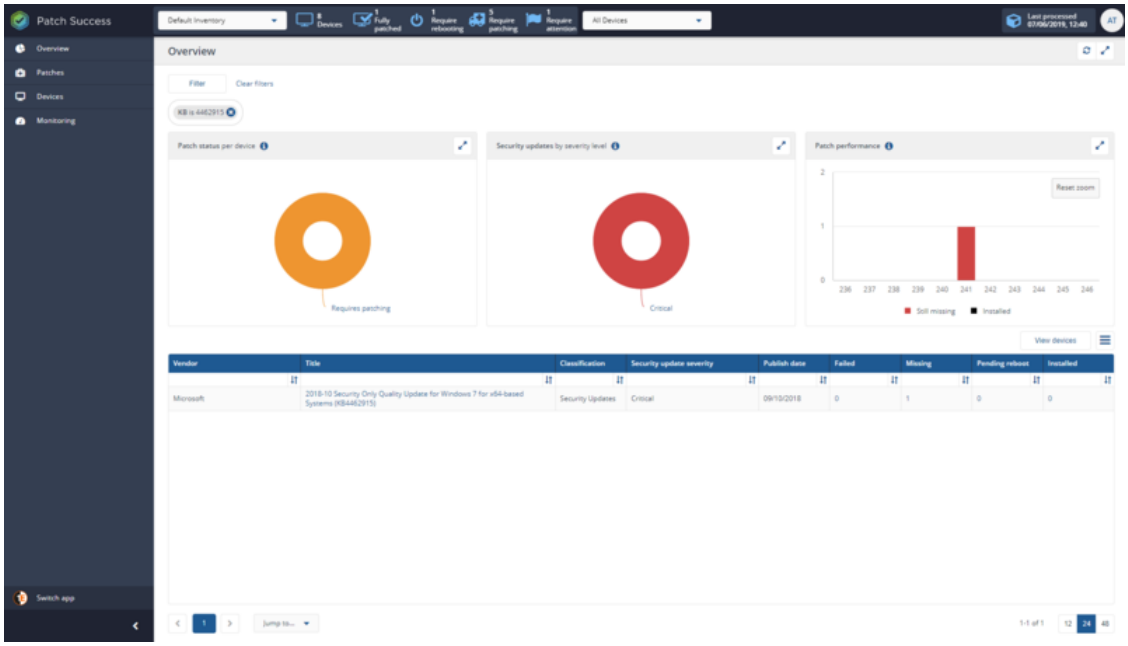
Select the **KB** filter and enter a value for the KB and a drop-down auto-fills a list of KBs, click **Add**.

In the **Filter** popup, click the **Apply** button.



In the **Overview** page, the filter has been applied to the all the charts, showing the overall status of the KB.

Click on the number in the **Missing** column. This opens a page for the specific device.



Device criticality - is criticality of a device

FQDN - is the fully qualified domain name of a device

Operating system - is the operating system of a device

User - is primary device user

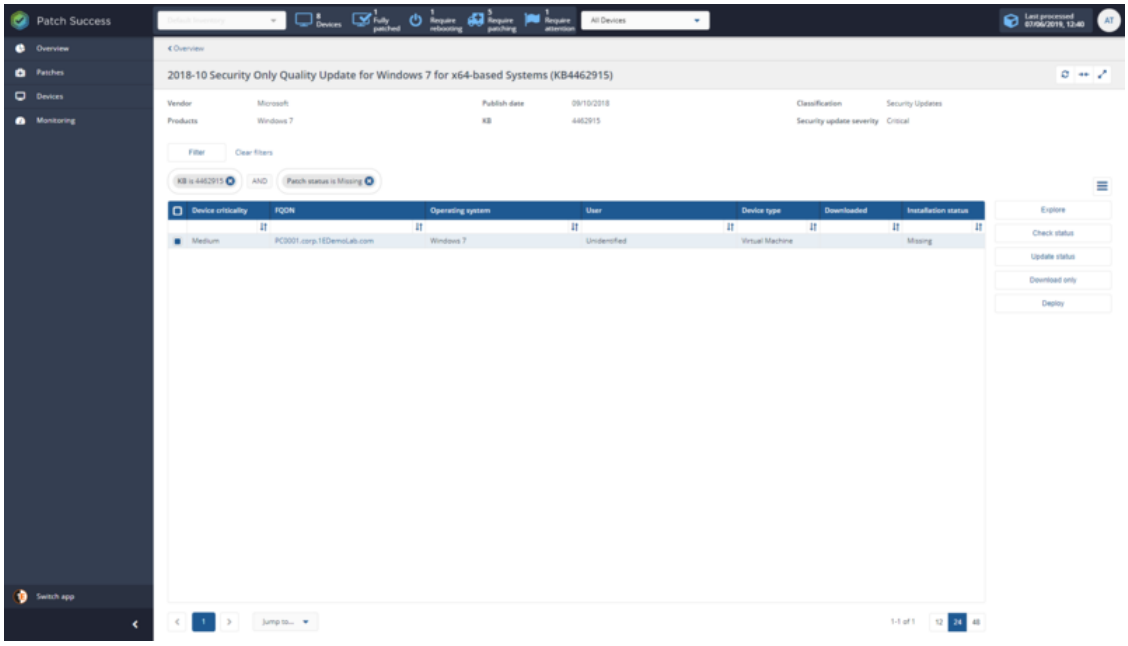
Device type - is type of device

Downloaded - is the patch already downloaded on the device

Installation status - is the status of the currently selected patch per device

On the displays patch with filter of the KB and Missing , and the List of devices shows a full list of devices where selected patch is applicable. Where:

Click the **Deploy** button. This will start an instruction to deploy the currently selected patch on the selected devices and switch to the **History** page to show the progress of the **deploy** instruction.



In **Monitoring→History** page. This shows the list of all the instructions issued by Patch Success with following details:

Instruction performed - a description of the instruction.

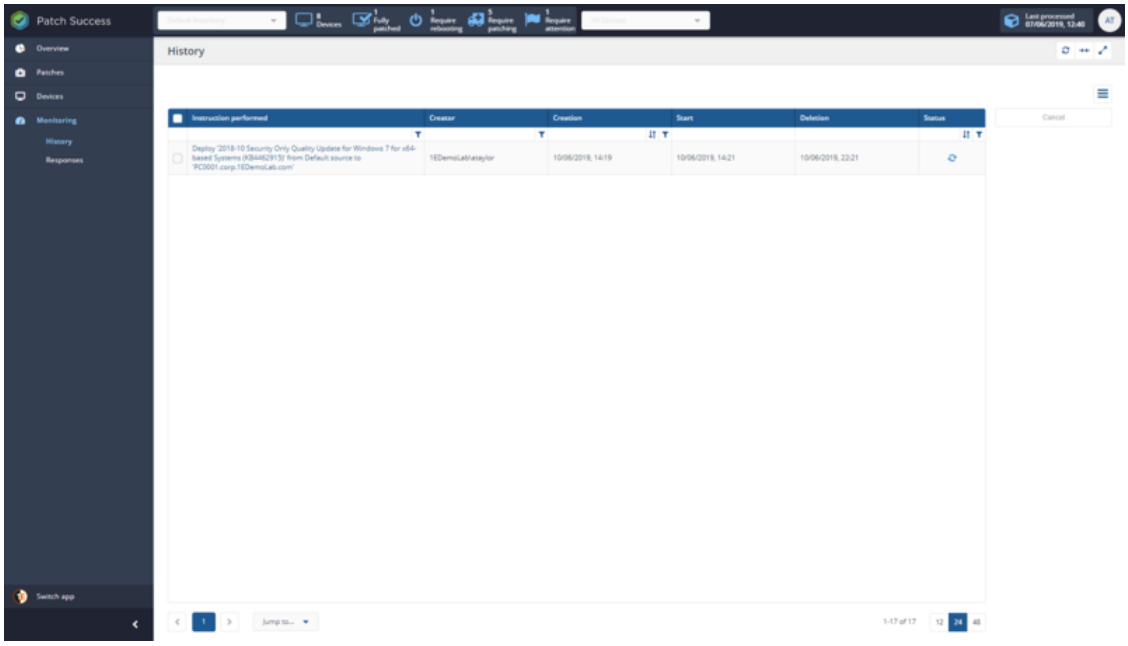
Creator - user that has created the instruction

Creation- creation time

Start - time at which the instruction was started

Deletion - time at which the instruction has ended

Status - current status of the instruction



In **Instruction Responses** page. This shows the list of all the responses received by Patch Success from the issued instruction, with following details;

Response time - time at which the response was received

FQDN - fully qualified name of the device that has responded

Title - title of the targeted patch.

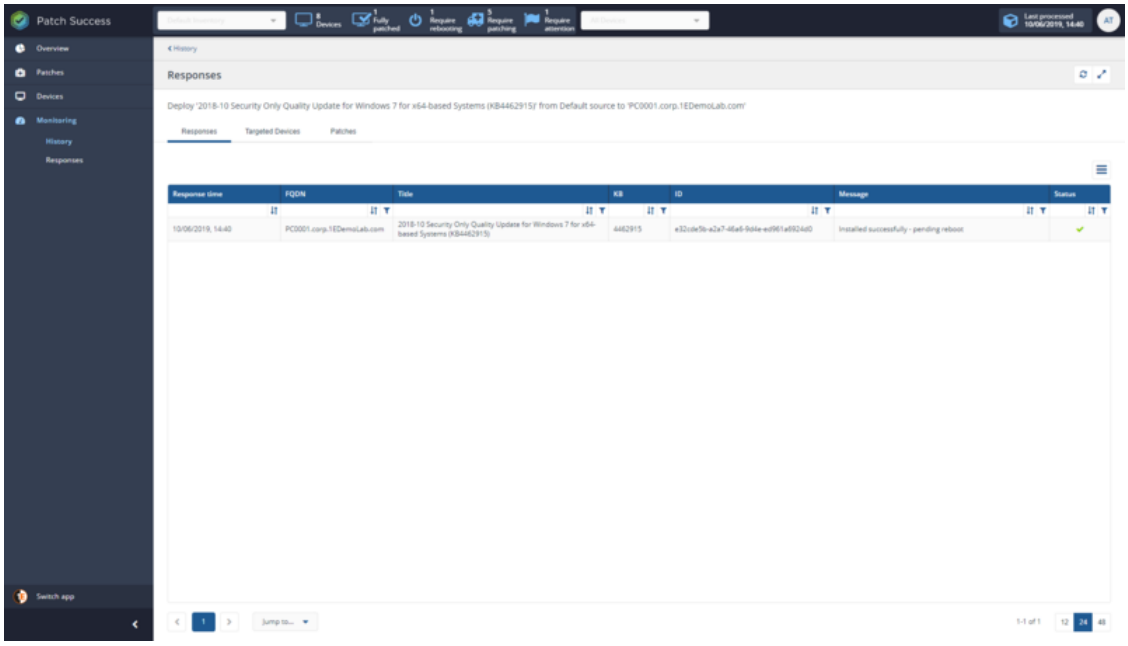
KB - knowledge base number for the corresponding patch.

ID - identifier for the corresponding patch.

Message - the result of the instruction.

Status - the status of the response.

Once the response is completed, navigate back to **Overview**. If you have remained in session then your previous filter will still be current. The missing patch will no longer display and will now show as installed. Furthermore, when you look at the **Device Patch Status** chart the device no longer reports as requiring attention, but rather as **Fully patched**.



7.5 Troubleshooting

A general methodology for investigating issues with Patch Success, as well as identifying key issues and their resolutions.

For known issues relating to specific components, please refer to the respective troubleshooting pages:

Clients	Platform	Applications	Integration
1E Client	1E	Endpoint Automation	1E Core for ServiceNow
1E Client Deployment Assistant		Experience Analytics	1E ITSM Connect for ServiceNow
PXE Everywhere		Endpoint Troubleshooting	1E Service Catalog Connect for ServiceNow
		Writing 1E Instructions (1E SDK)	1E Virtual Assistant

7.5.1 1E Support contact details

7.5.1.1 Support Web portal

Maintenance support customers can log onto the 1E Support Web Portal at https://support.1e.com/ using the login details provided with their maintenance contract. This provides issue tracking, product hotfixes, and knowledge base articles related to each product.

7.5.1.2 Telephone support

Maintenance support customers can contact the technical support department at 1E through the following support numbers. Just phone the relevant number for your area, so your call can be routed quickly and efficiently to the correct support group:

US/Canada:	1-866-349-4032 (Toll-Free)
	1-917-339-2360 (Standard)
UK/Europe:	+44 (0)208 326 3499
India:	+91 120 402 4002
Australia:	+61 739 111 118

7.5.1.3 Email support

Maintenance customers can use the following email for additional support. Evaluation customers can also use this email with the temporary access code that is provided through customercare@1e.com as part of their evaluation.

support@1e.com

7.5.2 The technical support process

Read through the Troubleshooting pages to see if there are known issues, or quick resolutions to any problems you may have encountered.

Maintenance support customers can use the 1E Support Web Portal to review knowledge base articles and download hotfixes.

If still encountering problems, create a technical report (log files and details) and then contact the 1E technical support team.

7.5.2.1 Creating a technical report

If possible, please obtain the following details and log files before contacting 1E, to include in your technical report.

7.5.2.1.1 Version details

The OS, version number, and patch level for:

Tachyon Servers

1E Client

Configuration Manager - if used

Other 1E Server software, for example, Shopping, Nightwatchman, and WakeUp.

For Nomad and Shopping, please provide OS, version number, and patch level for:

Configuration Manager DPs

Nomad extensions used on Configuration Manager Consoles

ActiveEfficiency Server.

7.5.2.1.2 Environmental details

If there were any recent changes made to your configuration

The name of the machines, Configuration Manager Application and/or Package IDs for when the issue occurred

7.5.2.1.3 Problem details

When did the issue occur, ensure log files cover this period

The scope of the issue – did it affect a particular geographical location, group of users, or client machines

Details of any self-help troubleshooting steps you carried out

In the event of a service crash or if you are experiencing high CPU or memory usage, provide us with the dump file, event viewer logs, and traces. We will provide you with FTP details to upload these files.

7.5.2.2 Log files

7.5.2.2.1 Tachyon Server log files

For any issue, please provide a zip containing log files from the following locations:

%ALLUSERSPROFILE%\1E\Catalog*.log

%ALLUSERSPROFILE%\1E\ContentDistribution*.log

%ALLUSERSPROFILE%\1E\Platform Consumers*.log

%ALLUSERSPROFILE%\1E\SLA Platform*.log

%ALLUSERSPROFILE%\1E\Tachyon*.log

If you are having licensing issues, please include:

%ALLUSERSPROFILE%\1E\Licensing*

Please refer to the Tachyon Platform 8.1 - Log files page for more details.

7.5.2.2.2 1E Client logs on Windows

%ALLUSERSPROFILE%\1E\Client\1E.Client.log (used by 1E Client and Tachyon features, and Shopping client)

%ALLUSERSPROFILE%\1E\Client\NomadBranchUninstall-YYYY_MM_HHTMM_HH_SS_000Z.log

7.5.3 Known Issues

Lists of the current known issues with implementing, configuring, and using 1E Patch Success.

If you cannot find an issue and its workaround on this page:

Refer to Known issues for the Platform and other applications.

Try searching the 1E Support Portal https://support.1e.com/ for issues that have hotfixes.

If you need further help, please refer to the Troubleshooting page for how to contact 1E Support and the technical support process.

Issue	Description	Workaround
Patch Success instructions that are using SCCM as a patch source log remote connections to Microsoft WSUS server.	1E Client logs creating a remote connection to Microsoft WSUS Server with a CheckOnline property set to false to indicate that 1E Client is using Windows Update Agent local cache to retrieve data. This log can easily be interpreted as an attempt to connect to the internet to collect data, which is not what the 1E Client is doing. Instead, the instructions are collecting additional information from WUA local cache in order to supplement missing data collected by ConfigMgr client and will therefore be regularly logged during normal operation of Patch Success instructions. ConfigMgr client omits Patch IDs for all installed patches and therefore requires additional information to be collected from a different source to match missing Patch IDs.	The log message should be interpreted as 1E Client performing a query against a Windows Update Agent local cache.
Deploying a missing patch directly via the internet returns the following error	If a missing patch is deployed onto a target device, but the Windows Update service is not running or	Ensure the Windows Update service is running

Issue	Description	Workaround
"overallDownloadResult is Null"	stopped, the 1E Client will return error: "overallDownloadResult is Null" In later versions of the 1E Client, the returned error will be: "End search for updates because: (0x8024001E). Operation did not complete because the service system was being shutdown"	before attempting to re-deploy the patch.
Deploying a missing patch to 1E Client may result with it logging "WARN - No updates to install" and the patch gets updated as "Not applicable"	If a missing patch is deployed, but there is no associated deployment package in ConfigMgr then the response will be returned as "Not applicable".	Ensure the patch has been packaged and deployed through ConfigMgr so that it is available to the CM clients before attempting to re-deploy the patch.
Patch Success charts and tables have inconsistent data.	Tachyon sync schedule process leads to new patch data being replaced with stale patch data when BI ETL is run. When syncs are scheduled in the recommended way then the nightly BI ETL will replace all device and patch data in the BI star schema and cube with potentially stale SLA inventory data.	Execute a new Tachyon sync, once the expected devices have reported in patch data (check Tachyon Explorer → Instructions → History → "Returns Patch status for...") then execute a new BI ETL. This will result in up to date device and patch data in both the BI star schema and the cube.
Deploying a patch directly via the internet may return failure "End search for updates failed because: Not enough storage is available to complete this operation" and WindowsUpdate.log will show an associated error:	On Windows 7 / Server 2008 R2 there is a known issue with the Windows Update that causes it to return an "8007000E" error message. This may be seen if in the Patch Success page, a patch is deployed with the check box enabled for	Please ensure the update that contains the improvements to Windows Update Client is applied in order to allow for further Patch Success deployments to function correctly.

Issue	Description	Workaround
"WARNING: WU client failed Searching for update with error 0x8007000e"	"Enable patches to be downloaded onto devices directly from the internet instead of the default (SCCM)".	
History page should be hidden when user only has Patch success viewer permissions	The history page is displayed when a user has no access to Patch Success instructions.	None
Patch Success will show all devices irrespective of the permissions on management groups.	BI cube does not have the permissions model required to filter the management groups correctly. In addition, the permissions model only assigns management groups to instructions therefore will not cater for BI cube permissions.	None

7.6 Reference

All the list type information, such as installer properties, in alphabetical lists etc.

7.6.1 Patch Success release information

7.6.1.1 1E Patch Success 8.1 release information – last updated 04-August-2022

These notes contain late-breaking information about this release of Patch Success. For the most up-to-date information, please see the online readme. You should read these release notes and the online documentation for Patch Success thoroughly before using the software.

7.6.1.1.1 New features in 1E Patch Success 8.1

Works with Tachyon Platform 8.1

No features or feature changes added in this release, but includes any hotfixes from previous versions.

7.6.1.1.2 Online help

Tachyon comes with online help that shows you how to install, configure and use the product. Click the following link to view the help:

1E Patch Success documentation.

For support queries, please:

Use https://support.1e.com/ where you can search the KB or submit a support case.

Contact support@1e.com.

7.6.1.1.3 Known issues

The current known issues related to Patch Success can be found on the Troubleshooting Known Issues page of the Patch Success documentation.

Known issues for the Platform and other applications can be found in the1E platform - Known issues documentation.

7.6.1.2 Patch Success Release History

Patch Success is a separately licensed application in the Tachyon Platform. Please refer to Tachyon release information for latest information, where you will also find details of previous releases, and hotfixes.

7.6.1.3 Patch Success features by release

A list of the Patch Success features organized by the release they were implemented in. Links through to the features have been provided for convenience.

7.6.1.3.1 New Features

Works with Tachyon Platform 8.1

No features or feature changes added in this release, but includes any hotfixes from previous versions.

7.6.1.3.2 Release History

7.6.1.3.2.1 Patch Success 8.1

Works with Tachyon 8.1

No features or feature changes added in this release, but includes any hotfixes from previous versions.

7.6.1.3.2.2 Patch Success 8.0

Works with Tachyon 8.0

No features or feature changes added in this release, but includes any hotfixes from previous versions.

7.6.1.3.2.3 Patch Success 1.3

Works with Tachyon 5.2

Unidentified patch publish dates show 'Not available' instead of 1970-01-01.

7.6.1.3.2.4 Patch Success 1.2.104

Works with Tachyon 5.1

No changes to this application for this release.

7.6.1.3.2.5 Patch Success 1.2

Works with Tachyon 5.0

The Patch and Device details pages now allow updating of all devices and patches for a given patch or a device respectively

Performance improvements.

7.6.1.3.2.6 Patch Success 1.1

Works with Tachyon 4.1

The **Patch performance** dashboard tile can now be used to interactively filter the page

A new **Monitoring** menu has been added that displays the history and responses for the Patch Success instructions

Download only functionality

Integration with Guaranteed State via **CM Patch Health** policy link.

7.6.1.3.2.7 Patch Success 1.0

Works with Tachyon 4.0

Patch module included in Tachyon Agent 4.0

7.6.2 1E Companion Products

A list of the feature dependencies between Patch Success and other 1E companion products.

This page describes the dependencies to and from Patch Success in regard to certain features that are implemented across companion 1E products. To view the general platform related dependencies for Tachyon please refer to Tachyon 8.1 - Supported Platforms.

7.6.2.1 1E companion products that 1E Patch Success 8.1 depends on

Supported versions of 1E companion products that 1E Patch Success 8.1 features depend on.

Products and features that Patch Success depends on	Supported versions of companion products	
1E SLA Business Intelligence	Business Intelligence and a SQL Server Analysis Server (SSAS) instance. Business Intelligence is installed using Tachyon Setup.	Business Intelligence 8.1 (included in Tachyon Platform 8.1)
1E Catalog	1E Catalog is installed using Tachyon Setup.	1E Catalog 8.1 (included in Tachyon Platform 8.1)

Products and features that Patch Success depends on	Supported versions of companion products	
1E Client	Tachyon requires the 1E Client (with Tachyon client features enabled) to be installed on all client computers. This replaces the legacy Tachyon Agent. Tachyon client features: the Patch Success application # command and script execution content distribution device criticality manipulation of files and processes manipulation of registry and WMI # security # software uninstallation user sessions, including Primary User Real-time response to instructions, which supports the retrieval of information using questions, and running actions Tags (freeform and device/coverage) Criticality and Location 1E Client UI to support the Real-Time Control Center, Announcements, Surveys, and Sentiment features of the Experience application # Inventory, including process usage, to support: the Tachyon Activity Record feature the Inventory and other consumer applications	1E Client 8.1 (with Tachyon client enabled) 1E Client 8.0 (with Tachyon client enabled) 1E Client 5.2 (with Tachyon client enabled)

Products and features that Patch Success depends on	Supported versions of companion products	
	Performance metrics features to support the Experience application # Policy feature to support consumer applications: Guaranteed State ##, Experience #, and Nomad # Modules to support: # not supported on non-Windows, ## partially supported on non-Windows Tachyon clients can optionally use the Nomad client module of 1E Client to more efficiently download content.	
Tachyon Platform	Patch Success is a consumer application of the Tachyon Platform, installed on the Tachyon Master Stack, and requires a full Tachyon infrastructure.	Tachyon Platform 8.1

Note

Tachyon Platform, 1E Catalog, Business Intelligence, and Patch Success, are all installed using Tachyon Setup.

7.6.2.2 1E companion products that depend on 1E Patch Success 8.1

Supported versions of 1E companion products with features that depend on 1E Patch Success 8.1.

Products and features that depend on Patch Success	Supported versions of companion products	
None	n/a	n/a

7.6.3 1E Patch Success product pack

Classic Product Pack used to create the **1E Patch Success** instruction set required by the Patch Success application.

For more details please refer to:

Configuring Patch Success for steps required to upload this product pack and create set

Using Patch Success.

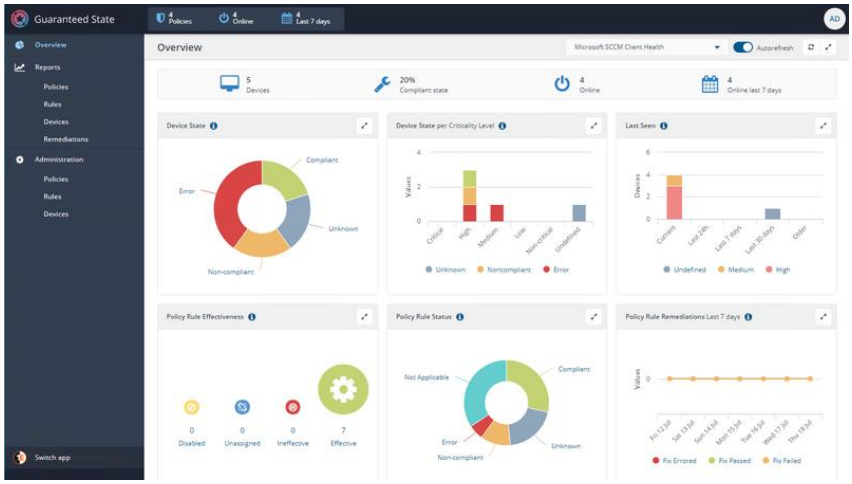
Instruction text (ReadablePayload)	Type	Description	Instruction file name	Version
<action> patch(es) specified by <patchSpec> identifier(s) from <source> source to targeted device(s) Where: **<action>** is either **Deploy** or **Download only** **<patchSpec>** is a list of comma separated GUIDs and/or KB numbers (without KB prefix) of patches to be installed **<source>** is the patch download source: **WSUSR** - Microsoft Update via the Internet **WSUSL** - WSUS **SCCM** - Configuration Manager **Default** - the value of **PatchSuccessSource** in the **GlobalSettings** table of the **TachyonMaster** database, as described in Configuring Patch Success: Configuring the source for Patch downloads.	Action	Deploys a specific patch or patches to targeted devices. **Note** Unlike the other instructions, the **<patchSpec>** parameter in this instruction does not support **all**. You must be specific which KBs you want to deploy. This instruction is used by the **Deploy** and **Download only** buttons, which allow users to deploy selected patches to devices. The **1E Patch Success Actioners** role requires **Actioner** permissions to see the **Deploy** and the **Download only** buttons. See Patch.Deploy in the Tachyon SDK.	**1E-PatchSuccess-Deploy**	5

Instruction text (ReadablePayload)	Type	Description	Instruction file name	Version
Returns patch status from <source> for <patchSpec> identifier(s) Where : **<source>** is the patch download source, as above **<patchSpec>** is either **all**, or a list of comma separated GUIDs and/or KB numbers (without KB prefix) of patches to be reported.	Question	Returns patch status for given KB article numbers on targeted devices. The instruction is used by the **Check Status** button, which allow users to check the patch status of the selected patches and represent the results in Explorer for further investigations. The **1E Patch Success Actioners** role requires **Questioner** permissions to see the **Check Status** button. See Patch.List in the Tachyon SDK.	**1E-PatchSuccess-Explore**	5
Returns patch status from <source> of given<patchSpec> identifier(s) for PatchSuccess consumption Where: **<source>** is the patch download source, as above **<patchSpec>** is either **all**, or a list of comma separated GUIDs and/or KB numbers (without KB prefix) of patches to be reported.	Question	Returns patch status for all known patches on targeted devices. Information is based on offline cache. When run, its response data is offloaded direct to the SLA-BI cube. The instruction is used by the **Update Status** button, which allows users to update the dashboard with the status of selected patches, to see for example **Pending reboot** and **Installed** states. The **1E Patch Success Actioners** role requires **Questioner** permissions to see the **Update status** button.	**1E-PatchSuccess-Refresh**	5

Instruction text (ReadablePayload)	Type	Description	Instruction file name	Version
		See Patch.List in the Tachyon SDK.		

8 Guaranteed State

Tachyonis a systems management tool that turns the traditional systems management model on its head. Guaranteed State is based on the concept that a device is aware of its own current state more accurately than any centrally held repository. Also, if you can query the device directly then the need to store masses of data becomes unnecessary.



8.1 Introducing Guaranteed State

An overview of Guaranteed State is presented; what it does and how it can benefit your organization.

8.1.1 Guaranteed State Concepts

Concepts used by the Guaranteed State application, which ensures device compliance with enterprise IT policies.

8.1.1.1 Overview

Guaranteed State allows you to easily check and enforce device state. Device state can represent just about anything you'd like to be set in a certain way for a collection of devices.

> **Note**
>
> Before using Guaranteed State you need to configure it and upload some policies (with their rules, triggers and preconditions), please refer to:

Configuring Guaranteed State

Uploading Integrated Product Packs

Deploying a Policy.

Once you have imported an Integrated Product Pack you can configure and deploy policies to manage various device attributes. For example:

Registry keys

Services

Config Manager metrics such as client cache usage

Disk free space

WMI namespaces and classes.

8.1.1.2 Integrated Product Packs

Integrated Product Packs are Zip files containing Guaranteed State policies, but can also contain instructions (as an alternative to classic Product Packs which can only contain instructions). They have a folder structure and files as shown in the following table (except for manifest.xml) all folders and files are optional.

You can upload these Zip files into Tachyon using the Tachyon Product Pack deployment tool, please refer to Uploading Integrated Product Packs for details.

Folder	Sub-folder	Files
Fragments	Check	xml files, each containing the definition of a **check fragment**
Fix	xml files, each containing the definition of a **fix fragment**	
Precondition	xml files, each containing the definition of a **precondition fragment**	
InstructionSets	<Instruction Set Name>	xml files, each containing the definition of an **instruction**
Policies	xml files, each containing the definition of a **policy** (a list of rules)	

Folder	Sub-folder	Files
Rules	xml files, each containing the definition of a **rule** (a list of fragments, triggers, and their parameter values)	
TriggerTemplates	xml files, each containing the definition of a **trigger template** and its available parameters	
manifest.xml	xml file containing name, description and version details that are only used for display by the **Product Pack Deployment tool** The presence of this file indicates the zip file is an Integrated Product Pack.	
<policy>.ico	icon file that is referenced in the manifest.xml (Not currently used).	

1E provide a number of ready-made policies which are described in the Integrated Product Packs pages:

MEMCM Client Health Policy

Implementing MEMCM Client Install fix

Nomad Client Health Policy

Windows Client Health Policy

Tachyon Core Utilities

These pages include lists of instructions, policies, rules, fragments (preconditions, checks and fixes) and trigger templates. The lists have links to more detailed information about each pack in the Tachyon Product Packs reference.

You can also create your own policies using rules, fragments and triggers from other Integrated Product Packs, for example, the Tachyon Core Integrated Product Pack.

8.1.1.3 Policies and Rules

Guaranteed State is enforced by the Tachyon client at each device using one or more policies that are deployed to devices according to their management group memberships.

A policy consists of one or more rules, which fall into two primary categories:

Category	Explanation
Check	Allow you to verify that a device has a particular state, such as a registry key having a specific value. You can then view summary and detail reports which show devices that are compliant and not compliant with the check rules.
Fix	Allow you to define a desired state for the device and then enforce that state. For example, you could mandate that a registry key exists and contains a specific value. Again, you can report on the application of these fix rules to devices.

Management groups use rules to determine device membership, enabling the devices to be administered as a group. For example, you can select devices based on their Active Directory Organizational Unit, or their operating system version, or any other criteria available to the management group rules. Please refer to Management Groups page page for details.

You can also create your own policies using rules, fragments and trigger templates from any Integrated Product Pack that you have uploaded, which are fully configurable, please refer to Defining your own policy for details.

The following are examples of check and fix rules provided by the **Tachyon Core Integrated Product Pack**:

1E-GuaranteedState-General-Check-RegistryValue

1E-GuaranteedState-General-Fix-RegistryValue

1E-GuaranteedState-General-Check-ServiceState

1E-GuaranteedState-General-Fix-ServiceState

8.1.1.4 Fragments

Fragments is a collective term for Rules, Trigger templates and Preconditions which are written in the Tachyon instruction language SCALE.

8.1.1.5 Triggers

Triggers define the conditions which will cause a rule to be evaluated. Each check rule and fix rule must have a rule trigger defined using a trigger template.

The following are examples of trigger templates provided by the **Tachyon Core Integrated Product Pack**:

TriggerTemplate-IntervalHours

TriggerTemplate-IntervalMinutes

TriggerTemplate-IntervalSeconds

TriggerTemplate-ProcessCrash

TriggerTemplate-ProcessLaunch

TriggerTemplate-ServiceStatusChange

TriggerTemplate-WindowsEventLog

TriggerTemplate-WindowsRegistryChange.

8.1.1.6 Preconditions

Both check rules and fix rules may have optional preconditions defined.Preconditions allow you to define a conditional test that must be met before the rule is evaluated.

> **Note**
>
> A precondition is not required. If you do not specify a precondition, then the rule is always evaluated when the trigger fires.

The following are examples of preconditions provided by the **Tachyon Core Integrated Product Pack**:

1E-GuaranteedState-General-PreCondition-InstalledSoftware

1E-GuaranteedState-General-PreCondition-MinWindowsVersion

1E-GuaranteedState-General-PreCondition-MinWindowsVersionAndVariant

1E-GuaranteedState-General-PreCondition-OperatingSystem

1E-GuaranteedState-General-PreCondition-OSAndSoftware

1E-GuaranteedState-General-PreCondition-OsTypeAndArchitecture

1E-GuaranteedState-General-PreCondition-Service

1E-GuaranteedState-General-PreCondition-WindowsDevice

8.1.1.7 Dependencies

Check rules require a:

Trigger

Check.

You can also optionally add a precondition.

Fix rules require a:

Trigger

Check

Fix.

You can also optionally add a precondition.

> **Note**

Be sure that you understand the key differences between **Check Rules** and **Checks and Fix Rules** and **Fixes**:

A **Check Rule** defines a **Check**, including a trigger and optional preconditions

A **Fix Rule** defines a **Check and a Fix**, including a trigger and optional preconditions. a fix is applied when a check is performed and the check result indicates a compliance failure.

8.1.1.8 Rule outcomes

A rule always returns two items to the Tachyon subsystem. One is a Pass/Fail value and the second is an arbitrary data item. A rule can also return an error status to the subsystem. This can occur if the rule logic terminates unexpectedly, for example, because a file could not be found etc.

Guaranteed State history will show the result of rule evaluation. It will clearly indicate whether a check rule returned a success (compliance), failure, or error. It will also show whether a fix rule (if applicable) indicated success, failure, or returned an error.

Note

Four things you should know about rule outcomes:

A check or fix rule that fails or results in an error causes a device to remain non-compliant from a Guaranteed State perspective.

History entries are only created in Guaranteed State when an overall compliance transition occurs, for example from false to true or true to false.

If the precondition for a rule returns failure on a device when evaluated, then the Guaranteed State subsystem indicates 'not applicable' against the device compliance status for the rule.

Rules that return 'not applicable' do not affect device compliance status. If all rules for a device returned 'not applicable' the device would still be regarded as compliant.

8.1.2 Guaranteed State Features

An overview of Guaranteed State features.The Guaranteed State application gives you the ability to ensure device compliance with enterprise IT policies. For more information please refer to the Using Guaranteed State section of this documentation.

Note

1E provide Integrated Product Packs contain some ready-made policies. Please refer to Uploading Integrated Product Packs for more details.

8.1.2.1 Policies and Rules

The Guaranteed State of a device is enforced by the Tachyon client at the device. One or more policies are deployed to devices according to the management groups the devices belong to. Each policy consists of one or more rules that are either check rules or fix rules.

Rule	Explanation
Check	Allow you to verify that a device has a particular state, such as a registry key having a specific value. You can then view summary and detail reports which show devices that are compliant and not compliant with the check rules.
Fix	Allow you to define a desired state for the device and then enforce that state. For example, you could mandate that a registry key exists and contains a specific value. Again, you can report on the application of these fix rules to devices.

For an explanation of management groups, please refer to the Management Groups page page. Management groups allow devices to be flexibly grouped, based on management group rules. This means you can easily administer devices based on, for instance, their Active Directory Organizational Unit, or their operating system version, or any other criteria supported by the management group rules.

Note

For more information on policies and rules please refer to:

Defining your own policy

Integrated Product Packs.

8.1.2.2 The Guaranteed State Overview page

The **Overview** page lets you view the current state of your enterprise in terms of the devices and policies that have been defined and applied. It consists of a number of charts that let you monitor the state in real-time.

Note

For more information on the Guaranteed State Overview page please refer to:

Guaranteed State Overview page

8.1.2.3 Guaranteed State Reports

The Guaranteed State application provides three reports that let you view the details for the currently defined **Policies**, **Rules** and **Devices**. The information in these reports is consolidated into the **Guaranteed State Overview** page charts.

Note

For more information on the **Policies**, **Rules** and **Devices** reports pages please refer to:

Guaranteed State Overview page

8.1.2.4 Exploring devices

Guaranteed State provides a **Devices** page where you can view the currently connected devices. On this page you can also select one or more of the devices and click an **Explore** button that

launches the **Explorer** application. You can then run an instruction using the selected devices as the coverage for the instruction.

> **Note**
>
> For more information on exploring devices please refer to:

Using Explorer to investigate devices in Guaranteed State.

8.1.2.5 Device Criticality

Device criticality is an attribute of a device that defines its importance within an organization. The default definition in Tachyon has these settings:

Undefined (or not set)

Non-critical

Low

Medium

High

Critical.

At present, criticality settings do not affect the primary operation of Guaranteed State. However, it is possible to use Tachyon to set device criticality and to view it within Guaranteed State.

Tachyon also supports the use of the criticality setting when defining coverage for an instruction. For example, you can target an instruction to be sent only to devices whose criticality is not **Critical**.

> **Note**
>
> For more information on device criticality please refer to:

Using Device Criticality.

8.2 Implementing Guaranteed State

Everything you need to know about getting Guaranteed State installed and running in your network. This section is structured in a way that leads you through the three phases of a typical implementation project.

Design, including requirements

Install, including preparation

Verify.

8.2.1 Design Considerations

The Design Considerations for Guaranteed State can be found on the Implementation Overview page.

8.2.2 Requirements

The Requirements for Guaranteed State can be found on the Planning for Tachyon pages.

8.2.3 Preparation

The Preparation for Guaranteed State can be found on the Preparation page.

8.2.4 Installing and upgrading

How to set up Tachyon Serverand deploy Tachyon clients, including a guide to upgrading.

At its minimum, Tachyon consists of two components: Tachyon Server and 1E Client (with Tachyon features enabled). Additionally, you may install Tachyon applications on the server.

You install Tachyon Server and its applications using **Tachyon Setup**.

You deploy 1E Client on Windows PCs using the **MSI installer**, or if you have Configuration Manager you can use **1E Client Deployment Assistant** (CDA).

8.2.4.1 Tachyon Product Pack deployment tool

The Tachyon Product Pack deployment tool can be used to upload multiple Classic and Integrated Product Packs into Tachyon.

8.2.5 Uploading Integrated Product Packs

How to upload the Product Packs provided with the Tachyon release.

1E provides a number of Guaranteed State policies and Instructions with the Tachyon release on the support portal.

8.2.5.1 Getting started

Integrated Product Packs are loaded into Tachyon using the Tachyon Product Pack deployment tool. For more details please refer to Tachyon Product Pack deployment tool.

8.2.5.2 Uploading Integrated Product Packs

After installation, Guaranteed State has no immediately available policies, you will first need to load some from the **tachyonproductpacks.<version>.zip** file - this can be done using the Tachyon Product Pack deployment tool. The following steps describe how this is done:

8.2.5.2.1 Checking the status of Guaranteed State just after installation

Log on to the Tachyon portal as a Guaranteed State administrator and navigate to the **Guaranteed State→Overview** page.

Before running the Tachyon Product Pack deployment tool, you will see at the top of the **Overview** page that there are **0 Policies** available.

8.2.5.2.2 Running the Tachyon Product Pack deployment tool

Navigate to the directory where the **tachyonproductpacks.<version>.zip** file has been unzipped.

You will see two directories: **Classic** and **Integrated**.

Navigate to the **Integrated** directory.

Double-click on **Tachyon.ProductPackDeploymentTool.exe**.

Click on **Yes** in any UAC dialog displayed.

The **Tachyon Product Pack deployment tool v5.0** dialog will appear.

You must specify the URL of the Tachyon Consumer API in the **Server** field and then click on **Test Connection** to verify that you have entered the correct value. If you run the tool on the Tachyon Server, the tool will automatically prefill the URL.

The **Style** column of the **Available Product Packs** table indicates whether each **Product Pack** is **Classic** or **Integrated**. The Available Product Packs table will be populated with all the Product Pack zip files encountered in the directory the tool was launched from and all its sub-directories.

The **Select all** box can be used to select or deselect all the items in the **Available Product Packs** table.

There are five **Integrated Product Packs** provided with the release and these are listed, and also selected, in the **Available Product Packs** table:

Endpoint Performance

Microsoft SCCM Client Health

Nomad Client Health

Tachyon Core

Windows Client Health

Uploading Product Packs is done by clicking the **Upload selected** button, which uploads all the selected items in the **Available Product Packs** table.

The progress of the upload is displayed in the **Results** field. When the upload has finished the word **Done.** will be displayed in the **Results** field.

After uploading has completed you can click the **Close** button on the deployment tool.

> **Tip**
>
> You can specify the parameters on the command-line as decribed in Tachyon Product Pack deployment tool:
>
> **-url "<ConsumerAPI>"** for example: **-url "https://tachyon.acme.local/Consumer"**.
>
> **-log <level>** for example **-log DEBUG**

8.2.6 Configuring Guaranteed State

What you need before using Guaranteed State.

In this version of Tachyon, you only need to configure users with the following roles to use and administer Guaranteed State:

Guaranteed State Viewers role, who can view the dashboards or an administrator

Guaranteed State Administrators role to upload, create and manage policies.

8.2.6.1 Prerequisites

To configure Guaranteed State, you will need the following:

An appropriate Tachyon License to permit using Guaranteed State. This is normally included in a standard Tachyon license.

A **domain security group** representing Guaranteed State Administrators who will use the Tachyon Guaranteed State application.

The steps below describe how a Tachyon user will be created for this group, and a role which grants access to the Guaranteed State pages and instructions.

A Tachyon user with the following role permissions:

Permissions Administrators role in order to create the above Tachyon user for the security group

Guaranteed State Administrators role to upload, create and manage policies (optionally member of the above security group)

Instruction Set administrator role to upload instructions

Log Viewers role to aid troubleshooting (optional).

One or more Integrated Product Packs.

> **Note**
>
> This process assumes you have already verified your Tachyon installation and have Tachyon clients deployed on some Windows devices.

8.2.6.2 Assigning users to the Guaranteed State Administrators role

To optionally create a new user:

Navigate to the **Settings**→**Permissions**→**Users** page.

Click the **Add** button to start the add user process.

In the **Add user** popup subsequently displayed, type the name of an Active Directory account or security group in the **Select user** field.

Select a name from the search results list and click the **Add** button.

The new user will be added to the **Users** table.

To assign the new user to the **Guaranteed State Administrators** role in the:

Users table, locate the row for the new user and click on the link in its **Name** column.

User : <user/group> page, click the **Edit** button.

Edit roles assigned to user popup, scroll down the list and check the checkbox for the **Guaranteed State Administrators** role.

Click **Save**.

To verify:

Logon to the Tachyon Portal using a Tachyon user account with the new **Guaranteed State Administrators** role.

> **Note**
>
> Guaranteed State can be reached directly using the following URL:
>
> `https://<tachyon DNS Name FQDN>/Tachyon/App/#/guaranteedstate/`
>
> where <tachyon DNS Name FQDN> is the one set up during the preparation phase, as described under the heading Preparation: DNS Names.

Navigate to the **Guaranteed State→Overview** page.

8.2.7 Verifying

The verifying considerations for Guaranteed State can be found on the 1E platform - Verifying page.

8.3 Using Guaranteed State

How to use Guaranteed State to ensure endpoint compliance to enterprise IT policies.

> **Note**
>
> Guaranteed State can be reached directly using the following URL:

`https://<tachyon DNS Name FQDN>/Tachyon/App/#/guaranteedstate/`

> where <tachyon DNS Name FQDN> is the one set up during the preparation phase, as described under the heading Preparation: DNS Names.

8.3.1 Integrated Product Packs

Guaranteed State includes a set of out-of-the-box policies known as Integrated Product Packs.

This section provides information on these Integrated Product Packs which are provided with the Tachyon release and includes details on how to upload them into Tachyon.

> **Note**

The Integrated Product Packs provided with the Tachyon release include predefined values determined through testing at 1E. Some of these values can be modified to meet specific environmental requirements. You should review the Integrated Product Pack pages below for guidelines, details of the predefined values and the available customization options, prior to deploying in your environment.

If you need to further customize any of the Policies, please contact 1E.

Note

A list of the instructions, policies, rules, and fragments is provided on each of the Integrated Product Pack pages. For more detailed information, please click on the link for an instruction, policy, rule, or fragment, to see a description in the Tachyon Product Packs reference.

8.3.1.1 MEMCM Client Health Policy

Many businesses rely on Microsoft Endpoint Manager Configuration Manager (MEMCM) to deploy software, patches and updates across their company networks. It is crucial that Configuration Manager is working effectively.

The MEMCM Client Health policy monitors Configuration Manager client health and performance. It checks for cache availability, inventory cycles, service availability and Configuration Manager WMI integrity - common causes of Configuration Manager client problems on devices.

The MEMCM Client Health policy replaces the previous SCCM Client Health policy and covers the following:

Ensure the correct version of the CM client is installed and running and assigned to the correct site

Ensure the CM client is not stuck in provisioning mode

Ensure that heartbeat discovery, inventory and state messages are being sent regularly

Ensures the CM client cache is set to the correct size

Ensure the CM client log settings are correct

Ensure the BITS service exists, configured to start up automatically and is running

Ensure the Windows Time service exists with correct startup settings

Ensure the Windows Management Instrumentation (WMI) service exists, configured to start automatically and is running

Ensure WMI is healthy, the core CIMv2 and ccm namespaces and classes exist and that the WMI repository is consistent

Ensure the Windows Update service exists with correct startup settings, is configured to use the correct source (CM, WSUS or Microsoft Update) and that the service can connect to the source

Note

This policy is intended for deployment to Windows devices only.

8.3.1.1.1 Important considerations

Before deploying the MEMCM Client Health Policy you need to be familiar with its contents and comfortable that you want to apply it to the devices in your network.

By default, automated fixes in the Policies provided by 1E are not enabled, this means you will have to specifically enable the ones you want to use before they can take effect.

A new or updated Policy should first be verified by deploying it to a Management Group containing a small number of devices, reviewing the Guaranteed State reports, and confirming the checks and enabled fixes are working as expected.

When you are comfortable with the results you can then deploy to larger Management Groups.

8.3.1.1.2 MEMCM Client Health Policy reference

For details on the policy, rules, triggers, preconditions, checks and fixes available in the MEMCM Client Health Policy please refer to MEMCM Client Health Integrated Product Pack.

8.3.1.1.3 Implementing MEMCM Client Install fix

8.3.1.2 Nomad Client Health Policy

Nomad is included as part of the 1E Client, and as part of that integration, we offer a Nomad client health compliance policy in Guaranteed State. This verifies common Nomad requirements such as ACP registration, disk availability, firewall exceptions, crash notifications and cache monitoring.

The Nomad client health policy replaces the client health tile in the Nomad dashboard plus additional remediation steps:

Keeps content distribution services up and running on Nomad clients, so that users are secure and productive

Ensures Alternative Content Provider (ACP) registration configuration is set

Maintains optimal disk availability and monitors cache size for storage capacity planning

Enforces Firewall exceptions.

> **Note**
>
> This policy is intended for deployment to Windows devices only.

8.3.1.2.1 Important considerations

8.3.1.2.1.1 Configuring and verifying

Before deploying the Nomad Health Policy you need to be familiar with its contents and comfortable that you want to apply it to the devices in your network.

By default, automated fixes in the Policies provided by 1E are not enabled, this means you will have to specifically enable the ones you want to use before they can take effect.

A new or updated Policy should first be verified by deploying it to a Management Group containing a small number of devices, reviewing the Guaranteed State reports, and confirming the checks and enabled fixes are working as expected. When you are comfortable with the results you can then deploy to larger Management Groups.

Please review the following specific considerations before verifying and deploying:

Rule	Considerations
Check rule: Ensure Nomad does not have its content indexed by ConfigMgr software inventory checks	Disable this check rule if the Nomad cache location has been changed from the default C:\ProgramData\1E\NomadBranch. The corresponding fix rule is disabled by default.

8.3.1.2.1.2 Deploying

Target the Policy at separate Management Groups for Distribution Points and Nomad clients, containing only Windows devices.

If you have deployed your Nomad clients with different baseline settings then consider creating different Management Groups for them, so that it will be easier to identify the potental differences in compliance. Target all clients to begin with and then target different groups as required.

> **Note**
>
> This policy is intended for deployment to Windows devices only, so in a cross-platform estate it is advisable to deploy this policy to a Management Group that is scoped to Windows devices. If you do target non-Windows devices then preconditions for the rules ensure those devices are unaffected and rules are reported as **Not Applicable**.

8.3.1.2.2 Nomad Client Health Policy reference

For details on the following instructions, policies, check rules, fix rules, triggers and preconditions, that are included in the Nomad Client Health Policy, please refer to Nomad Client Health Integrated Product Pack.

> **Note**

Instructions

1E-Explorer-NomadClientHealth-ElectionWeightVsCriticality

Policies

Nomad Client Health

Rules

Check Nomad ActiveEfficiency connectivity status

Check Nomad can communicate through the Windows Firewall

Check Nomad can generate LSZ files on ConfigMgr distribution points

Check Nomad can hash content

Check Nomad crash dumps status

Check Nomad does not have its content indexed by ConfigMgr software inventory checks

Check Nomad has a virtual directory on ConfigMgr distribution points to perform LSZ generation

Check Nomad has sufficient disk space to download content

Check Nomad is not using the Windows temp directory for caching

Check Nomad is registered as an Alternate Content Provider with ConfigMgr

Check Nomad run status

Check Nomad variant status

Check Nomad's share directory is accessible

Check Nomad's share is accessible by specific accounts

Ensure Nomad can communicate through the Windows Firewall

Ensure Nomad does not have its content indexed by ConfigMgr software inventory checks

Ensure Nomad has a virtual directory on ConfigMgr distribution points to perform LSZ generation

Ensure Nomad is registered as an Alternate Content Provider with ConfigMgr

Ensure Nomad is running

Ensure Nomad's share directory is accessible

Ensure Nomad's share is accessible by specific accounts

Fragments

1E-GuaranteedState-Nomad-PreCondition-MultiTests

1E-GuaranteedState-Nomad-Check-AEConnectivity

1E-GuaranteedState-Nomad-Check-AlternateContentProvider

1E-GuaranteedState-Nomad-Fix-AlternateContentProvider

1E-GuaranteedState-Nomad-Check-CacheInTemp

1E-GuaranteedState-Nomad-Check-CrashDumps

1E-GuaranteedState-Nomad-Check-DiskAvailablility

1E-GuaranteedState-Nomad-Check-DpLszEnabled

1E-GuaranteedState-Nomad-Check-DpLszVirtualDirectory

1E-GuaranteedState-Nomad-Fix-DpLszVirtualDirectory

1E-GuaranteedState-Nomad-Check-FirewallExceptions

1E-GuaranteedState-Nomad-Fix-FirewallExceptions

1E-GuaranteedState-Nomad-Check-HashingEnabled

1E-GuaranteedState-Nomad-Check-Share

1E-GuaranteedState-Nomad-Fix-Share

1E-GuaranteedState-Nomad-Check-ShareAccount

1E-GuaranteedState-Nomad-Fix-ShareAccount

1E-GuaranteedState-Nomad-Check-SkpSwiDat

1E-GuaranteedState-Nomad-Fix-SkpSwiDat

1E-GuaranteedState-Nomad-Check-StartService

1E-GuaranteedState-Nomad-Fix-StartService

1E-GuaranteedState-Nomad-Check-Variant

Trigger templates

TriggerTemplate-FileChange

TriggerTemplate-IntervalHours

TriggerTemplate-IntervalMinutes

TriggerTemplate-IntervalSeconds

TriggerTemplate-ServiceStatusChange

TriggerTemplate-WindowsRegistryChange

8.3.1.3 Windows Client Health Policy

Over time Windows devices can develop performance problems related to device or service availability. This policy verifies the available storage capacity on devices, notifies of application crashes, monitors WMI health and service function and also checks the behavior of core Windows services.

The Windows client health policy covers all of the following:

Manages Windows devices and service availability performance problems

Safeguards disk space integrity, ensuring sufficient storage capacity

Ensures optimum performance of the Configuration Manager client and that WMI is active and integrated

Notifies of application crashes and remediation assists. Investigates root cause for specific issues.

Note

This policy is intended for deployment to Windows devices only.

8.3.1.3.1 Important considerations

Before deploying the Windows Client Health Policy you need to be familiar with its contents and comfortable that you want to apply it to the devices in your network.

By default, automated fixes in the Policies provided by 1E are not enabled, this means you will have to specifically enable the ones you want to use before they can take effect.

A new or updated Policy should first be verified by deploying it to a Management Group containing a small number of devices, reviewing the Guaranteed State reports, and confirming the checks and enabled fixes are working as expected.

When you are comfortable with the results you can then deploy to larger Management Groups.

The policy contains the rule Check application crash count which by default specifies the Application Name as MyApplication.exe. You do not need to change this before deployment, but you can edit the rule to specify an the executable that you want to monitor, or clone the rule to monitor other executables. You will need to edit the rule and change the name in the Trigger and the Check tabs.

8.3.1.3.2 Windows Client Health Policy reference

For details on the policy, rules, triggers, preconditions, checks and fixes available in the Windows Client Health Policy please refer to Windows Client Health Integrated Product Pack.

Note

Instructions

1E-Explorer-WindowsClientHealth-ApplicationCrashes

1E-Explorer-WindowsClientHealth-ApplicationCrashesFiltered

1E-Explorer-WindowsClientHealth-GetLogFileContent

1E-Explorer-WindowsClientHealth-StartWMIService

Policies

Windows Client Health

Rules

Check application crash count (not assigned to any policy by default)

Check free disk space

Check WMI repository health

Ensure WMI service is running (not enabled and not assigned to any policy by default)

Fragments

1E-GuaranteedState-General-PreCondition-InstalledSoftware

1E-GuaranteedState-General-PreCondition-MinWindowsVersion

1E-GuaranteedState-General-PreCondition-OperatingSystem

1E-GuaranteedState-General-PreCondition-OSAndSoftware

1E-GuaranteedState-General-PreCondition-WindowsDevice

1E-GuaranteedState-General-Check-ServiceState

1E-GuaranteedState-WindowsClientHealth-Check-ApplicationCrashes

1E-GuaranteedState-WindowsClientHealth-Check-SystemDriveFreeSpace

1E-GuaranteedState-WindowsClientHealth-Check-WmiBasicHealth

1E-GuaranteedState-WindowsClientHealth-Fix-StartWMIService

Trigger templates

TriggerTemplate-IntervalHours

TriggerTemplate-IntervalMinutes

TriggerTemplate-IntervalSeconds

TriggerTemplate-ProcessCrash

TriggerTemplate-ServiceStatusChange

TriggerTemplate-WindowsEventLog

TriggerTemplate-WindowsRegistryChange

8.3.1.4 Tachyon Core Utilities

8.3.1.4.1 Overview

This Integrated Product Pack does not include any instructions, policies or rules. However, it does contain a number of triggers, preconditions, checks and fixes that can be used to help build your own policies, as described in Defining your own policy.

8.3.1.4.2 Core Utilities reference

For details on the triggers, preconditions, checks and fixes available in the Core Utilities please refer to Tachyon Core Integrated Product Pack.

8.3.1.4.2.1 Instructions

No Instructions.

8.3.1.4.2.2 Policies

No Policies.

8.3.1.4.2.3 Rules

No Rules.

8.3.1.4.2.4 Fragments

1E-GuaranteedState-General-Check-RegistryValue

1E-GuaranteedState-General-Fix-RegistryValue

1E-GuaranteedState-General-Check-ServiceState

1E-GuaranteedState-General-Fix-ServiceState

1E-GuaranteedState-General-PreCondition-InstalledSoftware

1E-GuaranteedState-General-PreCondition-MinWindowsVersion

1E-GuaranteedState-General-PreCondition-MinWindowsVersionAndVariant

1E-GuaranteedState-General-PreCondition-OperatingSystem

1E-GuaranteedState-General-PreCondition-OSAndSoftware

1E-GuaranteedState-General-PreCondition-OsTypeAndArchitecture

1E-GuaranteedState-General-PreCondition-Service

1E-GuaranteedState-General-PreCondition-WindowsDevice

8.3.1.4.2.5 Trigger templates

TriggerTemplate-IntervalHours

TriggerTemplate-IntervalMinutes

TriggerTemplate-IntervalSeconds

TriggerTemplate-ProcessCrash

TriggerTemplate-ProcessLaunch

TriggerTemplate-ServiceStatusChange

TriggerTemplate-WindowsEventLog

TriggerTemplate-WindowsRegistryChange

8.3.2 Deploying a Policy

How to deploy a Policy in Guaranteed State.

8.3.2.1 Overview

If you have uploaded the Product Packs provided with the Tachyon release using the PPDT, you will already have several Guaranteed State policies and Instructions available in the application. Please refer to Tachyon Product Pack deployment tool for details.

> **Important**
>
> When any policy artifacts are altered, the Policy infrastructure is marked as "dirty," prompting a **Deploy Policy** notification. This happens even if the modified artifacts are not utilized by any active Policy. If you are certain that none of the altered artifacts are in use, deployment is not necessary. However, if you are uncertain, you can proceed with the deployment without concern, as it will not impact anything if there are no changes. Refer to Instructions and product packs.

The policies included with the release are:

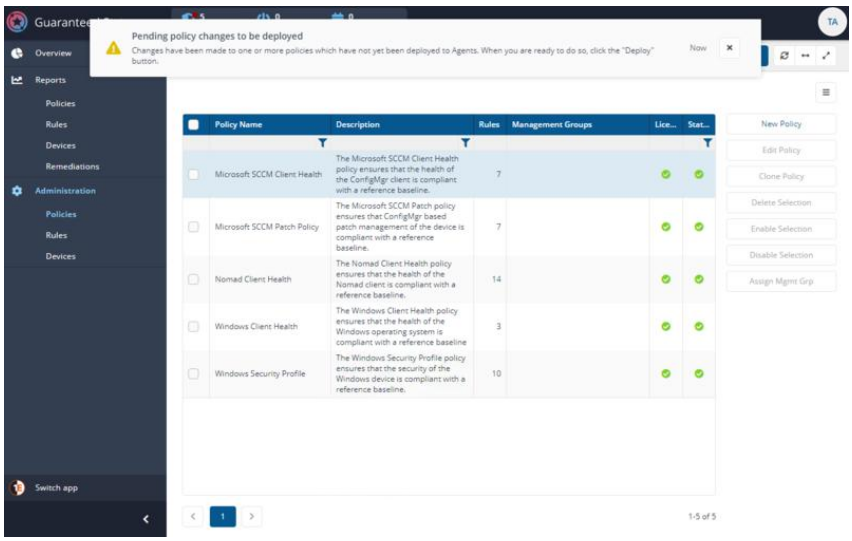
Policy name	Description
Microsoft SCCM Client Health	The Microsoft SCCM Client Health policy ensures that the health of the ConfigMgr client is compliant with a reference baseline.
Microsoft SCCM Patch Policy	The Microsoft SCCM Patch policy ensures that ConfigMgr based patch management of the device is compliant with a reference baseline.
Nomad Client Health	The Nomad Client Health policy ensures that the health of the Nomad client is compliant with a reference baseline.

Policy name	Description
Windows Client Health	The Windows Client Health policy ensures that the health of the Windows operating system is compliant with a reference baseline.
Windows Security Profile	The Windows Security Profile policy ensures that the security of the Windows device is compliant with a reference baseline.

When you first open the **Administration→Policies** page, you'll see a popup message advising that you have policy changes that can be deployed to Agents. This refers to the new policies in the above table that can be uploaded using the PPDT.

The next steps to using these new policies is to add them to one or more Management Groups and to deploy them to clients.

> **Note**
>
> For a new or updated policy to become effective, it must be deployed. Policies are deployed by clicking the **Deploy** button from the **Guaranteed State→Administration→Policies** page. Deployment affects all visible policies that are enabled, please refer to the section Deploying policies for details.



8.3.2.2 Assigning a policy to a management group

Before deploying a policy we must first define the devices to which the policy will be sent. We do this by assigning a policy to a management group.

To do this, go to **Guaranteed State→Administration→Policies** select the policy and click the **Assign Mgmt Grp** button.

By default, there will always be a management group for **All Devices**. We select this and then click **Save**.

> **Warning**

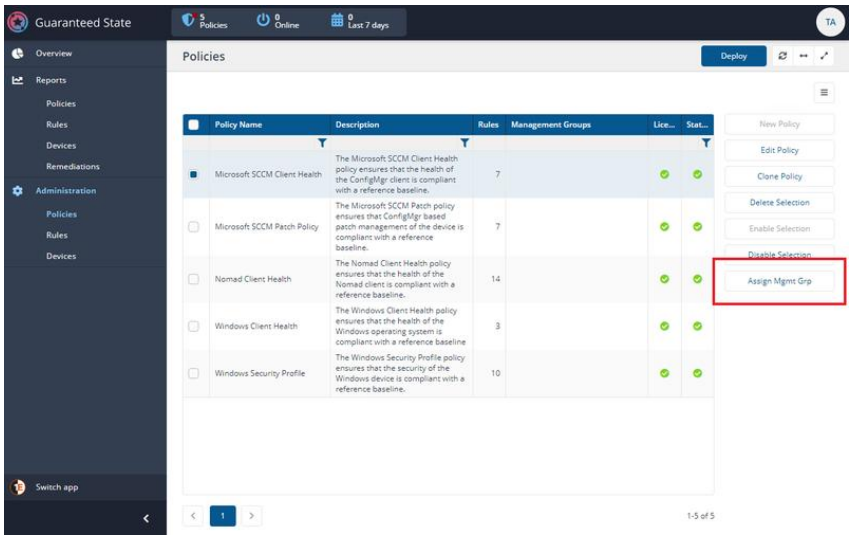
If you select **All Devices**, Guaranteed State will apply the policy to all devices including ones that are not currently online, which may include other OS or device types, for example servers.

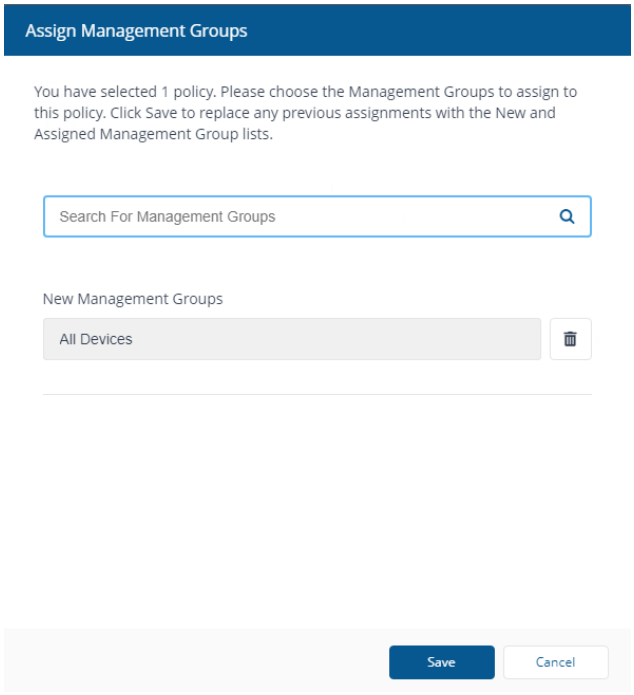
For this reason we recommend that you define a specific Management Group for your policy to limit its scope to just the devices included in the Management Group.

The Integrated Product Packs provided by 1E contain policies for Windows devices, therefore when you deploy these please ensure your Management Groups include only Windows devices.

Note

In Guaranteed State you can create your own custom polices and associated rules, refer to Defining your own policy for details.

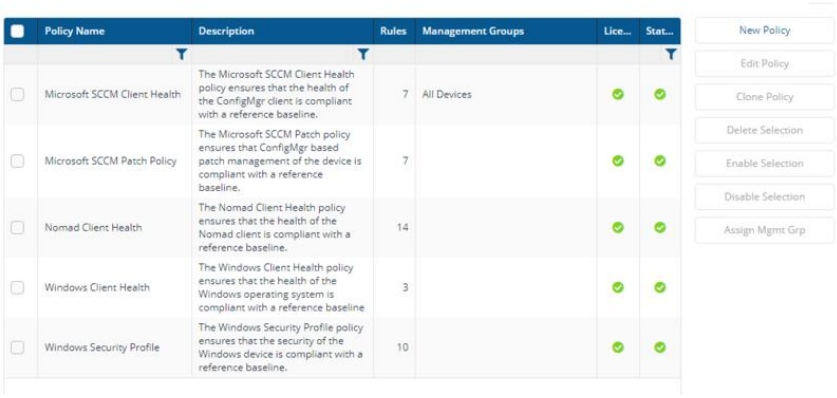




We should now see the assigned policy.

Note

The policy is now shown with its assigned management groups, in this case, the **All Devices** group.



8.3.2.3 Deploying policies

For a new or updated policy to become effective, it must be deployed. Policies are deployed by clicking the **Deploy** button from the **Guaranteed State→Administration→Policies** page. Deployment affects all visible policies that are enabled.

You can enable or disable a policy from this screen by selecting it and then clicking the **Disable Selection** or **Enable Selection** button (which will change the **Status** as appropriate based on the current state of the policy).

Policy state	Description
Deleted policies and deployment	If a policy is deleted, then clicking **Deploy** will also cause any Tachyon client that receives the deployment to remove the policy and to cease to enforce it.
Disabled policies and deployment	If a policy is disabled, then clicking **Deploy** will also cause any Tachyon client that receives the deployment to remove the policy and to cease to enforce it. If the policy is subsequently re-enabled, then the next time **Deploy** is clicked, it will be sent out again and become effective.

Note

Currently, you are prompted to deploy a policy as soon as you save it, after creating or editing. However, deploying a new policy where any of the following is true will not result in any action being taken by the 1E Client on devices because:

No rules have been assigned to the policy

All rules assigned to a policy are disabled

The policy has not been assigned to any Management Group.

However, once a policy has been deployed, re-deploying the policy will always affect the devices to which the policy was previously deployed. In the case where a re-deployed policy meets any of the above criteria, it will cease to be effective on the devices

If the change removes a policy from any management groups, devices affected by this change will receive a policy update. For example, suppose you had a policy P1 assigned to management group MG1 and you then re-target P1 to management group MG2 instead and re-deploy it. All the devices which ever received policy P1 previously will have that policy removed if they now fall outside management group MG2.

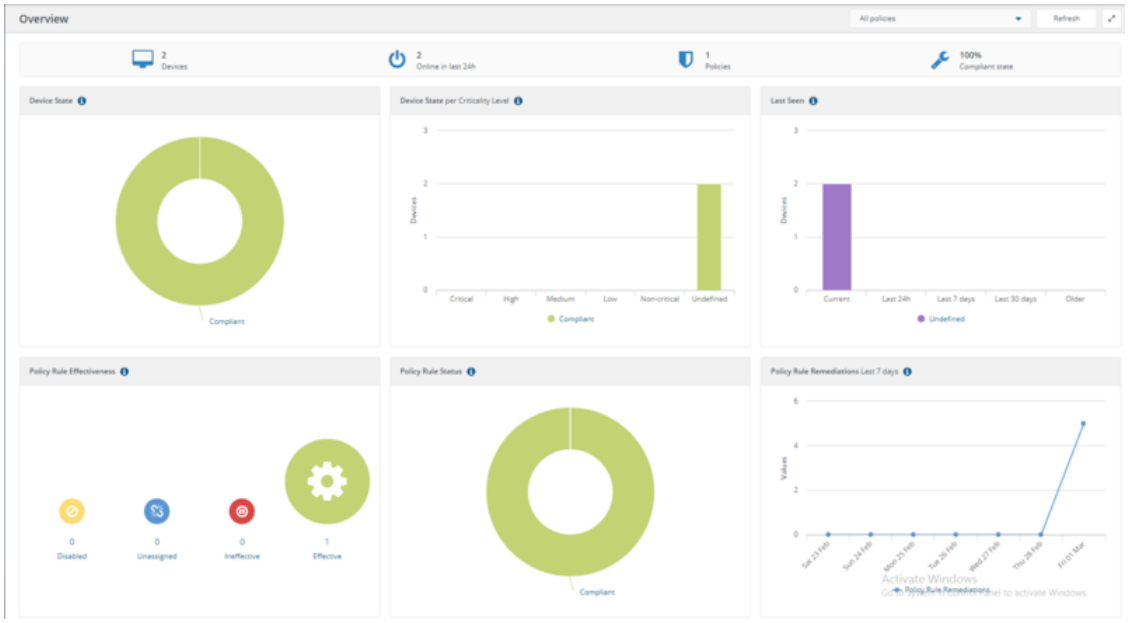
The distribution of policies to devices is staggered. The stagger period associated with this activity is designed to avoid excessive network traffic. It is not related to the DefaultStaggerRangeSeconds parameter which is defined during 1E Client installation, refer to Tachyon client settings for details.

8.3.2.4 Verifying policies

You can verify policy enforcement on the **Guaranteed State→Overview** page and confirm policy download and applications on the devices.

8.3.2.4.1 Verifying policy enforcement

The Guaranteed State overview shows us all compliant devices.

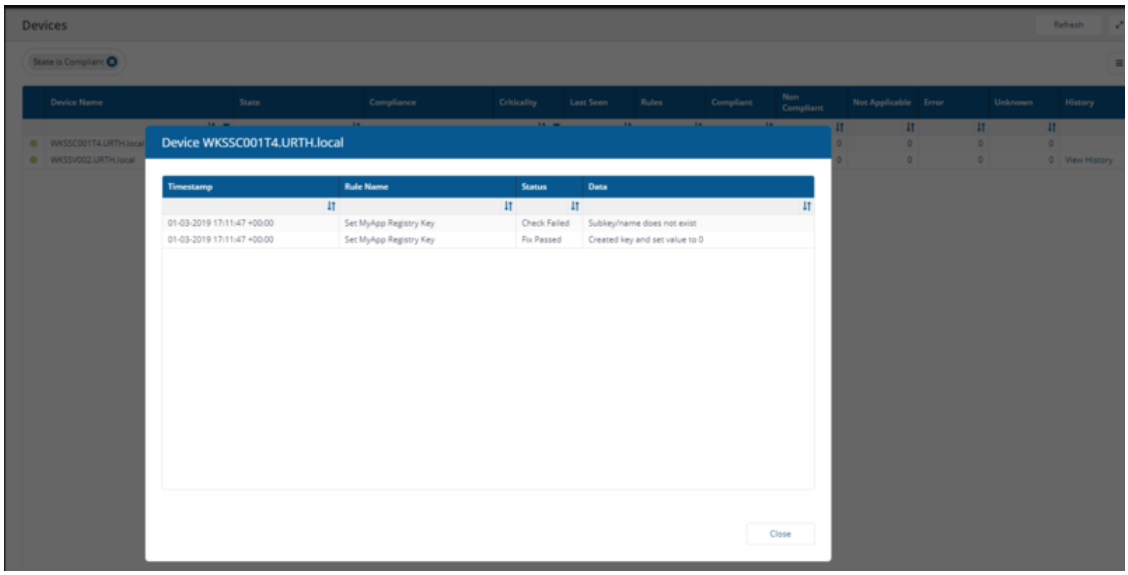


You can drill down on each chart. For example, clicking on the **Device State** chart allows us to see the specific devices that are associated with the chart. From there we can examine the history of each device, for example.

Note

History entries are only created when the status changes state from pass to fail or vice-versa. Even though you may have a rule evaluated periodically by the 1E Client, a history entry is not created for each evaluation cycle. The 1E Client only communicates a state change when the rule status changes.

This means that if the cause of a failure changes, you may not receive a history entry with the revised cause, because no updates are received until the compliance state changes. This limitation may be revised in a future release.



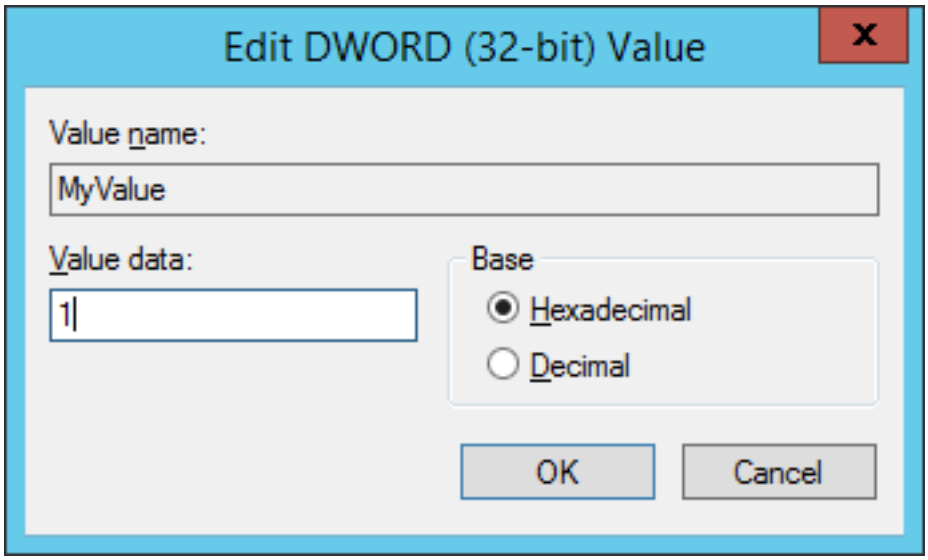
8.3.2.4.2 Verifying policy on 1E Client

We can also confirm that the policy was downloaded and applied on 1E Client by examining the 1E Client log on the device. Here we see that the policy was downloaded and successfully applied.

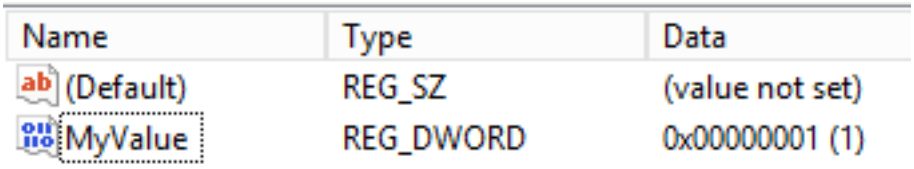
```
2019-03-01 17:11:47.268 [ 6892] INFO  - Downloaded and applied new policy with 1 rule(s) (829 bytes)
2019-03-01 17:11:47.271 [ 6892] INFO  - [Policy Rule 'Set MyApp Registry Key' (ID 4) (check)] Successfully processed instruction
2019-03-01 17:11:47.271 [ 6892] INFO  -  -> Policy Rule 'Set MyApp Registry Key' (ID 4) - check failed; running fix rule
2019-03-01 17:11:47.274 [ 6892] INFO  - [Policy Rule 'Set MyApp Registry Key' (ID 4) (fix)] Successfully processed instruction
2019-03-01 17:11:47.280 [ 6892] INFO  -  -> New Policy Rule 'Set MyApp Registry Key' (ID 4) evaluated; notifying status of 'fix passed'
```

If we now start the registry editor on the device, we can see that the **Value name** and **Value data** exist.

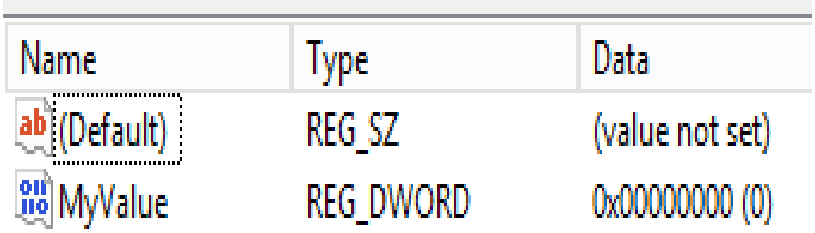
If we attempt to change the **Value data** to **1**.



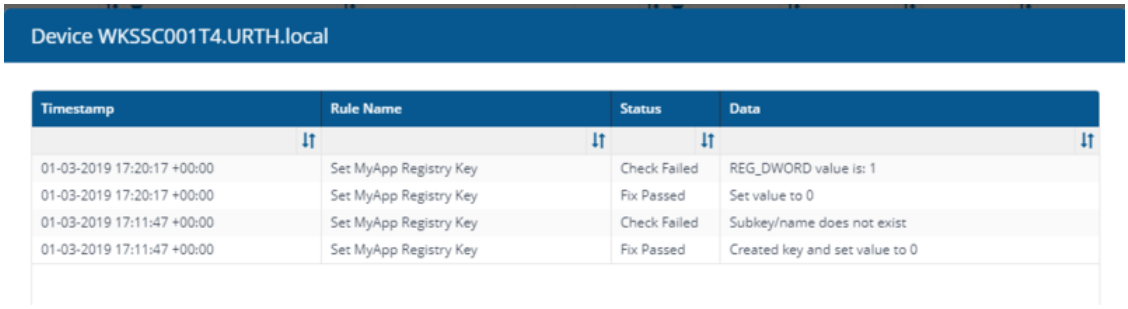
We see that, temporarily, it is out of compliance with the check rule.



However, after 30 seconds, it is automatically reset to be compliant.



If we view the device history from the Guaranteed State Overview screen, we see that the momentary compliance failure has been logged.



8.3.2.5 Device Status

The device status view in Guaranteed State shows the status of policies and rules for each device.

A device is shown as either **Compliant** or **Noncompliant**. The associated columns show more information on the status of rules on the device:

Column	Description
Rules	The number of rules which are active for the device. If there are several active policies applicable to the device, the rules count will be the sum of all the distinct rules associated with those policies. (i.e, if the same rule is included in two active policies against the device, the count of distinct rules is 1).
Compliant	The number of rules which returned a compliance status of success (specifically each rule which returned a boolean value of **True** when the rules were last evaluated).
Non-compliant	The number of rules which returned a compliance status of failure (specifically each rule which returned a boolean value of **False** when the rules were last evaluated).
Not applicable	The number of rules for which the precondition for the rule meant that for this device, the rule was not regarded as applicable and hence was not evaluated.
Error	The number of rules for which an error was raised during the execution of the rule. This means that the SCALE code associated with the rule failed with an error that caused the code to be terminated, or that the code deliberately raised an error using the SCALE Error function.
Unknown	The number of rules for which no status has yet been returned from the device.

8.3.3 Defining your own policy

How to define a policy in Guaranteed State.

For details of policy objects you can use to create your own policies, please refer to Tachyon Product Packs reference.

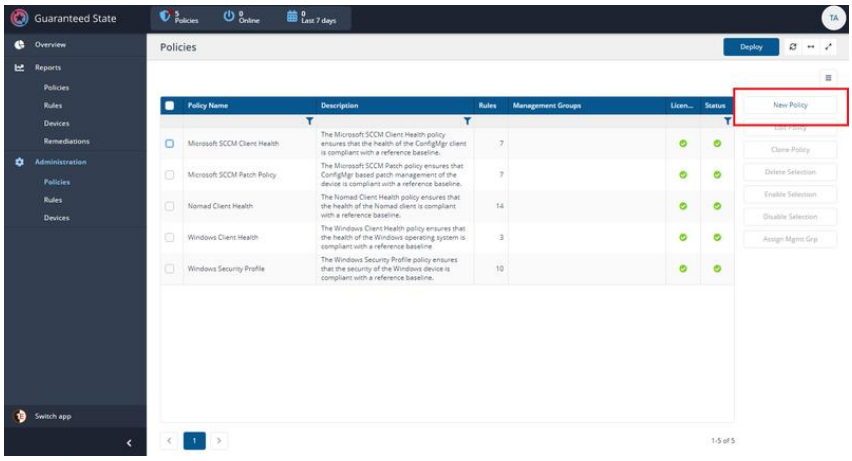
8.3.3.1 Defining a policy

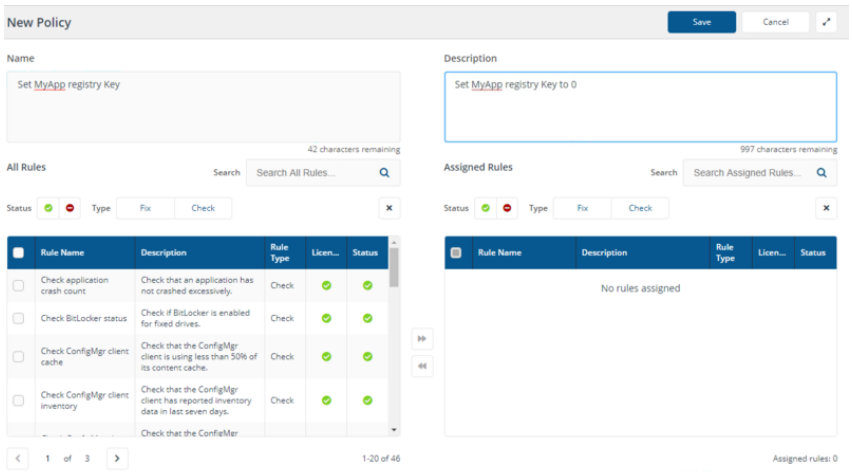
You define a policy from **Guaranteed State->Administration->Policies**.

Click **New Policy**, enter a name and description for the policy and click **Save**.

Note

The Managing rules section explains how to create and add rules for the new Policy.



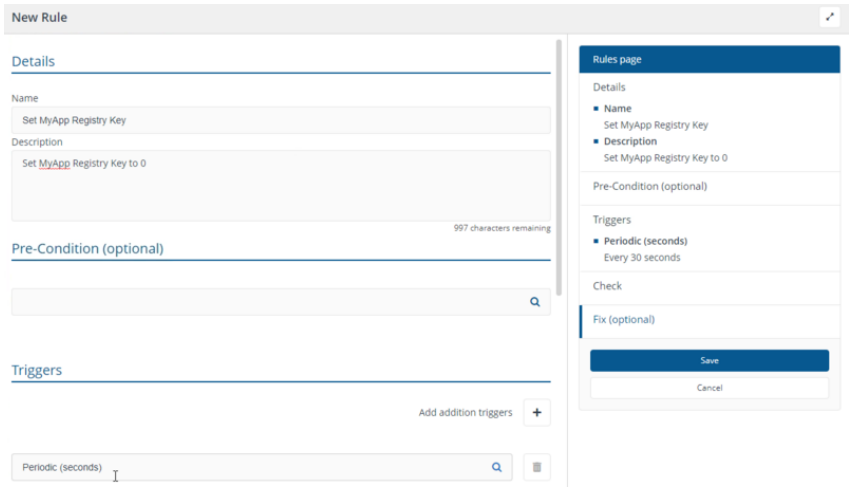


8.3.3.2 Managing rules

Policies need rules in order to be of any use. The following headings show how to define rules, caveats for editing rules and how to associate rules with policies.

8.3.3.2.1 Defining a rule

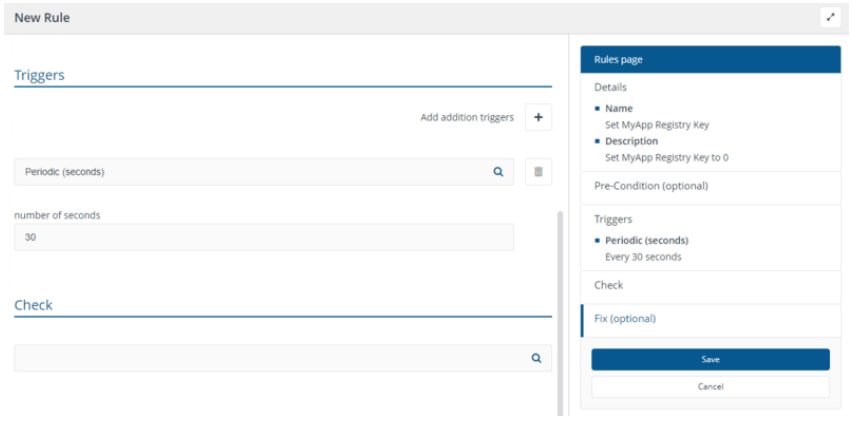
You define a rule from **Guaranteed State->Administration->Rules**. Click **New Rule** then enter a name and description.



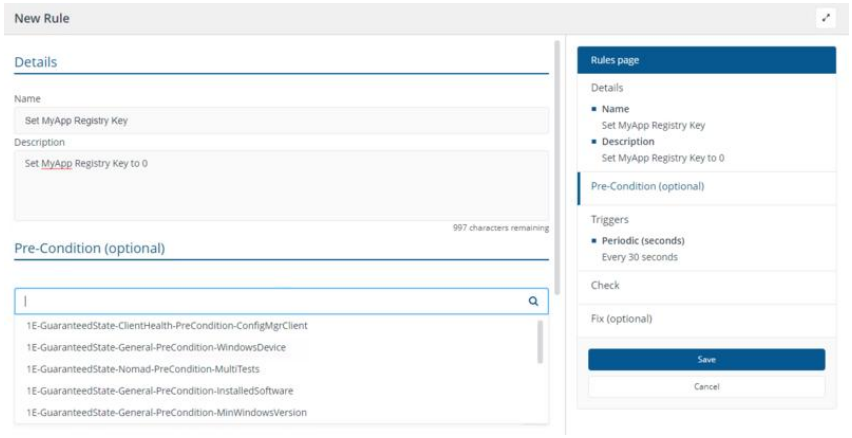
In the **Triggers** section we're going to define that the rule should be evaluated periodically, every 30 seconds. In the search window we choose **Periodic (seconds)** and set the **number of Seconds** to **30**.

You can add multiple **Triggers** using the add triggers plus sign, in this example we'll just use one.

> **Note**
>
> Do not specify a period less than 30 seconds. The rule may be accepted by the management interface but the 1E Client will not apply it.

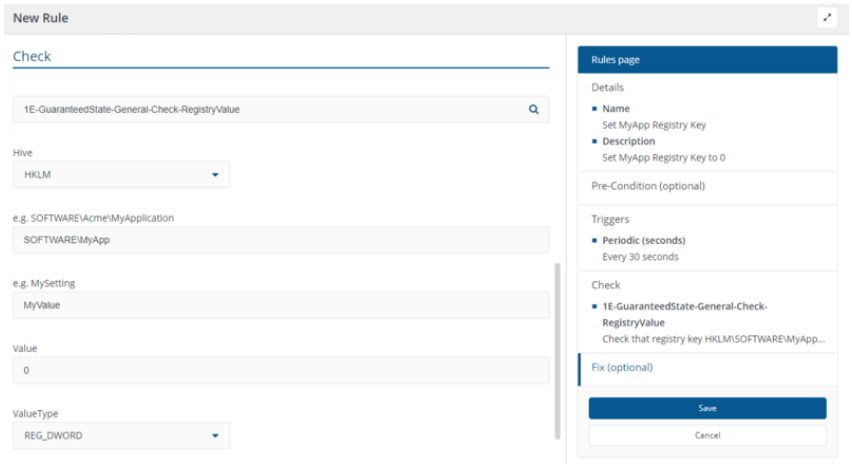


In the **Precondition** section, we will not define a precondition rule, but you can review the available choices, if you do want to set one.



In the **Check** section, we'll define a check rule that requires that there is a value **MyValue** in the registry hive HKLM and subkey **SOFTWARE\MyApp**. Its value should be of type **REG_DWORD** and it should be **0**.

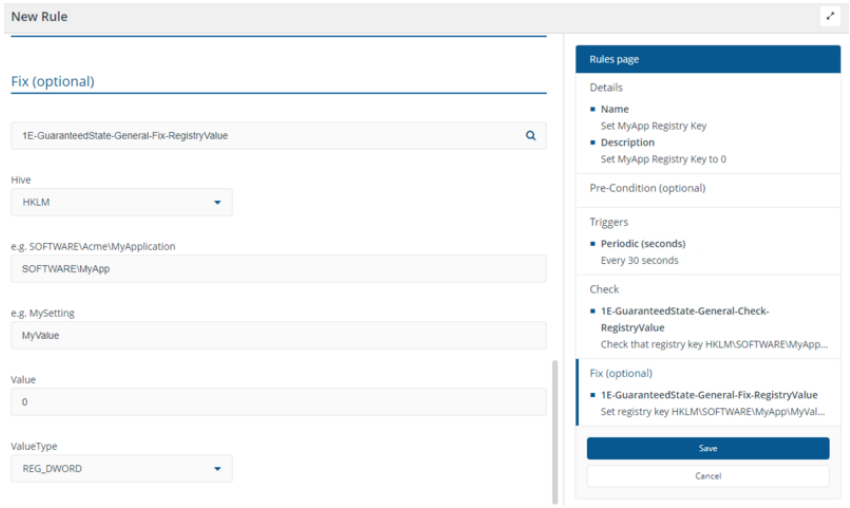
If any part of the **Subkey** is missing, or the **Name** or **Value** fail to match this check rule, then the fix rule will be applied.



In the **Fix** section, the fix rule will be identical to the check rule. This means that if the registry is not consistent with the check rule, it will be made consistent.

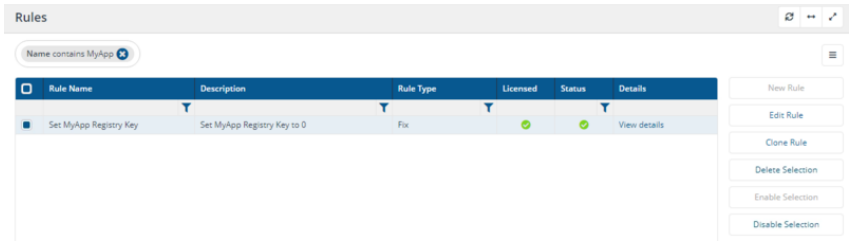
If any part of the **Subkey** does not exist, or the **Value** or **Name** is missing or has a different value or type, then all of these discrepancies will automatically be corrected and the registry value made to be consistent with the check rule.

Then click **Save**.



8.3.3.2.2 Editing existing rules

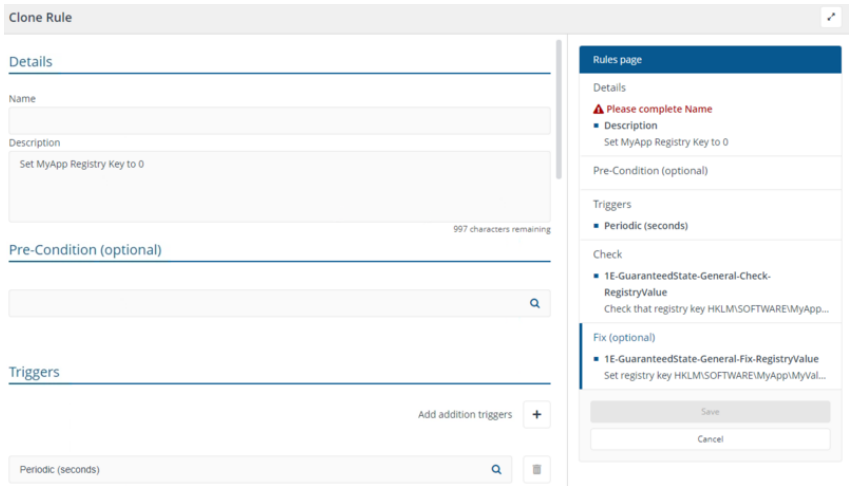
You can edit a rule by selecting it with the checkbox on the left and then selecting**Edit Rule**.



8.3.3.2.3 Cloning a rule

You can clone (copy) a rule by selecting it with the checkbox on the left and then selecting **Clone Rule**. When you do this, a copy of the rule is made.

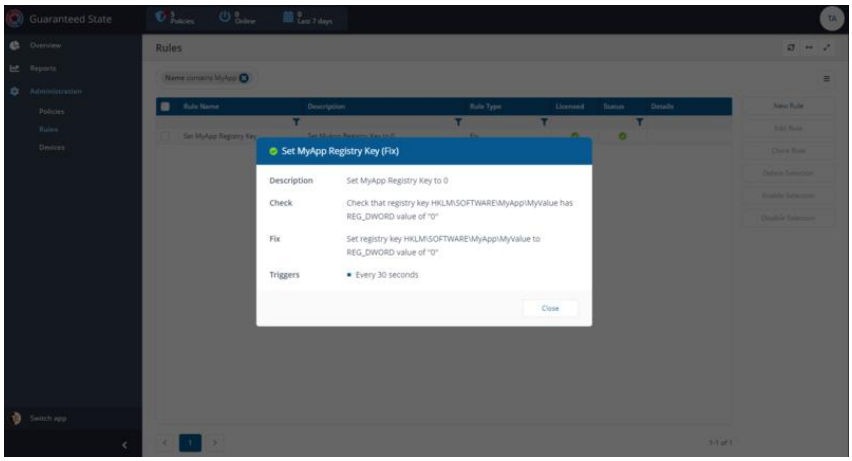
You will be prompted to enter a new name for the cloned rule. After this you can modify any property of the cloned rule and save it.



8.3.3.2.4 Viewing Rule Details

You can view the rule details for a rule by clicking the **View Details** link displayed on the rules page under the **Details** column, showing:

Heading	Description
Description	Rule description entered when the rule was created.
Check	The verification that a device has a particular state.
Fix	The defined desired state for the device and the enforcement that state.
Triggers	The definition of the conditions causing a rule to be evaluated.



8.3.3.2.5 Enabling and disabling rules

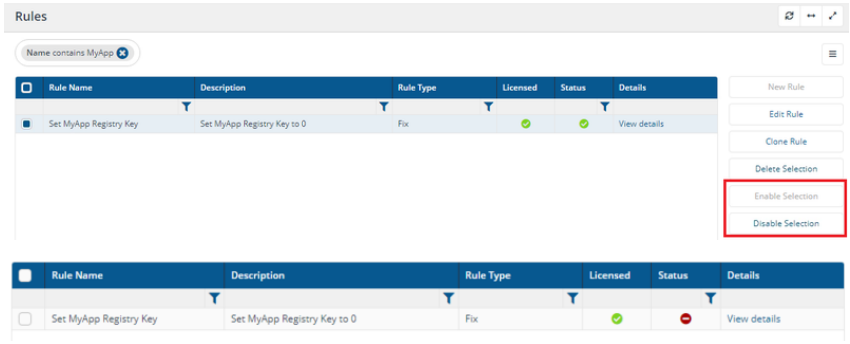
You can enable and disable rules by selecting the rule with the checkbox on the left and then selecting **Disable Selection**, if the rule is enabled, or **Enable Selection**, if the rule is disabled.

Disabled rules are shown with a disabled icon against them .

A disabled rule ceases to have effect within any policy that refers to that rule, when that policy is redeployed. In effect, a disabled rule acts as if the rule is not part of the policy.

You must redeploy any policies which contain a disabled rule for the change to become effective on any devices targeted by the policies.

If you enable a previously disabled rule then the rule becomes active again. You must redeploy any policies containing the rule for the change to become effective on any devices targeted by the policies.

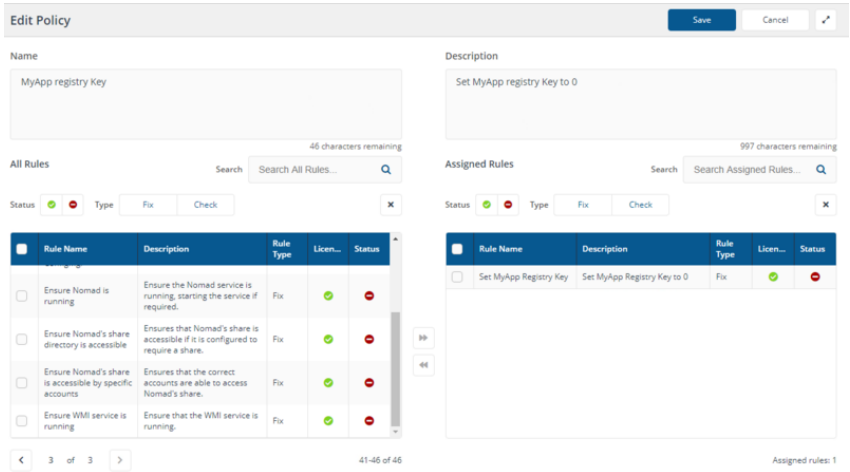


8.3.3.2.6 Associating a rule with a policy

You associate a rule with a policy from Guaranteed State →**Administration**→**Policies** by selecting the policy using with the checkbox on the left, then selecting **Edit Policy**.

The available rules are on the left of the page. You select the rule(s) you want to associate with the policy using the checkboxes and then click the button.

After selecting all the rules you want to associate, click **Save**.

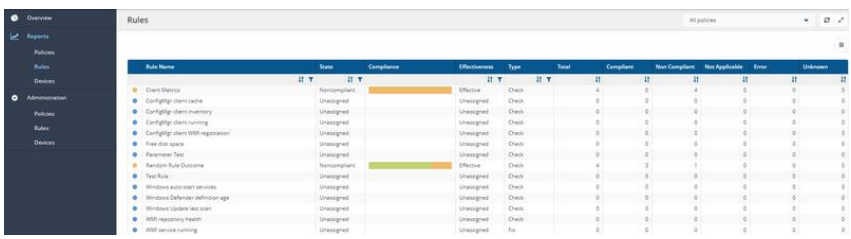


8.3.4 Using Explorer to investigate devices in Guaranteed State

How to investigate devices displayed in the Guaranteed State pages using Explorer.

8.3.4.1 Using Guaranteed State to define coverage for a question in Explorer

Selecting the **Rules** view from the **Reports** page in Guaranteed State shows the compliance status for each rule.

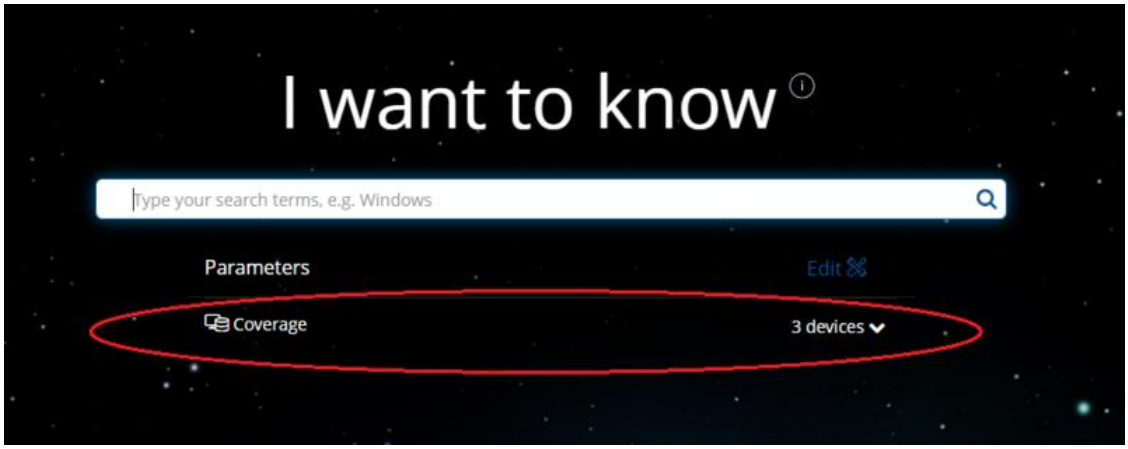


You can filter by policy, by selecting the applicable policy from the dropdown box at the top of the screen.

If you now click on the rule name, you will be taken to the devices against which the rule has been evaluated. You can then select one or more devices by clicking the selection checkbox to the left of each device row.

Having done this you can now click the **Explore** button. This switches to the **Explorer** application **Home** page, but note that the device coverage for any question or action has been set automatically, as shown opposite.

This makes it easy to follow up compliance issues by addressing questions only to devices with a specific compliance state.



8.3.5 Guaranteed State Overview page

The overview page shows a dashboard with six charts, reflecting the currently selected policy or all policies.

The dashboard is refreshed (recalculated) when:

Opened or the page is refreshed in the browser

A different policy is selected

Autorefreshed when the **Autorefresh** switch is enabled

The refresh button is clicked.

8.3.5.1 Dashboard charts overview

The Guaranteed State dashboard presents a number of panels:

Overview header pane

Device State

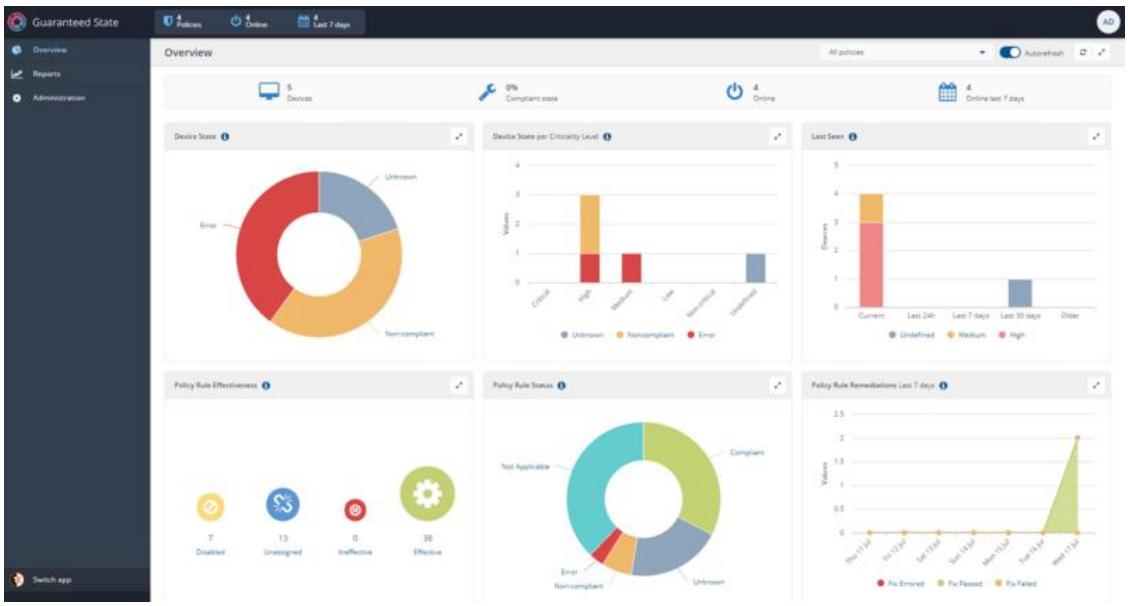
[Device State per Criticality Level]

[Last Seen]

[Rule Effectiveness]

[Rule Status]

[Policy Rule Remediations Last 7 days]



8.3.5.1.1 Overview header pane

The Overview header pane has three rows:

Top row:

Policies - shows the number of policies currently enabled, and is a shortcut to the Policies administration pane

Online - shows the number of devices currently online, and is a shortcut to the Devices administration pane

Last 7 days - shows the number of devices seen in the last 7 days, and is a shortcut to the Devices administration pane.

Middle row:

Policies drop-down list - filter on all policies or an individual policy, for example a selection of the Microsoft SCCM Client Health policy displays a filtered overview

Autorefresh toggle switch

A refresh button

A resize button to display the central panes with and without the Guaranteed State border panes.

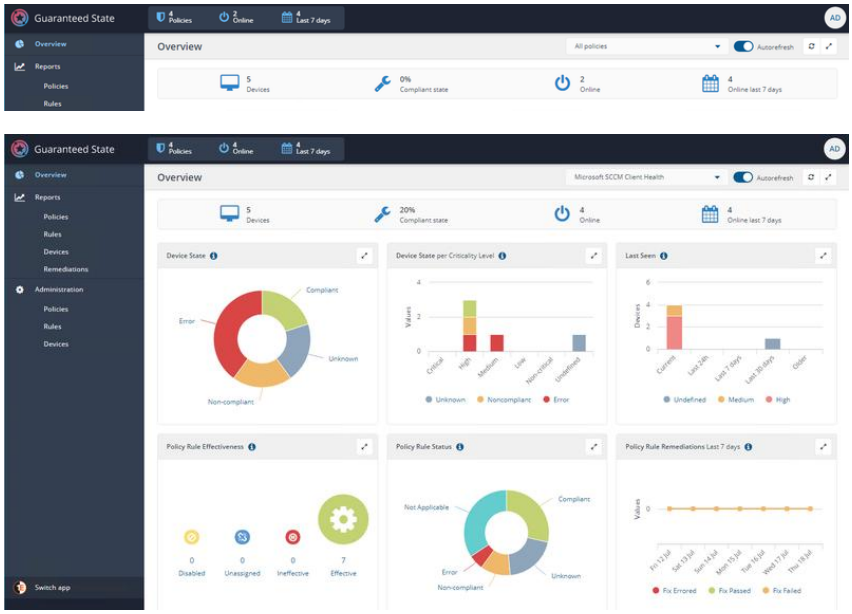
Bottom row:

Devices - shows the number of devices targeted by the selected policy, and is a shortcut to the Devices report pane

Compliance state - percentage of devices compliant with the selected policy filter - shortcut to the Devices report filtered on State is Compliant

Online - number of devices online - Shortcut to the Devices report filtered on **LastSeen is current**

Online the last 7 days - shortcut to Devices Report filtered on **LastSeen** is current OR **LastSeen is 24h** or **LastSeen is 7 days**.



8.3.5.1.2 Device State

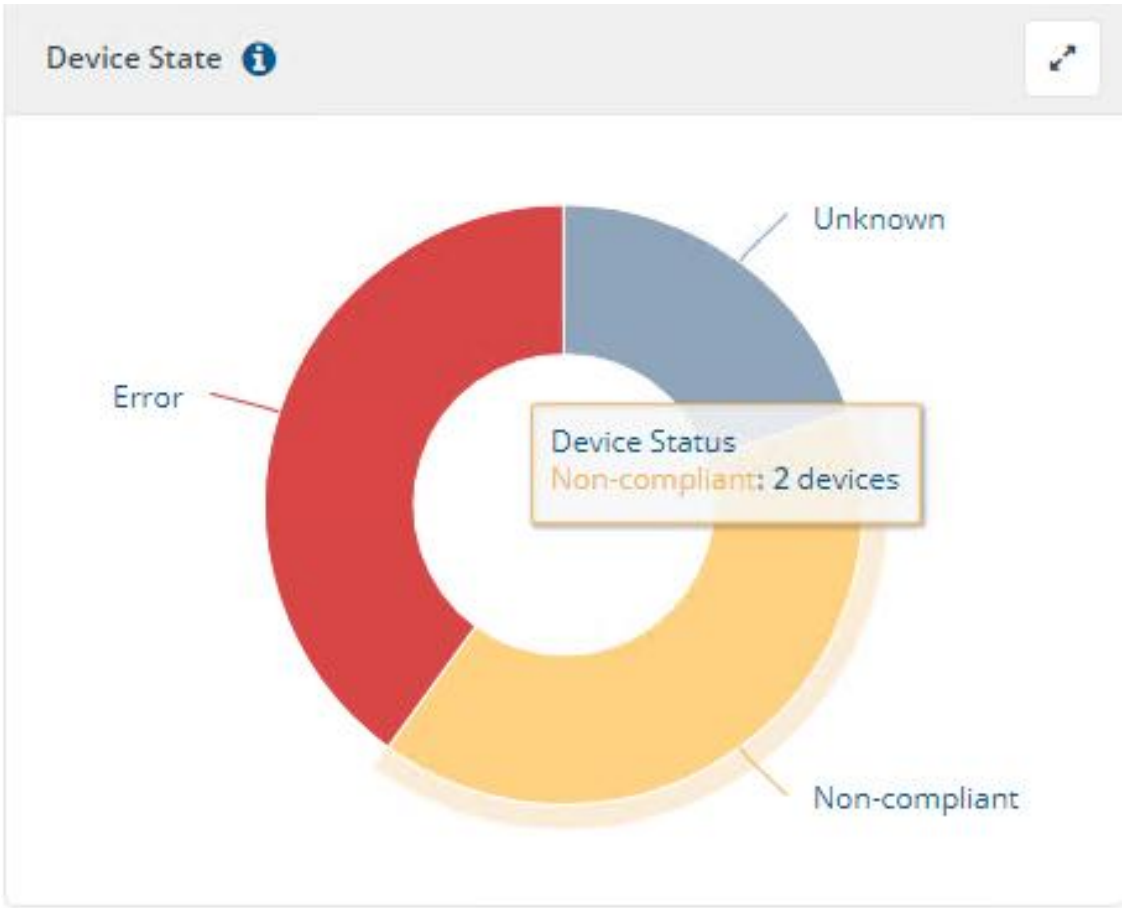
The state of devices where Guaranteed State policies have been deployed is represented in this form.

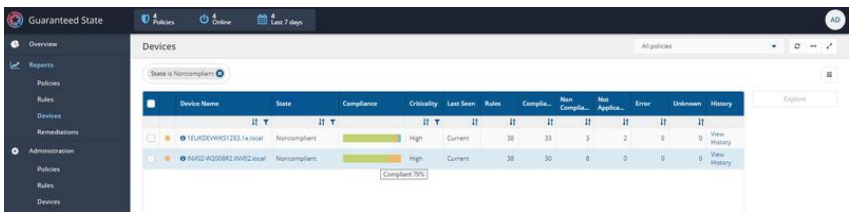
The user has the ability to drill down into the percentage of failures for each group of device states. For example, where the meaning of device states and their precedence is as follows:

State	Description
Unknown	The device has yet to receive, evaluate or report back on its compliance state for at least one rule.
Error	The device has failed to evaluate at least one deployed rule. For example a device may report 97% of deployed rules as **Not Applicable**, but since 3% of the deployed rules reported as Error this means the whole Device State is marked as **Error**.
Not Applicable	At least one rule deployed to the device is not applicable.

State	Description
	For example, this would occur if a Windows specific rule was deployed to a non-Windows device.
Non-compliant	At least one rule deployed to the device failed compliance checks. For example in the example above 86% of policy rules are compliant for the high-lighted device, but since 8% of the rules are Non-compliant the state of the whole device is marked as Non-compliant.
Compliant	The device passed compliance checks for every deployed policy rule.

The drill down navigates to the **Devices** report filtered on the selected **Device State** such as **Noncompliant**.

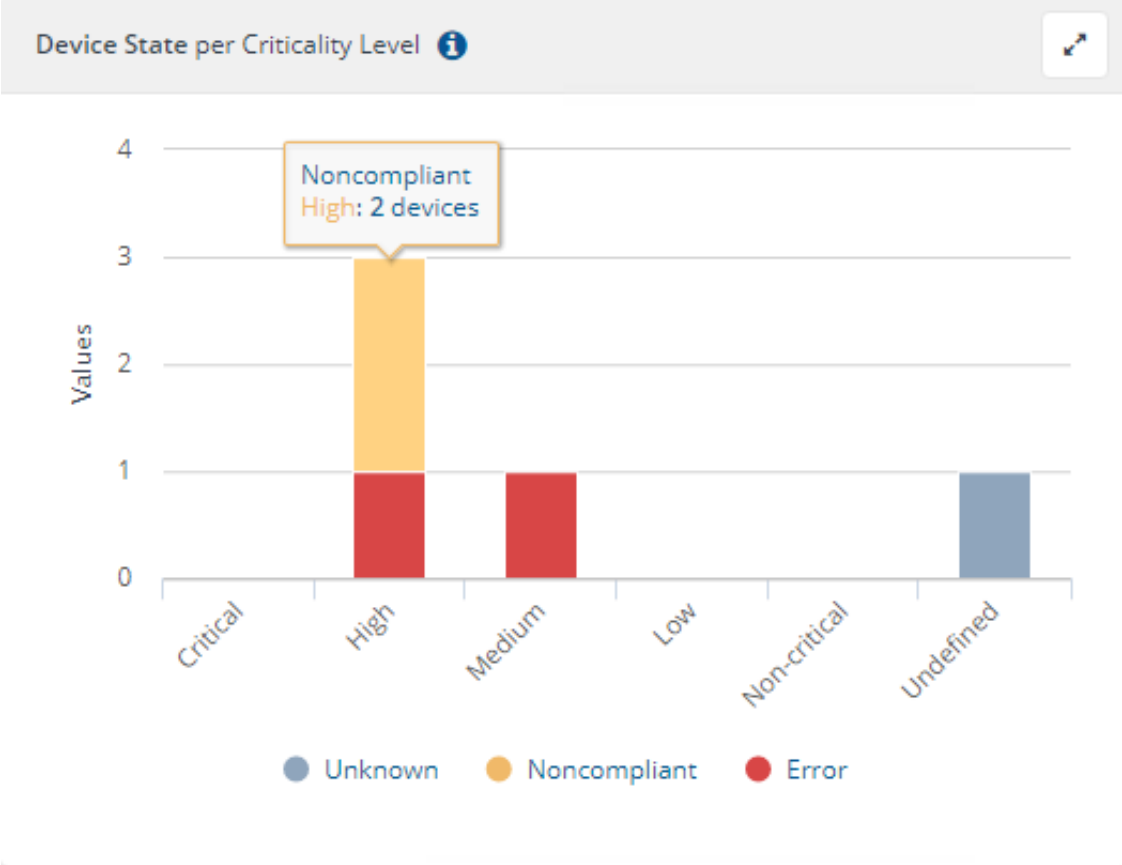


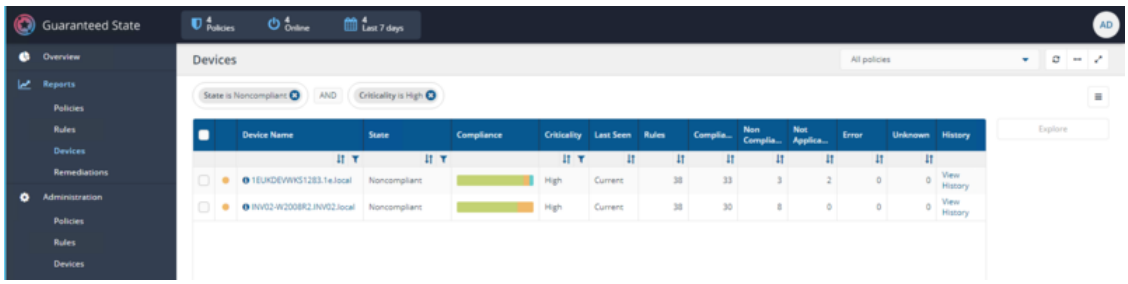


8.3.5.1.3 Device State per Criticality Level

This pane presents a breakdown of the number of devices reporting against each compliance state against the device criticality groups.

The drill down navigates to the **Devices** report filtered by **Device State** and **Criticality Level**, such as **State is Noncompliant** AND **Criticality is High**.

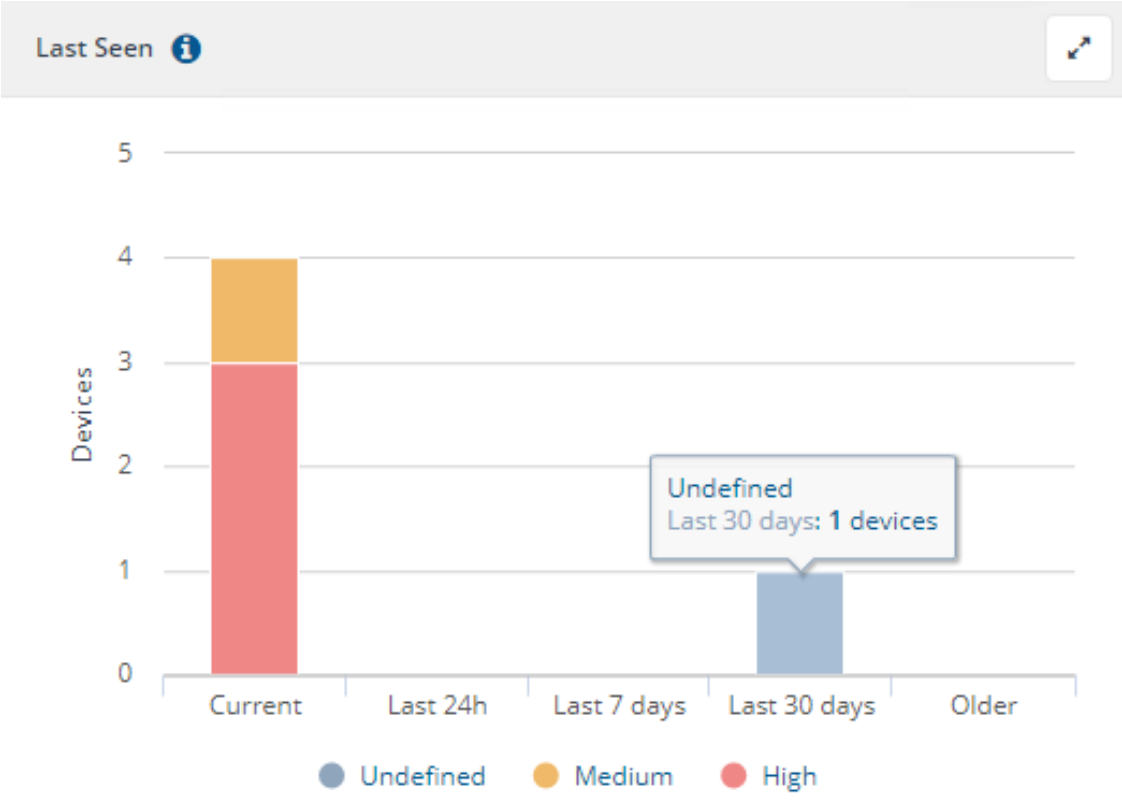


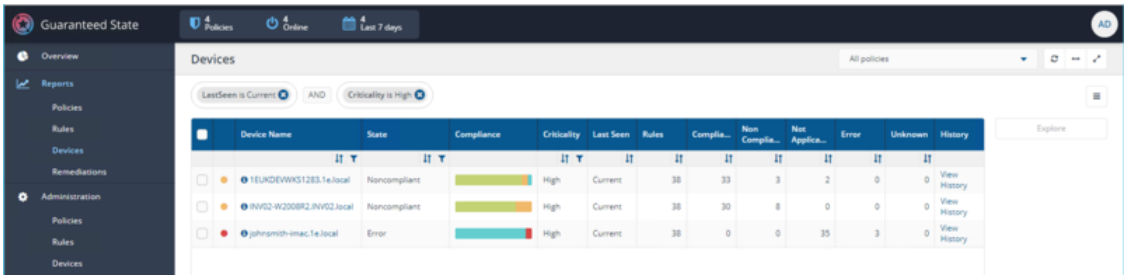


8.3.5.1.4 Last Seen

This panel shows a summary of when devices last made contact with the Tachyon server, grouped by the criticality level assigned to each device.

The drill down navigates to the **Devices** report filtered by **LastSeen** and criticality, such as **LastSeen is Current** AND **Criticality is High**.





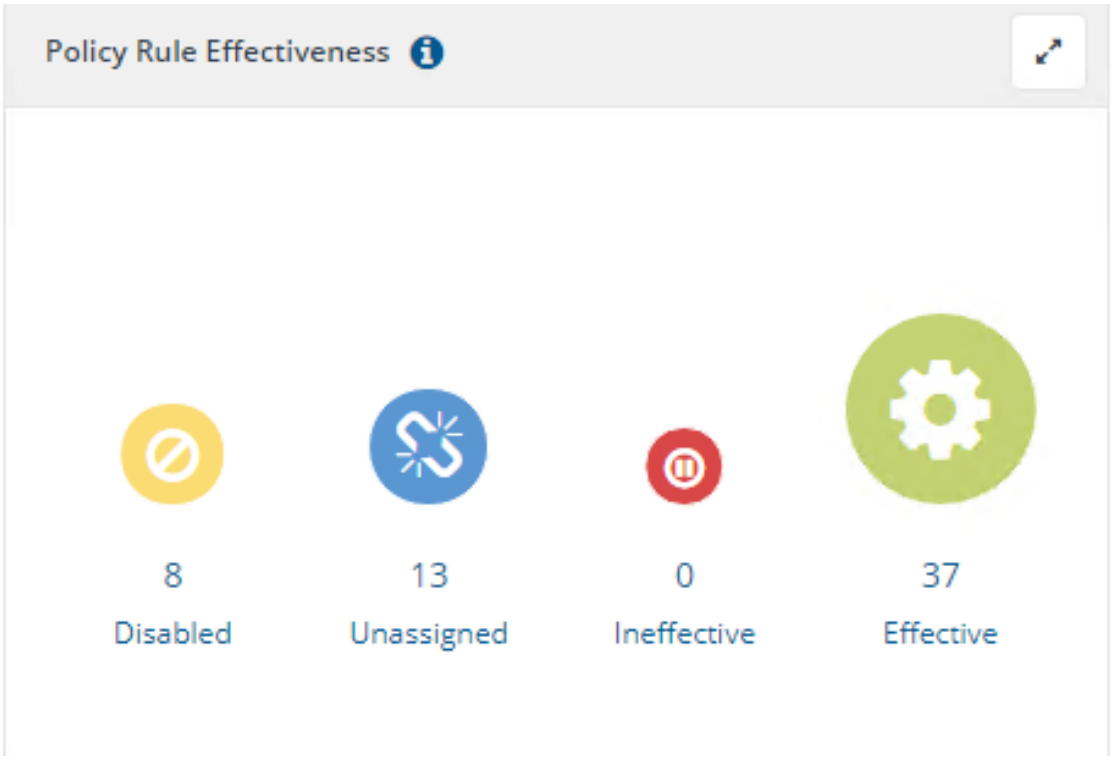
8.3.5.1.5 Policy Rule Effectiveness

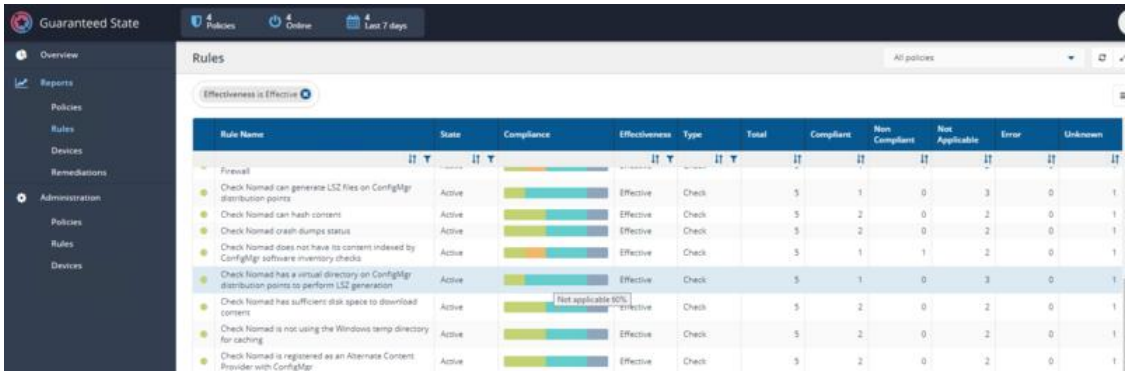
Policy rule effectiveness is the usefulness of policy rules and is represented as follows:

State	Description
Disabled	The rule has not yet been enabled from the Guaranteed State Rule Administration page, so it is not currently active.
Unassigned	The rule is enabled, but has not been deployed to any devices. To deploy a rule : The rule must be included in at least one policy.

State	Description
	That policy must be assigned to a Management Group containing at least one device. The policy must be deployed.
Ineffective	The rule has been deployed, but no devices have changed their compliance position for this rule in the last thirty days. (The thirty day limit is received from the **EffectiveThresholdDays** row within the SQL **TachyonMaster GlobalSetting** table).
Effective	The rule has been deployed and at least one device has changed its compliance position for this rule in the last thirty days. (The thirty day limit is received from the **EffectiveThresholdDays** row within the SQL **TachyonMaster GlobalSetting** table). Effective plus Ineffective gives the total number of Policy Rules deployed.

The drill down navigates to the **Rules** report filtered by **Effectiveness**, such as **Effectiveness is Effective**.





8.3.5.1.6 Policy Rule Status

A user has the ability to drill down into a segment, for example, to examine exactly which policy rules reported failures across all the devices for which it was deployed.

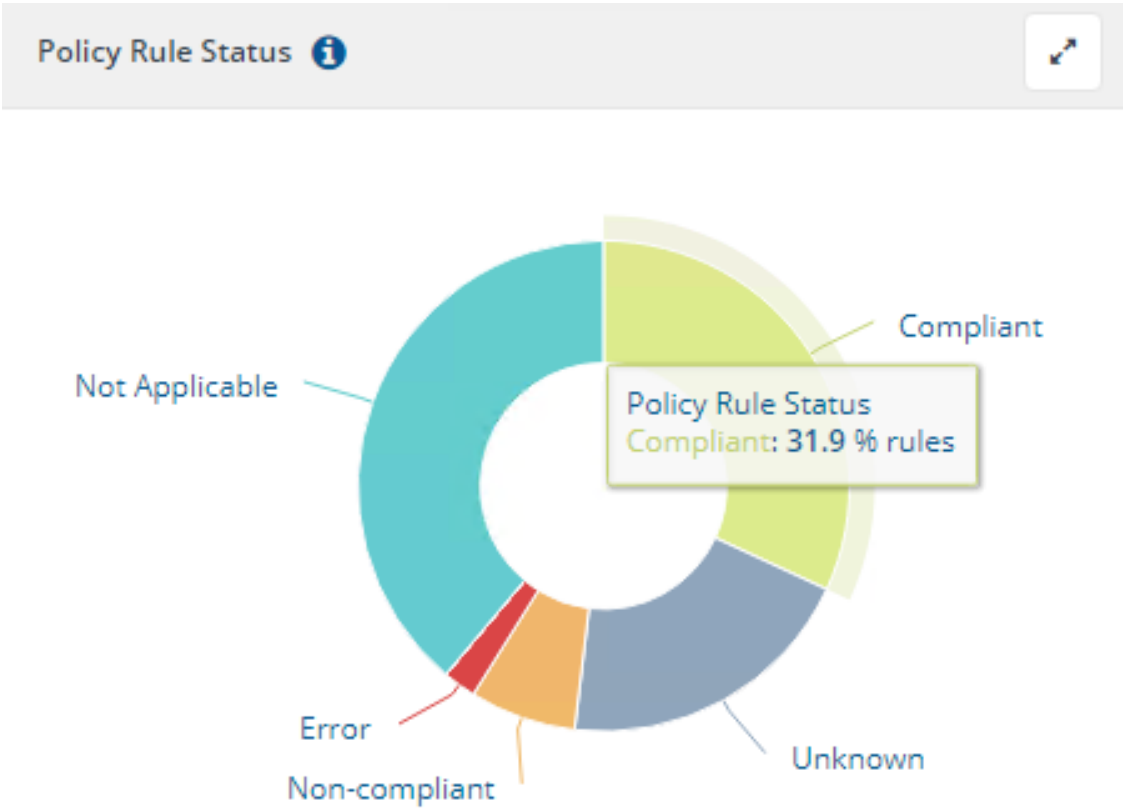
In the above example, 37 rules were deployed to a representative sample of 5 devices across the IT estate. This gives 185 policy rule deployments of which 59 rule deployments reported Compliance giving an overall Policy Rule compliance of 31.9%.

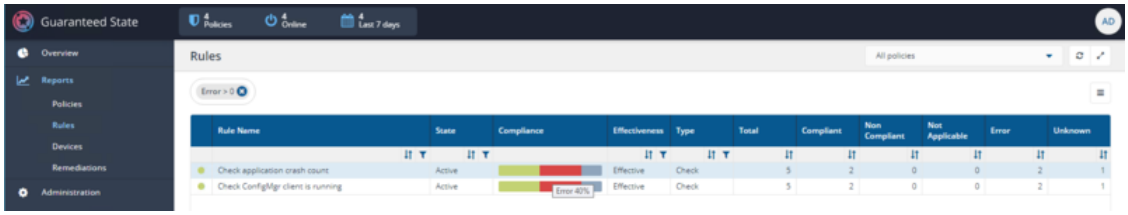
State	Description
Compliant	The proportion of policy rule deployments for which devices reported compliance.
Non-compliant	The proportion of policy rule deployments for which devices reported non-compliance.
Error	The proportion of policy rule deployments for which devices reported rule evaluation failure.
Not Applicable	The proportion of policy rule deployments for which devices reported not applicable. Typically, this would occur for devices to which a deployed rule was applicable only for a different platform, such as deploying Windows Client Health policy rules to macOS devices.
Unknown	The proportion of policy rule deployments for which devices have yet to receive, evaluate or report back on their compliance position. In the example above 20% of the policy rule deployments report as Unknown because one of the five devices to which policies have been deployed has remained offline for several days.

After the hotfix:

State	Description
Compliant	Rule check passed.
Non-compliant	Rule check failed.
Error	Rule could not evaluate its precondition, triggers, check or fix.
Not Applicable	Rule precondition did not pass. Typically, this would occur for devices to which a deployed rule was applicable only for a different platform, such as deploying Windows Client Health policy rules to macOS devices
Unknown	Rule hasn't yet been delivered, evaluated or reported a compliance status. In the example above 20% of the policy rule deployments report as Unknown because one of the five devices to which policies have been deployed has remained offline for several days.

The drill down navigates to the Rules Report filtered by Policy Rule Status, such as Policy Rule Status is Error.

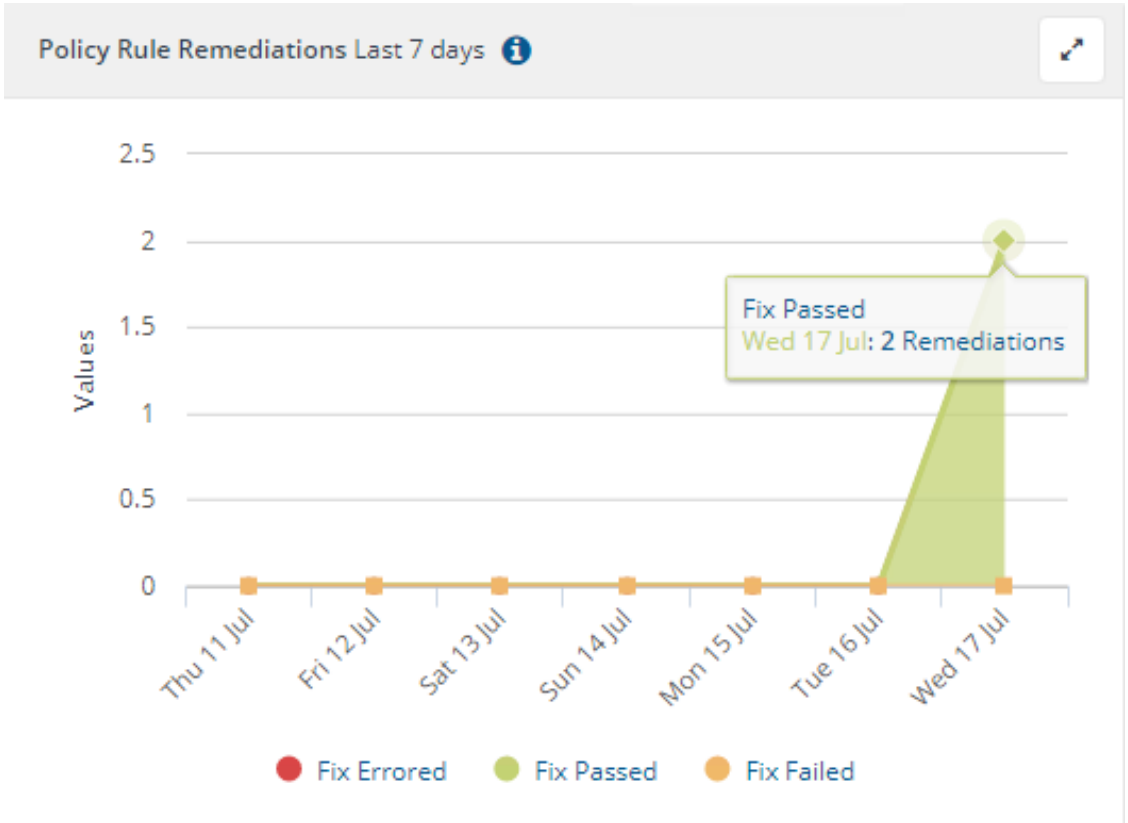


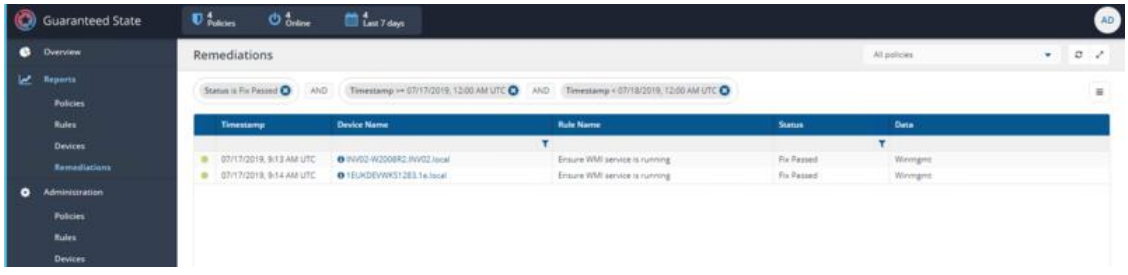


8.3.5.1.7 Policy Rule Remediations Last 7 days

This pane shows a daily remediation summary applied to non-compliant devices by policy rules.

The drill down navigates to the **Remediation** report filtered by remediation status and timestamp period, such as remediation status is fixed and timestamp in a given time period.





8.3.6 Administration menu

Creating and configuring Guaranteed State Policies.

Note

Guaranteed State can be reached directly using the following URL:

`https://<tachyon DNS Name FQDN>/Tachyon/App/#/guaranteedstate/`

where <tachyon DNS Name FQDN> is the one set up during the preparation phase, as described under the heading Preparation: DNS Names.

8.3.6.1 Policies page

The **Policies** page lets you view and manage the current Guaranteed State policies. From this page you can:

Create a **New** policy and assign and unassign existing rules

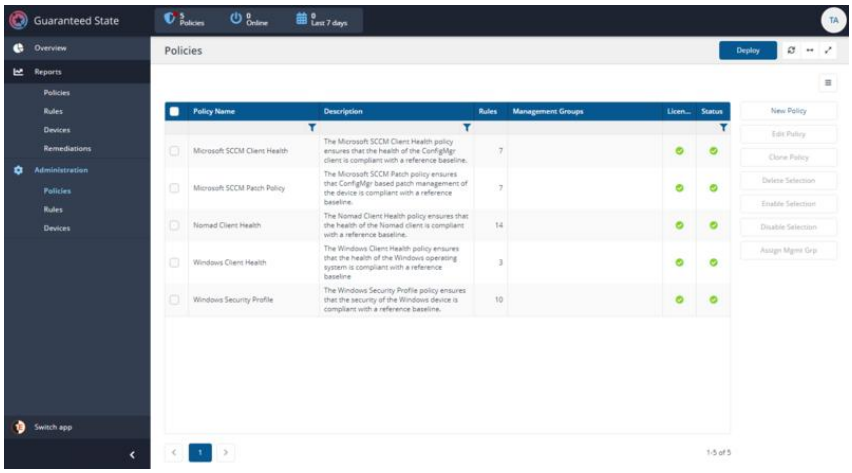
Edit an existing policy and assign and unassign existing rules

Clone an existing policy

Delete an existing policy

Enable or **Disable** an existing policy

Assign (or unassign) an existing policy to one or more Management Groups.



8.3.6.1.1 Creating a new policy

To create a new policy from selected Instructions:

<some instructions here>

8.3.6.1.2 Editing an existing policy

<some instructions here>

8.3.6.1.3 Cloning a policy

<some instructions here>

8.3.6.1.4 Deleting an existing policy

<some instructions here>

8.3.6.1.5 Enabling or Disabling an existing policy

<some instructions here>

8.3.6.1.6 Assigning or unassigning an existing policy

<some instructions here>

8.3.6.2 Rules page

The **Rules** page lets you view and manage the Guaranteed State rules. From this page you can:

Create a **New** rule and configure it

Edit an existing rule and configure it

Clone an existing rule with a new name

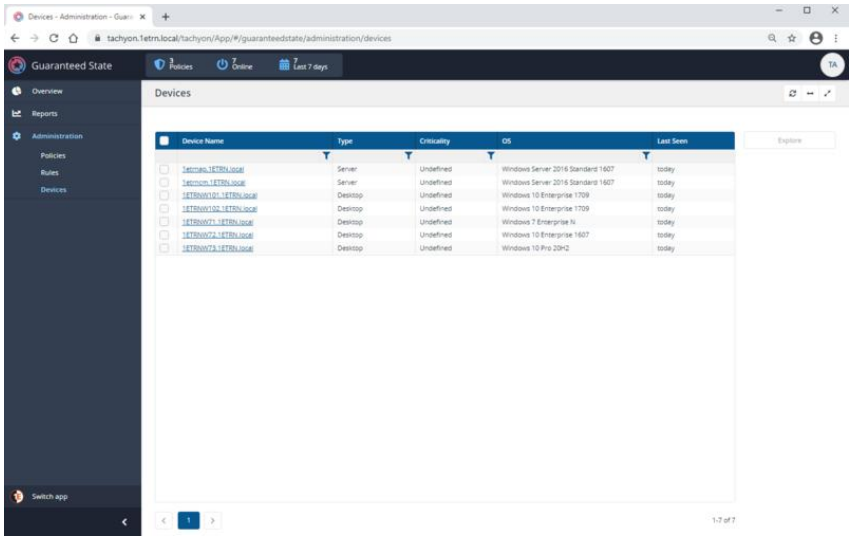
Delete an existing rule

Enable or **Disable** an existing rule

<picture>

8.3.6.3 Devices page

The **Devices** page provides a list of all devices visible to Guaranteed State. You can display a Device view for a selected device by clicking on its link in the **Device Name** column. You can also select one or more entry from the list and choose to use that selection as the scope for an Explorer session.

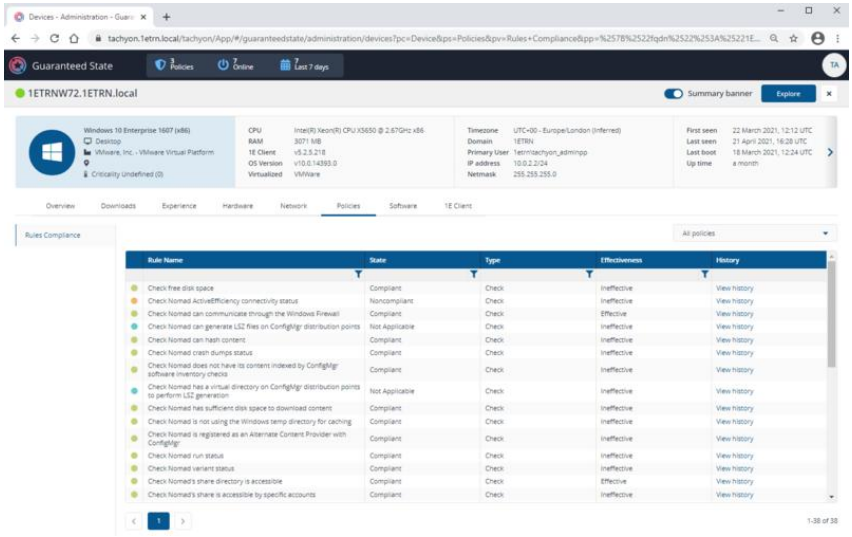


8.3.6.3.1 The Devices view Policies tab

The default view in the Guaranteed State devices view is Policies. The remaining tabs display information corresponding to an app, feature or data set implemented in Introducing Tachyon. Other tabs are visible if an app has been installed and licensed, and the user has permissions to use the app.

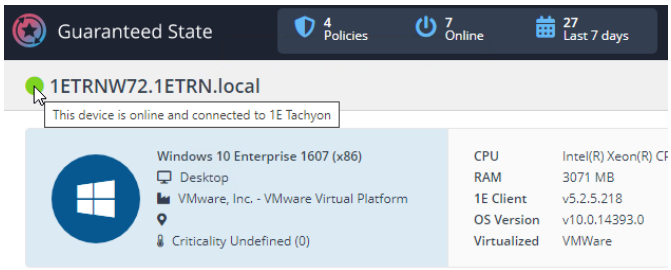
Clicking on one of the links in the **Device Name** column of the **Devices** page displays the Device view for the selected device. The aim of the Device view is to provide a combined overview of all the information known about a device along with the ability to retrieve information about the device in real time. When displaying the Device view from a Guaranteed State page the view defaults to the **Policies** tab. The **Policies** tab contains information derived from and useful for using Guaranteed State.

The **Summary banner** toggle at the top of the page (the default toggle setting is off), shows general device details, and the **Explore** button navigates you to the Explorer app, refer to Using Tachyon Explorer for details.

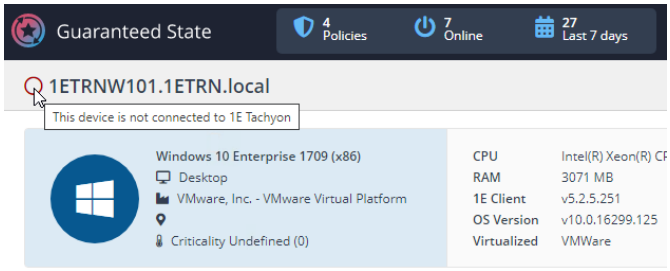


8.3.6.3.1.1 Is the Device is online and connected to Tachyon

In the picture opposite the device 1ETRNW72 is showing as online and connected to Tachyon, this is indicated by the green traffic light next to the device name at the top of the page. Hovering your mouse over the traffic light displays the message
This device is online and connected to 1E Tachyon.



In the picture opposite the device 1ETRNW101 is showing as not connected to Tachyon, this is indicated by the gray traffic light next to the device name at the top of the page. Hovering your mouse over the traffic light displays the message **This device is not connected to 1E Tachyon**.

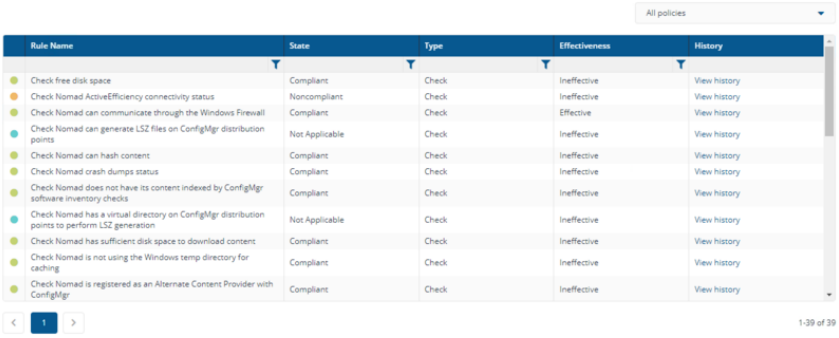


8.3.6.3.1.2 Device View table

In the Device View you can see if a device is compliant to the rules deployed in your environment, if they are effective and view information to assist with troubleshooting.

Column	Description
Traffic light	Traffic light status relates to the **State** column. Green - Device is **Compliant** Orange - Device is **Noncompliant** Blue -Device is **Not Applicable**.
Rule Name	Name of a specific rule.
State	Device state per rule, for example: **Compliant** - rule check passed. **Noncompliant** - rule check failed. **Not Applicable** - rule precondition did not pass.
Type	Whether the rule is one of two types: **Fix** - allows you to define a desired state for the device and then enforce that state. For example, you could mandate that a registry key exists and contains a specific value. Again, you can report on the application of these fix rules to devices. **Check** - allows you to verify that a device has a particular state, such as a registry key having a specific value. You can then view summary and detail reports which show devices that are compliant and not compliant with the check rules.
Effectiveness	Rule effectiveness, either:

Column	Description
	Effective - the rule has been deployed and at least one device has changed its compliance position for this rule in the last thirty days **Ineffective** - the rule has been deployed, but no devices have changed their compliance position for this rule in the last thirty days.
History	Clicking View history displays the related history per rule for the selected device. **Timestamp** - for example **29-04-2021 11:34:01 UTC** **Status** - if the Check or Fix failed or passed **Data** - details related to the event. For example, a message related to the rule **Check Nomad's share directory is accessible** , with a **Check Failed** message showing as the **Status** might return a message like, **Permissions on the Nomad share are not valid**.



8.3.6.3.1.3 Policies filter

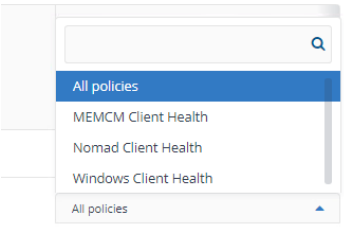
You can use the policies filter to differentiate between device compliance for the different policies you have deployed in your environment, the default view is **All Policies**.

In our example we have deployed three policies:

MEMCM Client Health

Nomad Client Health

Windows Client Health.



In the example we have filtered the view on the **Windows Client Health** policy which shows two Rules:

Check free disk space

Check WMI repository health.

For more information about Guaranteed State policies and using them refer to Using Guaranteed State for the following:

Integrated Product Packs

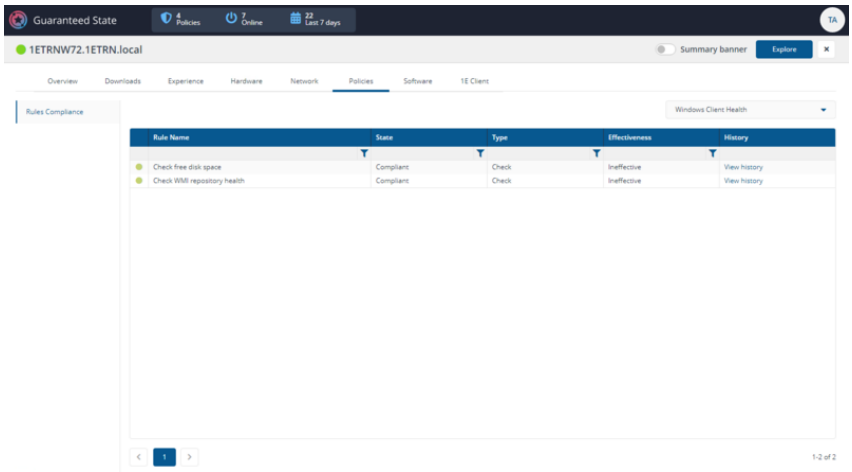
Deploying a Policy

Defining your own policy

Using Explorer to investigate devices in Guaranteed State

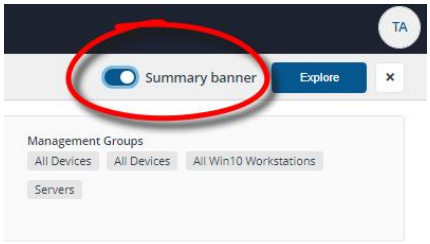
Guaranteed State Overview page

Administration menu.



8.3.6.3.2 The Device View Summary banner

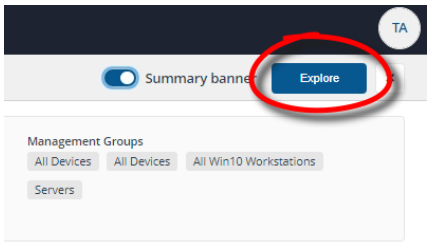
The Summary banner displays a quick summary of the information provided in the various tabs displayed in the Device View. It can be viewed by toggling the **Summary banner** switch to on.



The following image shows the Summary banner displayed for a particular device.

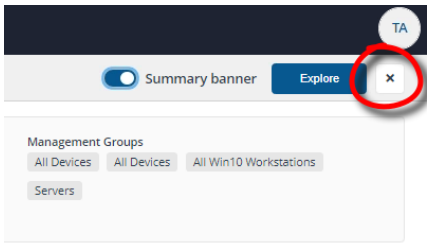
8.3.6.3.3 Launching the Explorer from the Device View

You can click on the **Explore** button in the Device View to launch Explorer with the current device set as the scope.



8.3.6.3.4 Closing the Device View

The Device View is a popup that is displayed when clicking on the name of a device on a page where devices are displayed. To return to the page you came from you need to click the x button.



8.3.6.3.5 Additional Device View tabs

In addition to the **Policies** tab, there are a number of other tabs, each corresponding to an app, feature or data set implemented in Introducing Tachyon:

The **Overview** and **1E Client** tabs are always present in the **Device View**. Other tabs are visible if an app has been installed and is licensed.

Each tab has one or more panels with tiles populated with data from various sources, some by instructions that are run instantly, with results cached for 3 minutes. An appropriate error message is displayed instead of a tile in the following circumstances:

If the device is offline, as indicated by the color of the icon in the top left

The user does not have at least Viewer permission to view use the license the tab or panel

The user does not have questioner permission to run the instruction

An instruction has not been uploaded.

The Device View tabs and panels page lists the names of tabs and their panels, and a description of each tile indicating how the tile is populated.

Tab	Panel	Description	Data source
Overview	**Details**	Displays a number of tiles sorted into **Identification**, **Hardware and Operating System** and **Connectivity and Activity** columns that show information for the selected device retrieved from the online status information stored in the Tachyon Master database. The columns and tiles are shown in the following table: Column / Tile / Description **Identification** / Identification / Display's the current device: FQDN Name Domain	Data from Tachyon Master (the latest online status message)

Tab	Panel	Description			Data source
				Criticality Serial Number 1E Client Tachyon GUID.	
			Location	Displays the device's: Timezone Offset Location Locale.	
			Grouping	Displays the device: Tags - freeform tags applied to	

Tab	Panel		Description		Data source
				the device Coverage Tags - any device tags applied to the device Mgmt. Groups - lists the management groups the device is a member of.	
		Hardware and Operating System	Hardware	Shows hardware details for the device:	

Tab	Panel	Description		Data source
			Virtual /Physical	
			Manufacturer	
			Model	
			Device Type	
			Chassis Type	
			RAM	
			CPU Type	
			CPU Architecture	
			SMBIOS GUID.	
		Operating System	Shows operating system, type and version for example:	

Tab	Panel	Description			Data source
				Type	
				Version	
				Version Number	
				Architecture	
				Installation.	
		Connectivity and Activity	Connectivity	Shows current device connectivity status:	
				Status	
				Last Connected	
				First Connected	
				Certificate Type	
				Certificate Expiry	

Tab	Panel	Description			Data source
				Connection State Local IP Address MAC Address Connecting IP.	
			Activity	Shows Last Boot date and time and current user.	
Env. Variables	Shows a list of the environment variables set on the device.				
Resource Usage	Two panels: **Resource Usage over the last hour** - shows system disk, CPU and memory usage per minute for the last one hour **Resource Usage at** *day/month/year time* - shows executable resource usage for a specific minute:	1E-TachyonPlatform-Hardware-ResourceUsage 1E-TachyonPlatform-Hardware-ResourceUsageByMinute			

Tab	Panel		Description	Data source
	Column	Description		
	Product	Resource name, for example 1E Client		
	Executable	Resource executable, for example 1e.client.exe		
	Instance Count	Number of currently running instances.		
	Cpu Percent	Perentage of CPU currently being consumed.		
	Memory Virtual Mb	Virtual memory consumed in Mb.		
	Memory Physical Mb	Physical memory consumed in Mb.		
	Io Read Kb Per Second	Number of associated read input/output operations per second.		
	Io Write Kb Per Second	Number of associated write input/output operations per second.		
	Handle Count	The number of object handles.		
Downloads	**Summary**		Download activity and status for the device. Whenever you click on an FQDN on any of the Nomad pages then the **Device View** will be displayed with the **Downloads** tab selected.	Data from Content Distribution.

Tab	Panel	Description	Data source
Content	Content Titles on the selected device, the default view is from **All Sources**, **All Types** and **All Status**. **Note** You may see a difference in the number of items in a device's Nomad cache versus that displayed in the Nomad app Device View. This is because if downloaded content has been deleted from Configuration Manager, the content titles cannot be resolved in the Nomad app and are not displayed. This is under consideration for re-design and may be revised in future versions of Nomad.	Data from Content Distribution.	
Nomad Configuration	**1E Nomad Branch Settings .**	1E-Nomad-NomadBranchSettings	
Experience	**Metrics**	Metrics are the data points that are collected by the 1E Client and sent to the Tachyon server. They are collected at different intervals depending on the type of data that is being collected.	Data from Experience metrics
Trends	The Trends tab shows the changes in the scores over time. Hovering over any of the bars shows the details for that time and event. If the user viewing the device details also has the ability to at least ask a question in Explorer the Explore button will be visible.	Data from Experience metrics	

<table>
<tr><th>Tab</th><th>Panel</th><th>Description</th><th>Data source</th></tr>
<tr><td>Logs</td><td>The Event Logs tab gives you a listing of the Windows Event log entries for that device. This brings that data to this view and is very useful when determining the root cause of an issue that has been reported on the device.</td><td>Data from Experience metrics</td><td></td></tr>
<tr><td>Application Interactions</td><td>Shows user interaction times and ratios across applications measured over the last 30 days</td><td>1E-Experience-ApplicationInteraction</td><td></td></tr>
<tr><td>User interactions</td><td>Shows user interactive sessions with activity over last 30 days.</td><td>1E-Experience-UserInteractionHistory</td><td></td></tr>
<tr><td>Hardware</td><td>Disk drives</td><td>Shows disk drives, including hardware and usage information.<table><tr><th>Column</th><th>Description</th></tr><tr><td>Drive</td><td>Drive letter.</td></tr><tr><td>Volume Name</td><td>Volume name, if set.</td></tr><tr><td>Drive Type</td><td>Drive type, for example:
Removable Disk
Local Disk</td></tr></table></td><td>1E-Tachyon Platform-Hardware-DiskDrives</td></tr>
</table>

Tab	Panel	Description		Data source
			Compact Disk.	
		Size Gb	Total disk size in Gb.	
		Free Space Gb	Current free space in Gb.	
		Usage Percent	Percentage used of total drive space.	
		File System	File system, for example NTFS.	
		Manufacturer	Standard or SSD drive.	
		Model	Drive manufacturer.	
		Serial Number	Unique disk serial number.	
		Partition	Drive and partition of the specific drive.	

<table>
<tr><th>Tab</th><th>Panel</th><th>Description</th><th>Data source</th></tr>
<tr><td></td><td></td><td>Firmware Revision Drive firmware version.

Device ID Device ID of the specified disk.</td><td></td></tr>
<tr><td>Peripherals</td><td>Shows the list of plug and play hardware devices (Windows only).

Column | Description
Device Type | Hardware device, including for example things like:
Battery
Monitor
Keyboard
Mouse
Ports
SoftwareDevice.
Name | Device name.
Instance Count | Number of instances of a peripheral device.
Service | Associated Windows service, for example atapi, serial, PCI, ACPI.</td><td>1E-TachyonPlatform-Hardware-Devices</td><td></td></tr>
<tr><td>Network</td><td>Throughput</td><td>Shows network throughput on all adapters for the last</td><td>1E-Tachyon Platform - Network</td></tr>
</table>

<table>
<tr><th>Tab</th><th>Panel</th><th>Description</th><th>Data source</th></tr>
<tr><td></td><td></td><td>hour, represented by the following tiles:

Average throughput - including Timestamp, Bytes Recieved per Second, Bytes Sent Per Second

Bytes received per second

Bytes sent per second.</td><td>- Average Throughput</td></tr>
<tr><td>Interface configuration</td><td>Returns the output from the native network interface configuration command (e.g. ipconfig or ifconfig).</td><td>1E-TachyonPlatform-Network-InterfaceConfiguration</td><td></td></tr>
<tr><td>DNS</td><td>Shows the Cache and Host file tiles:

DNS Cache Contents - with the entries from local DNS cache, Host Name and Address.

HOSTS file - shows the content of the drivers/etc/hosts file.</td><td>1E-TachyonPlatform-Network-DnsCache

1E-TachyonPlatform-Network-HostFileContent</td><td></td></tr>
<tr><td>TCP connections</td><td>Returns a list of established TCP connections.

<table><tr><th>Column</th><th>Description</th></tr><tr><td>Process Name</td><td>Local process name.</td></tr><tr><td>Process Id</td><td>Uniquely identifies an active process.</td></tr><tr><td>Class</td><td>Class of Internet networking protocol.</td></tr></table></td><td>1E-TachyonPlatform-Network-TcpConnections</td><td></td></tr>
</table>

Tab	Panel		Description	Data source
	Local Address	Local network address.		
	Local Port	Network port used by a specific process.		
	Remote Address	Source IP address from which the traffic came from.		
	Remote Port	Remote port used by a specific process.		
	Latency Ms	The time taken in milliseconds for data or a request to go from a source to a destination.		
Listening ports	Returns a list of processes which are listening for network connections.		1E-TachyonPlatform-Network-ListeningPorts	
	Column	Description		
	Process Name	Local process name.		
	Process Id	Uniquely identifies an active process.		
	Class	Class of Internet networking protocol.		
	Local Address	Local network address.		
	Local Port	Network port used by a specific process.		
	Product	Related product, for example host process for Windows Services,		

<table>
<tr><th>Tab</th><th>Panel</th><th>Description</th><th>Data source</th></tr>
<tr><td></td><td>Local Security Authority Process, SCNotification.</td><td></td><td></td></tr>
<tr><td>ARP Cache</td><td>Returns a list of processes which are listening for network connections and also shows routing tables.</td><td>1E-TachyonPlatform-Network-ArpCache

1E-TachyonPlatform-Network-RoutingTable</td><td></td></tr>
<tr><td>WIFI</td><td>Shows a list of visible wifi networks, including basic network properties.

<table>
<tr><th>Column</th><th>Description</th></tr>
<tr><td>SSID</td><td>WiFi network name.</td></tr>
<tr><td>Is Connected</td><td>Shows as either true or false, dependent on whether the corresponding adapter is connected to the network.</td></tr>
<tr><td>Is Hidden</td><td>Shows as true if the WiFi network is not broadcasting a public SSID.</td></tr>
<tr><td>Is Secure</td><td>Shows as either true or false:

true - if the WiFi network is secure

false - if the network is open.</td></tr>
<tr><td>Signal</td><td>Shows WiFi signal quality; from 0 (worst) to 100 (best).</td></tr>
<tr><td>Authentication</td><td>The default authentication mechanism supported by the network.</td></tr>
<tr><td>BSSI IDs</td><td>The Service Set Identifier (SSID) of the network, it will</td></tr>
</table>
</td><td>1E-TachyonPlatform-Network-WiFiNetworks</td><td></td></tr>
</table>

<table>
<tr><th>Tab</th><th>Panel</th><th>Description</th><th>Data source</th></tr>
<tr><td></td><td></td><td>be empty if the network is hidden.</td><td></td></tr>
<tr><td></td><td>Encryption</td><td>Shows the default encryption mechanism supported by the network.</td><td></td></tr>
<tr><td></td><td>Adapter</td><td>Shows the WiFi network adapter name to which this network is visible.</td><td></td></tr>
<tr><td>Policies</td><td>Rules Compliance</td><td><table><tr><th>Column</th><th>Description</th></tr><tr><td>Rule Name</td><td>Name of rules applied to the current device. The viewable list relates to the selected Tachyon policy from the policy dropdown on the page.</td></tr><tr><td>State</td><td>If the device state is Compliant, Noncompliant or Not Applicable.</td></tr></table></td><td>Data from Guaranteed State</td></tr>
</table>

Tab	Panel	Description		Data source
		Type	Rule type: Check - allows you to verify that a device has a particular state, such as a registry key having a specific value Fix - allows you to define a desired state for the device and then enforce that state.	
		Effectiveness	Policy rule effectiveness is the usefulness of policy rules and is represented as either: Disabled - the rule has not yet been enabled from the	

Tab	Panel	Description	Data source
		Guaranteed State Rule Administration page, so it is not currently active Unassigned - the rule is enabled, but has not been deployed to any devices Ineffective - the rule has been deployed, but no devices have changed their compliance position for this rule in the last thirty days Effective - the rule has been deployed and at least one device has changed	

Tab	Panel	Description		Data source
			its compliance position for this rule in the last thirty days.	
		History	Rule history.	
Software	**Installations**	Shows (per-device) installed software.		1E-Tachyon Platform-Software-Installations
		Column	Description	
		Product	Software product name.	
		Publisher	Software publisher.	
		Version	Product version number.	
		Architecture	Instruction set architecture (ISA) version.	
		Install Date	Software installation date.	
Windows	Shows list of installed Windows services and their current state.	1E-TachyonPlatform-Software-Services		

<table>
<tr><th>Tab</th><th>Panel</th><th>Description</th><th>Data source</th></tr>
<tr><td>services</td><td>
<table>
<tr><th>Column</th><th>Description</th></tr>
<tr><td>Name</td><td>Windows service name.</td></tr>
<tr><td>State</td><td>Windows service state, Running or Stopped.</td></tr>
<tr><td>Startup Type</td><td>Windows service startup type, for example Automatic, Automatic (Delayed Start), Manual, Disabled.</td></tr>
<tr><td>Process Id</td><td>Uniquely identifies an active process.</td></tr>
<tr><td>Description</td><td>Windows service description.</td></tr>
<tr><td>Logon Account</td><td>Windows service logon account context.</td></tr>
<tr><td>Type</td><td>Windows services type, for example file system driver, kernel driver, shared process.</td></tr>
</table>
</td><td></td><td></td></tr>
<tr><td>Env. Variables</td><td>Shows operating system environment variables.</td><td>1E-TachyonPlatform-Software-EnvironmentVariables</td><td></td></tr>
<tr><td>Processes</td><td>Shows detailed information about all running processes.
<table>
<tr><th>Column</th><th>Description</th></tr>
<tr><td>Product</td><td>Software product name.</td></tr>
<tr><td>Executable</td><td>Executable name.</td></tr>
</table>
</td><td>1E-TachyonPlatform-Software-Processes</td><td></td></tr>
</table>

Tab	Panel	Description	Data source
	Version	Product version number.	
	Devices count	How many devices are reporting.	
	Crashes	Number of times this software crashed during the last 24-hour reporting period.	
	Hangs	Number of times this software crashed during the last 24-hour reporting period. **Note** Software crash and hang information is obtained from Windows event data. For background information on Windows events and the event viewer refer to https://support.microsoft.com/en-gb/help/302542/how-to-diagnose-system-problems-with-event-viewer-in-microsoft-windows	
	Performance anomalies	Number of performance anomalies detected in this software during the last 24-hour reporting period.	
	I/O write KB/s	Average disk I/O read rate per second during the last 24-hour reporting period.	

Tab	Panel	Description	Data source
	I/O write KB/s	Average disk I/O write rate per second during the last 24-hour reporting period. **Note** For background information on analyzing disk storage performance refer to https://docs.microsoft.com/en-gb/archive/blogs/cotw/analyzing-storage-performance	
	Virtual Memory Usage KB	Average Virtual Memory Usage KB during the last 24-hour reporting period. **Note** For an explanation of Windows Virtual Memory organization refer to https://answers.microsoft.com/en-us/windows/forum/windows_10-performance/physical-and-virtual-memory-in-windows-10/e36fb5bc-9ac8-49af-951c-e7d39b979938 and https://support.microsoft.com/en-us/help/2160852/ram-virtual-memory-pagefile-and-memory-management-in-windows	
	Processor Time Seconds	Each instance of the executable will burn processor time. This column gives the average of the total time consumed by each process instance per second. Each instance uses the sum of all time used by each core in parallel. Therefore, it is possible to see more seconds here than in a day	

Tab	Panel	Description	Data source
		(usually 60 x 60 x 24 = 86400) for the whole column, if your system is working extremely hard 24x7. The theoretical maximum would be somewhere near ***number of cores*** x ***seconds per day*** . Hence, 'Processor Time' rather than 'Human Time'	
	Processor Time %	This is an easier notion than Processor Time Seconds. This is the average of the processor consumption of each instance. Each instance of this process will have caused different percentages of compute resource in all the processors and cores to be used over time (unless they have specifically requested certain core affinity). For each minute each process is running, a profile of the usage is built for the whole day. This value is the average of all of those samples. There is no way to work out, for any one of the process instances involved, how long any particular instance was running for. This could indicate a process that is going wild with resources, but it would take more investigation on the device to discover for how long this is happening. It is perfectly possible to see all the values in this column adding up to more than 100% as the processes were not necessarily running at the same time. **Note** For further information on Processor time refer to https://social.technet.microsoft.com/wiki/contents/articles/12984.understanding-processor-processor-time-	

Tab	Panel	Description	Data source

and-process-processor-time.aspx

Responsiveness Impact %

An indicator of how reactive a process is to activity by other processes on the device. Typically, anti-virus products watch and respond to potentially suspicious activity such as increased network traffic. Anti-virus products will differ in their impact on the overall performance of a device.

Note

Responsiveness Impact % is used to indicate how sensitive a process appears to be to the use of system resources by other processes on a device. For example, Security Protection software present on a device may reveal a spike in its activity whenever a new process is started on that device.

This would typically be because the Security Protection software may wish to ensure that the new process starting on the device is present in a security white list. Other software may also react to activity by other processes and by reacting they impact system resource uses, thereby adversely affecting the user's experience. So it is useful to be able to identify

Tab	Panel	Description	Data source
		software with the highest Responsiveness Impact on a device and potentially investigate further. **Note** Responsiveness Impact % represents the proportion of the increased CPU activity detected by the 1E Client as a result of performing a set of operating system-level operations that can be attributed to a given running process. Examples of these would be Windows registry and resource creation operations. It is reported as a percentage to normalize results across devices that offer a range of computing power. For example, if *software.exe* on a device is attributed a Responsiveness Impact of 53% this means that more than half of the spike in CPU usage caused by software monitoring activity on that device can be attributed to *software.*	
	Handle Count	Average number of Windows handles used by this software during the last 24-hour reporting period. **Note**	

Tab	Panel		Description	Data source
		For further information on Windows handles refer to https://docs.microsoft.com/en-us/windows/win32/sysinfo/handles-and-objects For tips on examining open handles for any Windows process refer to https://docs.microsoft.com/en-us/sysinternals/downloads/handle and https://techcommunity.microsoft.com/t5/windows-blog-archive/pushing-the-limits-of-windows-handles/ba-p/723848		
	Physical Memory Usage KB	Average Physical Memory Usage KB during the last 24-hour reporting period. **Note** Please refer to https://docs.microsoft.com/en-us/sysinternals/downloads/rammap for a useful tool to examine physical memory allocation on a device.		
1E Client	**Binaries**		Shows a list of the binary files in the executable folder of the 1E Client. Column: **File Name** Description: Associated 1E	1E-Tachyon Platform-Client-Binaries

<table>
<tr><th>Tab</th><th>Panel</th><th>Description</th><th>Data source</th></tr>
<tr><td></td><td></td><td></td><td>Client file name.</td><td></td></tr>
<tr><td></td><td></td><td></td><td>File Version</td><td>Software version.</td></tr>
<tr><td></td><td></td><td></td><td>File Size</td><td>File size in bytes.</td></tr>
<tr><td></td><td></td><td></td><td>Description</td><td>File description</td></tr>
<tr><td></td><td></td><td></td><td>Date Created</td><td>The date the file was written to disk.</td></tr>
<tr><td></td><td></td><td></td><td>Date Modified</td><td>The date the file was last saved.</td></tr>
<tr><td>Configuration file</td><td>Shows the full content of the 1E Client configuration file, including:
Logging settings
Communication settings
Agent settings
Module settings.</td><td>1E-TachyonPlatform-Client-ConfigFileContent</td></tr>
<tr><td>Extensibility</td><td>Shows extensibility objects (modules and providers) loaded by the 1E Client.
<table><tr><th>Column</th><th>Description</th></tr><tr><td>Type</td><td>Module or Provider component.</td></tr></table></td><td>1E-TachyonPlatform-Client-Extensibility</td></tr>
</table>

Tab	Panel		Description	Data source
	Binary Name	Associated 1E Client binary name, for example 1E.Client.Module.Interaction.dll		
	Name	Name, for example Interaction.		
	Version	1E Client version, for example 5.2.5.251		
Local Storage	Shows **Data Files** and **Client Inventory Database Use** tiles that display the list of: Data files (logs, databases, etc) created by the 1E client Tables in the 1E Client Inventory database, along with a row count per table.		1E-TachyonPlatform-Client-DataFiles 1E-TachyonPlatform-Client-InventoryDatabaseUse	

8.4 Troubleshooting

For a general methodology for investigating issues, as well as identifying key issues and their resolutions, and for known issues relating to specific components, please refer to their troubleshooting pages, refer to 1E Troubleshooting.

8.4.1 Known issues

Lists of the current known issues with implementing, configuring, and using Guaranteed State.

If you cannot find an issue and its workaround on this page:

Refer to Known issues for the Platform and other applications.

Try searching the 1E Support Portal https://support.1e.com/ for issues which have hotfixes.

If you need further help, please refer to the Troubleshooting page for how to contact 1E Support and the technical support process.

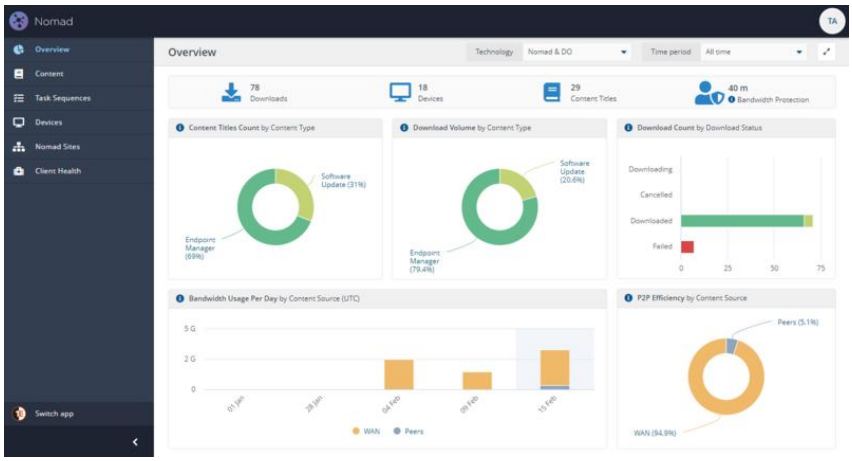
Issue	Description	Workaround
Any pending changes in Guaranteed state and/or Experience applications that are	Tachyon Setup runs a post installation action to automatically deploy all	Ensure any pending deployment changes under review are either deployed

Issue	Description	Workaround
deployed during upgrade process from Tachyon Platform v5.1 to v5.2 or v8.0. This is also true if there is an already deployed unlicensed rule/recondition/check or fix.	policies and event subscriptions.	prior to upgrade process is initiated or respective rule/policy/Survey should be marked as disabled to prevent deployment during upgrade process
Guaranteed State Overview pages show incorrect devices when Policy with no Rules have been assigned to a Management Group.	On the Guaranteed State Overview page, the Online, Online last 7 days and Last seen per Criticality Level charts all show incorrect counts when a Policy is assigned to a Management Group, but no Rules have been assigned yet. This will display correct values once Rules are assigned and devices have responded to the events.	None
Opening an instruction or fragment that has been exported using the Consumer API displays the following message when viewed in TIMS: "This instruction definition was signed by CN=Tachyon Explorer Instructions but the content has been tampered with.	An instruction exported through Postman can generate file with whitespace differences and file size between the original file which is not accepted by TIMS as it's considered to be tampered.	Use alternative API tools (e.g Fiddler).
"Ensure Nomad can communicate through the Windows Firewall" remediation is being executed even when firewall is disabled from the GPO.	"Ensure Nomad can communicate through the Windows Firewall" remediation is being carried out when there is a firewall policy which has been disabled through group policy. This means that when firewall policy has been	None

Issue	Description	Workaround
	disabled explicitly, instead of ignoring the fix, the firewall is being set to enabled and the firewall exceptions are set for Nomad.	
On a ConfigMgr Distribution Point, the Rule to "Check the Nomad has a virtual directory on ConfigMgr distribution points to perform LSZ generation" always passes even though a failure reason may be returned in the Data field.	The check fragment should verify that the LSZFILES website setup by Nomad on a DP has certain characteristics, but even when errors are found the check status is "Passed". The logic in the PowerShell parts of the fragments uses a $errorOccurred variable to set the exit code, but this variable is initialized to $false and then never changed even when an error is detected. e.g Data field returns: "Windows authentication not enabled. Require SSL flag is not disabled. Directory browsing not correctly set."	None
1E Client logs several unsuccessful remediation attempts within a 24hr period.	There is currently no longer a cap on the number of time a remediation step can occur on a machine within 24hrs. This differs from 1E Client Health where after 3 failures to remediate an issue, further remediation would not occur until 24hrs have passed.	None

9 1E Content Distribution

Nomad removes the need for distributed servers and intelligently uses only available bandwidth for all content distribution. This means the business is never impacted by Configuration Manager or Windows deployments.



9.1 Introducing Nomad

Nomadremoves the need for distributed servers and intelligently uses only available bandwidth for all content distribution. This means the business is never impacted by Configuration Manager or Windows deployments.

9.1.1 New features in Nomad

Many Nomad features are available with minimal configuration of the 1E Client. However, some features require additional configuration of the 1E Client on Configuration Manager Distribution Points.

9.1.1.1 Platform

Works with Tachyon 8.1

Insights on how Nomad enhances user experience - with the rapid shift to a Work From Anywhere (WFA) workforce and an increased focus on the Digital End-User eXperience, Nomad on Tachyon Platform now provides insights into how it helps to ensure a great user eXperience. With the introduction of Nomad's Bandwidth Protection Reporting, you can now see how Nomad is preventing end-user disruption due to software and update deployments. Bandwidth Protection Reporting will allow you to see the positive impact Nomad is having across the organization, to individual sites, subnets, all the way down to a single client.

Support for Cloud-based content in Task Sequences - cloud-based services to support Work From Anywhere (WFA) users are becoming more critical to the way enterprises work, there is an increased reliance on Cloud Distribution Points for distributing content.

Feature improvements - as Configuration Manager evolves and new features are released, Nomad on Tachyon Platform is being continuously maintained to ensure it works seamlessly with new releases.

9.1.1.2 Client

NomadBranch 8.1 client is the Nomad module in 1E Client 8.1

Support for Cloud-based content in Task Sequences - cloud-based services to support Work From Anywhere (WFA) users are becoming more critical to the way enterprises work, and there is an increased reliance on Cloud Distribution Points for distributing content.

Enhancements:

Improvements to the Certificate Selection criteria to authenticate with a DP (or any download source)

Download reporting now includes back-off data, for Bandwdith Protection Reporting.

9.1.1.3 Tools

Nomad AdminUI Console Extensions now require .NET Framework 4.8

Cloud infrastructure support

Enhancements:

Provide a way for SCCM Console users to use alternate credentials to authenticate with ContentDistribution/Platform, for details refer to Using Nomad pre-caching.

PlatformUrl validation is improved, by logging a warning during installation. In UI mode users have the option of continuing with the installation, for details refer to Installing Nomad Branch Tools.

9.1.2 Nomad overview

An overview of features and enhancements.

Nomad removes the need for distributed servers and intelligently uses only available bandwidth for all content distribution, so the business is never impacted by Configuration Manager or Windows deployments.

In the world of Windows 10 and modern management, there is more content being distributed on your network than ever before to get Windows and applications deployed and keep them up to date. While you are carefully managing some of those deployments through Microsoft Endpoint Manager, others are out of your control. Modern applications self-update, Windows updates may be pulled as required based on policies and users have access to download apps from the Microsoft Store or Store for Business. A lot of that activity is currently invisible to you and may be causing you to miss compliance deadlines.

There is no single, comprehensive view of exactly what is being distributed, to where and from which sources, so you don't really have a clue how it is all affecting your network. How well are peer-to-peer technologies (Nomad, Delivery Optimization) working to reduce the effect this content distribution has on your WAN bandwidth usage? How can you make them more effective? These are the questions we can answer with the Nomad.

9.1.2.1 Simple Nomad Architecture

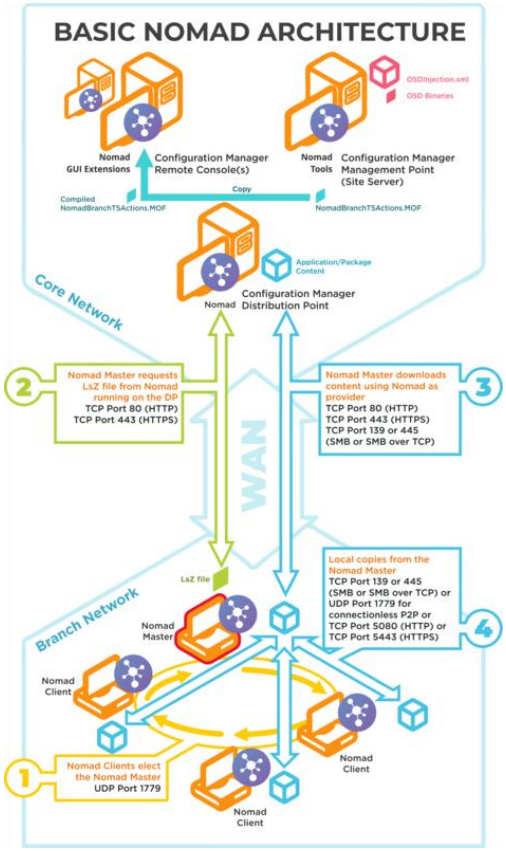
In response to customer demand to simplify the deployment, we've made two architectural changes:

Reduced the number of agents required - 1E has merged the client functionality of Nomad, PXE Everywhere, WakeUp, Shopping and Tachyon into a single 1E Client.

Modernized the back-end infrastructure - Nomad requires a back-end server, which was previously our legacy ActiveEfficiency platform. This now is replaced with the unified Tachyon Platform.

The 1E single agent and platform is a remote endpoint management solution designed to significantly improve IT's ability to support the Work From Anywhere Enterprise. Built around a revolutionary real-time engine, and providing both holistic digital experience monitoring and remediation, it's a powerful tool that helps IT to deliver great employee experiences, anywhere.

Once you are on the Tachyon Platform, you can enable further features including Experience, User Sentiment, Guaranteed State and Patch Success, as well as opening up real-time management to any task by acquiring the appropriate license. To find out more, refer to Introducing Tachyon.



Ports	Notes
UDP 1779	**Step 1** By default, Nomad uses UDP Port 1779 to communicate during the election process for determining the master on a subnet. The Nomad installer will automatically add *NomadBranch.exe*,*NomadPackageLocator.exe* and *PackageStatusRequest.exe* to the list of excepted programs in the native Windows Firewall. The default value for the port may be changed at install time using the MODULE.NOMAD.P2PPORT installer property or post-installation by changing

Ports	Notes
	the P2P_Port registry value. If you change the default port, you must ensure all Nomad clients communicate using the same port. The Nomad port (by default UPD Port 1779) must be open on all wireless access points to facilitate Nomad peer-to-peer communications. Not all vendors enable this port by default, please refer to the specific device vendor's documentation for details on how to enable ports on each WAP device.
TCP 80 (HTTP) TCP 443 (HTTPS)	**Step 2** Nomad Master requests LSZ file from Nomad running on the DP.
TCP 80 (HTTP) TCP 443 (HTTPS) TCP 139 (SMB) TCP 445 (SMB over TCP)	**Step 3** Nomad Master downloads content using Nomad as provider. This communication depends on how the DP is configured. It may be one of the following: HTTP HTTPS SMB SMB over TCP For Configuration Manager the default setting is HTTP or HTTPS.
TCP 139 (SMB) TCP 445 (SMB over TCP) UDP 1779 (used for connectionless P2P) TCP 5080 (HTTP) TCP 5443 (HTTPS)	**Step 4** Local copies from the Nomad master. The recommended way to facilitate Nomad cache access is to enable Windows File and Print Sharing. If this is not feasible on your network environment you can configure Nomad to use different means to access network shares, see Nomad cache for more details on configuring this option. Connections may use one of the following: SMB SMB over TCP Connectionless P2P HTTP

Ports	Notes
	HTTPS

9.1.2.2 Nomad Security

Nomad is a peer-to-peer technology that works by using HTTP/HTTPS or the native Windows OS File and Print Sharing services to share content among computers.

With Nomad, you get improved security features like:

Certificate-based client authentication for peer-to-peer communication, removing the need for a local user account.

Support for Enhanced HTTP in Configuration Manager, including support for removal of the CM Network Access Account support for multiple Certificate Authorities when using HTTPS for peer-to-peer communication.

For more details about Nomad security refer to Ensuring Nomad is secure.

9.1.3 Nomad fundamentals

An overview of the fundamental concepts and terminology needed to understand what Nomad will do for you.

9.1.3.1 What is Nomad?

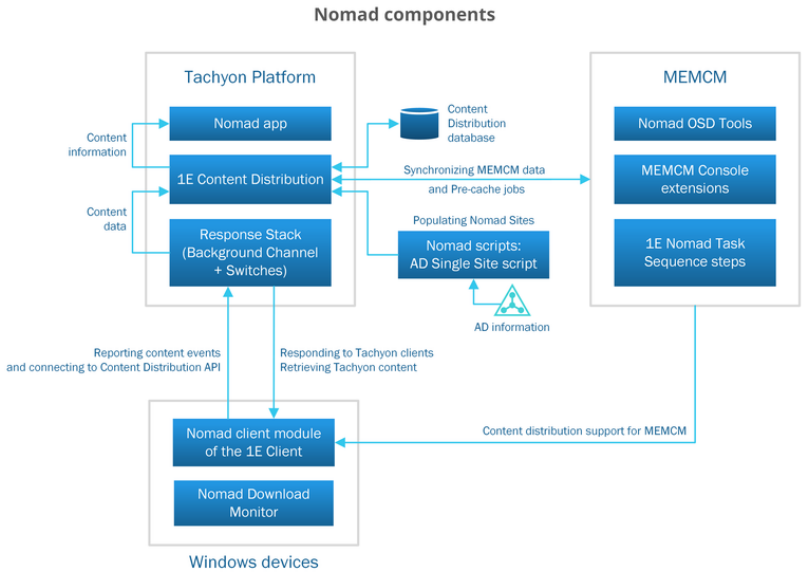
Nomad removes the need for distributed servers and intelligently uses only available bandwidth for all content distribution, so the business is never impacted by Configuration Manager or Windows deployments.

Nomad uses Configuration Manager console extensions to enhance the Configuration Manager Admin console, so you can configure Nomad settings, pause and resume Nomad downloads, use Nomad pre-caching and create baseline configuration items. By integrating with your OSD strategies Nomad maximizes the efficiency of distributing large OS content across the network. It does this by providing a number of Task Sequence steps that can be integrated directly into your OSD Task Sequences. Nomad also supports content distribution for Configuration Manager and Tachyon with the 1E Client.

A new Tachyon Platform component, called 1E Content Distribution, provides support for a number of Nomad features such as Single Site Download. Nomad clients send information back to Content Distribution related to the Nomad features and the performance of Nomad. Content Distribution is a replacement for ActiveEfficiency used in earlier versions of Nomad.

In addition, with the Tachyon Platform there is the new Nomad app replacing the Configuration Manager Nomad Dashboard. The Nomad app provides a high level view of the current status of content throughout the entire network.

The picture opposite shows the high-level relationship between the Nomad components listed in the Nomad components table.



9.1.3.1.1 Nomad components

Nomad component	Description	Dependency
1E Client	The 1E Client, includes the Nomad module which supports content distribution for Configuration Manager and Tachyon. The 1E Client includes other features and modules which are optionally enabled and configured, including: Tachyon PXE Everywhere Shopping Wakeup. The 1E Client is installed on each Windows device as a service, and the 1E Client Deployment Assistant (CDA) can be used with Configuration Manager to deploy it.	Tachyon Platform
Nomad app	The Nomad app provides visibility of content distribution activity and cache status for content distributed by both Nomad and Delivery Optimization. The Nomad app is installed through Tachyon Setup. After installation the Nomad app is available on the Tachyon Platform portal homepage and can be accessed using the Tachyon DNS Alias FQDN. For example:	Tachyon Platform 1E Client

Nomad component	Description	Dependency
	https://tachyon.acme.local/Tachyon	
1E Content Distribution	Content Distribution is a Tachyon Consumer providing control and visibility on content deployments and delivery and is installed through Tachyon Setup. Content Distribution offers visibility for the following via the Nomad app: The status of all deployments, including both delivery and execution of content The effectiveness of Peer to Peer technologies like Delivery Optimization (DO), Nomad and BranchCache Historical trends like Peer to Peer effectiveness Where content is located or cached by a Peer to Peer technology.	Tachyon Platform Configuration Manager
Background Channel	The Background Channel is a Introducing Tachyon component which provides a means for the Nomad module of the 1E Client to retrieve large data items from Tachyon without loading the Tachyon Switch: Stores Tachyon content provided by the Consumer API in the Background Channel for Tachyon clients to retrieve Responds to Tachyon clients retrieving Tachyon content from the Background Channel.	Tachyon Platform
Configuration Manager console extensions	The Nomad Configuration Manager console extensions are installed where its Console is installed. The extensions add the custom Task Sequence steps among other Configuration Manager console extensions. The Nomad Configuration Manager console extensions provide the following capabilities in the Configuration Manager Console:	Configuration Manager

Nomad component	Description	Dependency

Configuration Manager capability	Description
Configure Nomad settings	In software deployment and client settings policies associated with packages, applications and software updates.
Nomad Download Pause	Buttons to pause and resume Nomad downloads, monitoring report to view paused content.
Nomad Pre-caching	Menu item to start the Pre-cache Wizard, monitoring report to view pre-cached content.
Nomad Baseline wizard	Menu items to create and edit baseline configuration items.

The additional Nomad attributes are configured through the Configuration Manager console using custom console extensions. These add properties pages to the standard package, task sequence and client settings dialog boxes and wizards.

Nomad component	Description	Dependency
Nomad OSD Tools	Nomad OSD Tools are required for integrating Nomad with OSD task sequences in Configuration Manager. The tools are installed on the CM Site server(s) and SMSProvider server(s) and install the Nomad files that get injected into a boot image.	Configuration Manager
Nomad download monitor	The Nomad Download Monitor tool is useful for administrators to view the status of downloads on local and remote Nomad client devices. The tool is required only for testing and troubleshooting on selected devices, and is not required or recommended for general deployment.	None

Nomad component	Description	Dependency
Nomad scripts	Sample PowerShell scripts for populating the Content Distribution database to support the following Nomad features: Single Site Download (SSD) Single-site Peer Backup Assistant (SSPBA) High Availability Peer Backup Assistant (HAPBA) WakeUp integration Located in the zip's Scripts folder.	Configuration Manager
1E Nomad Task Sequence steps	Nomad can integrate with OSD to maximize the efficiency of distributing large OS content across the network. The three areas where Nomad integrates with OSD are: WinPE support – providing Nomad functionality when imaging a device Custom task sequence actions – enabling Nomad functionality to be integrated directly into OSD task sequences Configuring PBA hosts – enabling Nomad functionality to be used during OSD to back up user files and settings (USMT data). To support the above, Nomad provides a number of Task Sequence steps that can be integrated directly into your OSD Task Sequences: 1E Nomad task sequence actions 1E Nomad PBA task sequence actions 1E Nomad Pre 6.0 task sequence actions 1E OSD task sequence actions Peer Backup Assistant - PBA.	Configuration Manager

9.1.3.2 Distributing software with Nomad and Configuration Manager

Nomad integrates with the Configuration Manager (CM) client content download process. When Nomad is installed, it registers with the Configuration Manager client as an Alternate Content Provider (ACP), which means the CM client will use Nomad as an alternative to BITS when it requires content if Nomad is enabled for the requested content object. Nomad can be enabled on individual packages (including Driver Packages, Operating System Images, Operating System Upgrade Packages and Boot Images) and Task Sequences.

For Applications and Software Updates, Nomad is enabled on each client for all Applications and Software Updates through Default Client Settings. When the CM client requires Nomad-enabled content, it passes a request to Nomad, which in turn downloads the content, places it in the CM client cache and passes back to the CM client for execution. The 1E Client (with Nomad client module enabled) must be installed on all CM client machines and on all Distribution Points (DP).

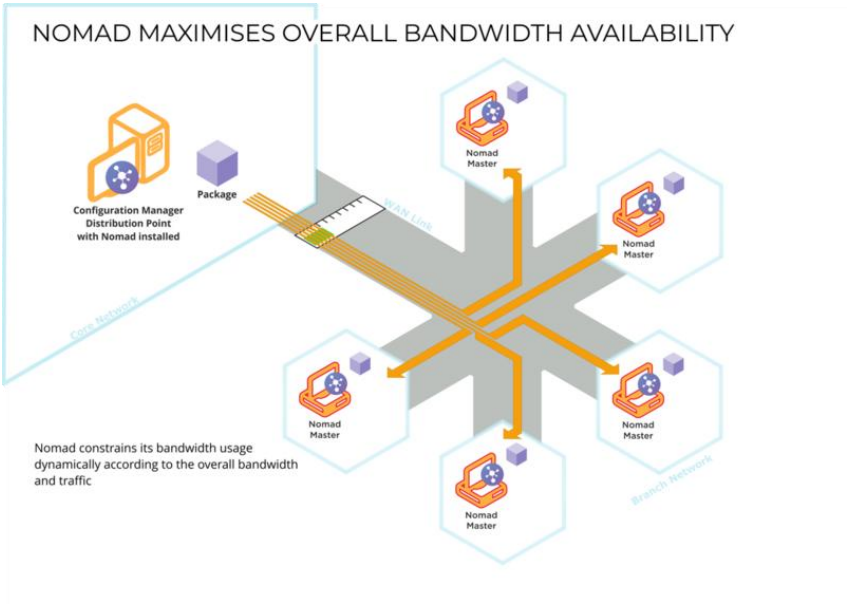
9.1.3.3 Bandwidth Protection

Nomad dynamically analyzes the overall WAN traffic to ensure that it only uses a percentage of the total. It is also aware of mobile devices and knows the difference between wireless and wired connections and is able to select the most efficient available connection to use.

9.1.3.3.1 Full control over WAN link usage

Nomad respects business data on the network – it detects the true end-to-end available bandwidth and monitors this throughout the duration of the download. This is calculated using a sophisticated algorithm that looks beyond the receiving capabilities of each device's network card. If bandwidth is available, the transfer speeds up; if it becomes restricted, the transfer slows down. As a result, overall WAN availability is maximized and the impact on the critical link between the branch networks and the central network is minimized.

To avoid placing a burden on office wireless bandwidth and to use the most efficient transfer system possible, Nomad can be configured to switch from a wireless to a wired network connection automatically when one becomes available. (Please refer to Design Considerations - Managing stable LAN connections).



9.1.3.3.2 Maximizing download speed for high-bandwidth links using Dynamic Block Sizes

The Dynamic Block Size (DBS) feature increases block size on high-bandwidth links to get maximum efficiency, and reduces it on low-bandwidth links to reduce the impact. Using DBS, Nomad is able to automatically decide the appropriate block size for a given link bandwidth and also adjust it as needed during the download if the link conditions change. As a result, Nomad is far more efficient and faster on all types of connection bandwidths while retaining its minimal impact on other link traffic.

> **Note**
>
> DBS is enabled or disabled by configuring Bit 25 in the CompatibilityFlags registry. Setting Bit 25 disables DBS and clearing Bit 25 enables DBS.
>
> In Nomad 7.0 onwards, the DBS feature is turned off by default for new installations, and not changed for upgrades.
>
> Prior to v6.3 the default value of BlockSize registry setting was 32KB (0x8000). From v6.3 onwards the default is 128KB (0x20000).
>
> The installer automatically sets this to 128KB for both fresh installs and upgrades from previous versions. The only exceptions to this are:

It will use the specified value if the BLOCKSIZE property is used in the installation command line or in a MST transform, when doing a fresh install or upgrade

It will retain the previous value of BLOCKSIZE if it was set to anything other than 32KB (the older default), when doing an upgrade.

9.1.3.3.3 Download once to branch

Nomad ensures that software packages are only ever copied once per branch over the WAN, utilizing local computers as temporary file caches to distribute the software locally. This reduces

the bandwidth required for delivering software updates and means that small offices or sites connected by poor network links can receive software updates more reliably.

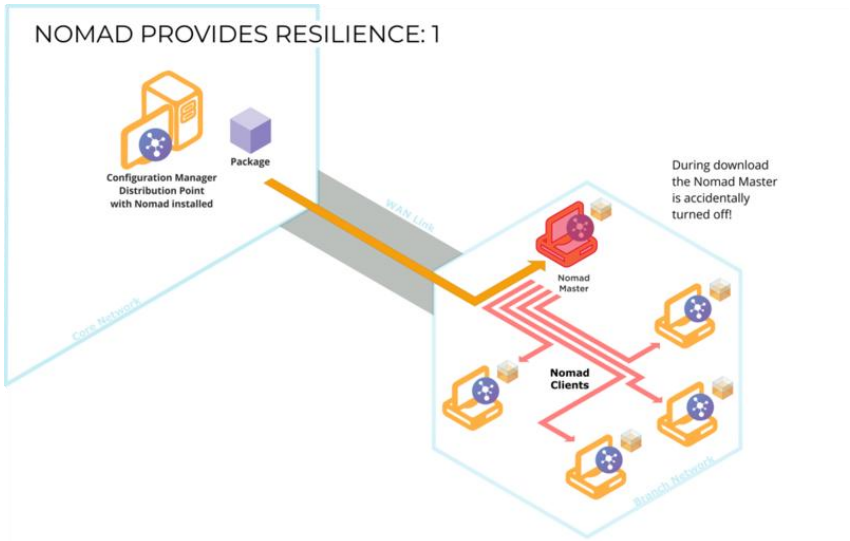
The Nomad clients with local copies of the package can themselves act as the master if the need arises. This significantly reduces the number of Configuration Manager servers required to manage a Configuration Manager hierarchy, thereby reducing initial and ongoing maintenance costs.

9.1.3.3.4 Nomad master elections

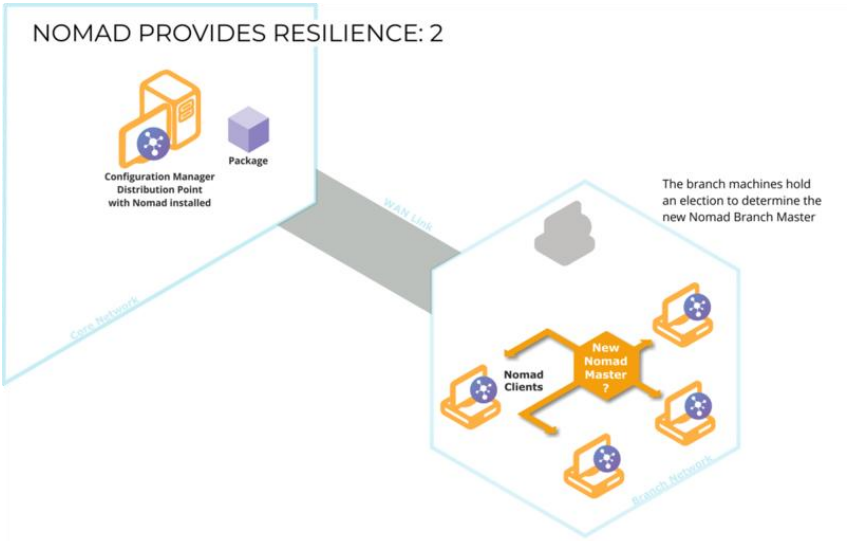
When a software package is deployed to the Nomad clients, an election is held per subnet in the branch to find an appropriate Nomad master, this Nomad master then downloads the software. The software is stored in the Nomad share which is then accessed by the other Nomad clients on the same subnet that require the software package.

Nomad is installed on each computer in the branch and on the distribution point. The computers on the branch network elect a local master. This acts as the single contact point for downloading packages from the distribution point and handles the local redistribution.

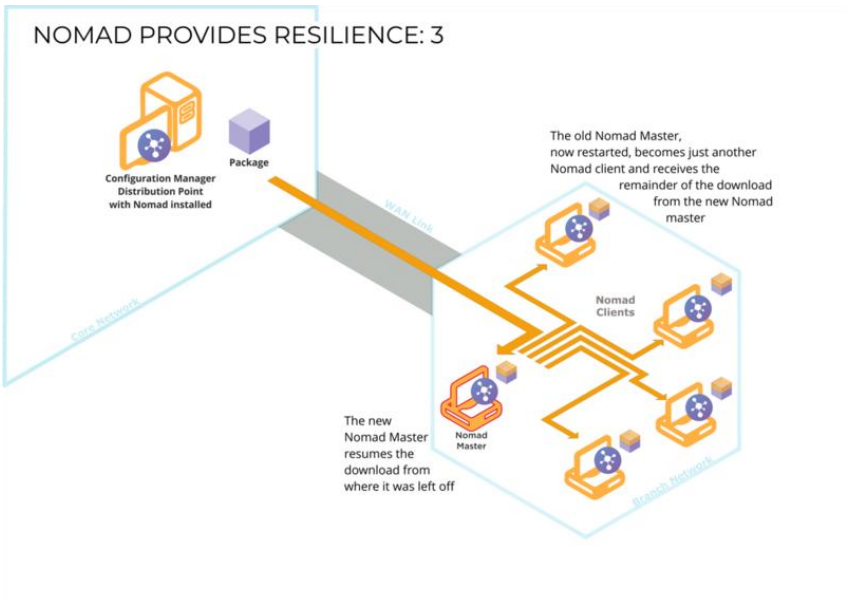
It is possible that a particular Nomad master may be affected in some way during the download. It could be turned off or disconnected from the network for example. If this is the case Nomad ensures that the download continues.



During download, elections continue to be held periodically to determine if the current Nomad master is still the most suitable candidate. If the local Nomad master is affected some way, for example if it is turned off during a download, the other Nomad clients on the branch network interact to elect a new master. The elections are weighted towards the most suitable candidate using a combination of rules.



Once a new master is elected, the download continues to this new master starting from the point at which the download is currently at in that client's cache. The other treat this new master in exactly the same way as the previous master. In fact, if the previous master is turned back on, it may receive the rest of its interrupted download from the new master instead.



See Election rules and master elections for more details about the election process.

9.1.3.4 Download resumption and consistency checking

To minimize repeated downloads of the same content from the Distribution Point, Nomad supports download resumption and consistency checking.

9.1.3.4.1 Download resumption

Nomad downloads include checkpoint recovery, so if the connection to the distribution point is disrupted during a download, it is resumed when the connection is next available. Download resumption starts from the point it had reached when the connection was lost. This means that no previous time spent downloading the package is wasted.

9.1.3.4.1.1

9.1.3.4.2 Consistency checking

Nomad must be installed on all the Configuration Manager DPs. This not only lets central multicast work, but also enables package file checksums to be calculated centrally allowing efficient recovery from file transfer issues if one exists. The central creation of the checksums also minimizes the computational overhead.

Nomad uses manifest files to describe the download contents of Configuration Manager applications and packages. This enables it to provide file-level transfer and, when integrated with Configuration Manager remote differential compression (RDC), file delta downloads. The Nomad client automatically generates a manifest for each version of each package. The generation request occurs as the first Nomad client attempts to download the newest version of a package.

9.1.3.4.3

9.1.3.5 Nomad cache

An overview of the Nomad cache including different methods used by Nomad peers to access the cache on the elected master. The Nomad cache is essential to Nomad's download once to branch feature. The cache enables Nomad to hold its downloaded content so that it can be distributed locally to other Nomad peers. The Nomad cache contains downloaded content (such as packages, applications, and software updates) which can vary in size from relative small patches to rather large OS image files.

9.1.3.5.1 Cache management

The downloaded content in the Nomad cache consume disk space, therefore management of the cache is critical. Because files may be re-used and distributed to other devices on the same subnet or site, the simple solution of deleting the files as soon as they have finished downloading and executing is not sufficient. Instead, Nomad has a cache cleaner utility that automatically but intelligently maintains control over the cache's disk usage.

9.1.3.5.2 Peer copy over HTTP or HTTPS

Nomad peer-to-peer content transfer uses SMB by default, which requires File and Print services to be enabled in order for it to share the content. For better security Nomad can be configured to use HTTP or HTTPS for peer-to-peer content transfer, removing the requirement for file shares. When Nomad is configured to use HTTP/S, if Peer Backup Assistant is enabled it will also use HTTP/S.

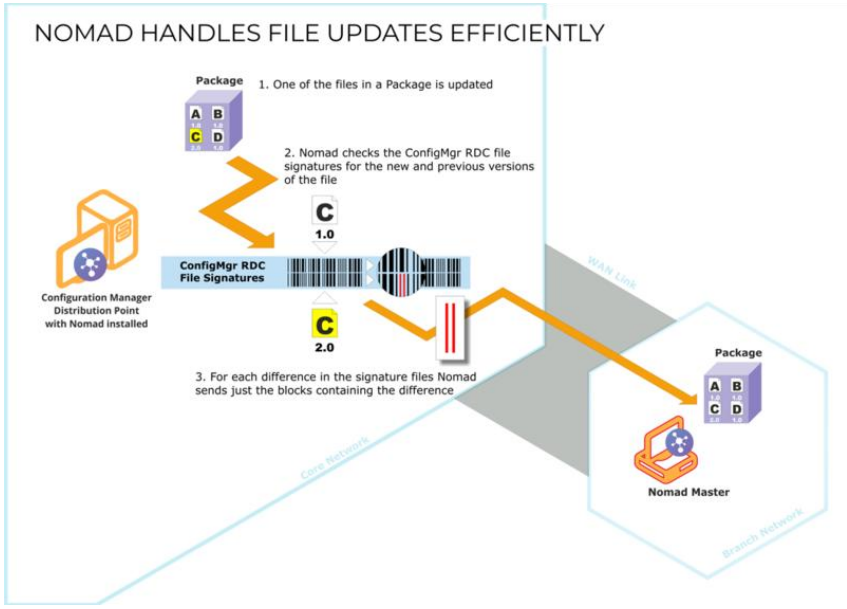
9.1.3.5.3 The Nomad share

The Nomad cache is configured as a share that enables peer-to-peer distribution of downloaded content. Nomad provides control over the accounts that have access to the share and also provides an advanced Nomad FanOut mechanism that can overcome the connection limit to shares on workstations to ensure that content is distributed efficiently and securely.

9.1.3.6 Remote differential compression (RDC) integration

Not only is Nomad aware of the file level differences between different versions of a package so that only changed files are downloaded, it is also aware of the differences within individual files, refer to File-level delta downloads for details.

In our example, a package that has been previously downloaded has one of its files updated. Nomad compares the Configuration Manager RDC signature file (where each block in the file is given a number that identifies it according to its contents) for the new version of the file and the one before it. By identifying the changes, Nomad is able to download just the file blocks containing the differences.



9.1.3.7 Nomad app

The Nomad app provides visibility of content distribution activity and cache status for content distributed by both Nomad and Delivery Optimization. This includes Configuration Manager content distributed with Nomad and Software Updates content distributed with either Nomad or Delivery Optimization.

9.1.3.8 Content Distribution

1E Content Distribution is a Tachyon Consumer, providing control and visibility on content deployments and delivery in an organization.

9.1.3.9 Support for IPv4 and IPv6

Nomad supports IPv4 by default, and optionally supports IPv6, which is commonly required when clients connect to the corporate network using the DirectAccess.

9.1.3.10 App-V support

Nomad supports application virtualization (App-V) applications which are deployed as streamed content by Configuration Manager.

9.1.3.11 FIPS compliant communication encryption

Nomad has always provided encryption for most of its communications and uses an advanced FIPS compliant encryption algorithm. The United States Federal Information Processing Standard (FIPS) http://en.wikipedia.org/wiki/FIPS_140-2 is a standard that defines security requirements for software used by the U.S. federal government. It stipulates that applications that encrypt any sensitive data should use only a certain set of approved encryption algorithms.

9.1.3.12 Nomad Pre-caching

Pre-caching lets you preload the Nomad caches of particular machines directly from the Configuration Manager console. This enables downloads to be available on the branch prior to a deployment taking place, which can be very useful in large-scale deployment scenarios.

9.1.3.13 Nomad FanOut

Windows imposes a limit on the number of concurrent connections on the Nomad share. The FanOut featurecompensates for this limitation by enabling any peer that has more content than the requester to respond to the FanOut request. It is not limited to peers that have an active connection to the master.

9.1.3.14 Single-site download - SSD

Nomad's Single Site Download (SSD) feature ensures a download across the WAN only happens once per site. It does this by maintaining information about which subnets are neighbors of each other (accessible on LAN rather than WAN), so that when an elected master considers a download from a DP rather than a peer in its subnet, it can discover which other local subnets already has the package. These subnets are typically at a single customer site, specifically a single geographical location.

Nomad SSD uses Content Distribution. When a Nomad client downloads a package, it registers this information with Content Distribution, enabling a profile to be created on which Nomad clients hold particular packages.

9.1.3.15 Peer Backup Assistant - PBA

The Peer Backup Assistant (PBA) feature enables files and settings data to be backed-up to a peer device so that they can be maintained when the device is being migrated to a new Operating System. Using PBA, you can avoid the cost of State Migration Point servers to hold the backup

data, as peer devices can be used to provide this storage. The risk of losing user data through the migration process is also greatly reduced in the process.

9.1.3.15.1 Single Site Peer Backup Assistant - SSPBA

Peer Backup Assistant (PBA) enables Nomad clients to use local storage on peers to temporarily store user state data during an OS deployment, removing the need for Configuration Manager State Migration Points. By default, it uses network broadcasts to identify peers with available storage on the local subnet. Single Site Peer Backup Assistant (SSPBA) uses Single Site Download (SSD) features to enable Nomad to use storage available on PBA hosts in adjacent subnets. This enables you to:

Designate appropriate devices to provide the Nomad PBA data store for all devices on the site, not just the local subnet

Avoid the issue where clients on particular subnets do not have sufficient disk space to offer the role of a Nomad PBA data store.

9.1.3.16 Support for Software Updates

9.1.3.16.1 Deploying Office 365 updates

Configuration Manager introduced support for Office 365 agents in Current Branch 1602, and Nomad introduced support in version 6.1.100. This section describes how Office 365 deployments differ in terms of ACP requirements and goes on to describe how Nomad behaves during the download.

9.1.3.16.2 Windows 10 Express Installation Files and Delta Content for Updates

As Windows 10 cumulative updates get very big, very quickly (often in excess of 1GB a few months after any given Feature Upgrade), Microsoft started publishing express installation files for these updates in addition to the traditional full update files. Configuration Manager introduced support for Windows 10 Express Installation File updates in Current Branch 1802 hotfix KB4163547.

Express installation files are a much larger payload on the Distribution Point compared to traditional software update files, but the feature enables clients to download delta byte-ranges from these files, so each month the amount of data a client has to download is typically much smaller. Configuration Manager Current Branch can be configured to support express installation files (refer to https://docs.microsoft.com/en-us/configmgr/sum/deploy-use/manage-express-installation-files-for-windows-10-updates for more details).

With the release of Windows 10 1809, Microsoft replaced express update files with a new way of managing deltas within software updates. In Configuration Manager 1902 the **Enable installation of Express installation files on clients** option in Software Update Client Settings was replaced with **Allow clients to download delta content when available**.

> **Note**
>
> Nomad supports the download of Express installation files and delta content for updates.

9.1.3.16.3 Downloading content for CM Software Updates from Microsoft Update

This feature enables Nomad to download content from Windows Update / Microsoft Update (WUMU). Starting in CB version 1806, software updates can be deployed to devices without first downloading and distributing content to Distribution Points, instead clients download updates directly from the cloud.

9.1.3.17 Integrating Nomad with WakeUp

Nomad integration with WakeUp enables Nomad to share content from its devices that are holding particular content, even if those devices are offline. One reason why peers in the local subnet may not respond to the request even though they have content in their caches is that they are offline (shutdown, in hibernate or sleep mode). However, if WakeUp is integrated, the Nomad client would know which offline device has the content and can wake it up when it queried Content Distribution.

The wake up list is maintained by Content Distribution and is the same list that Single Site Download (SSD) uses. Separate lists of peers are returned for subnet and site. This feature requires Nomad SSD to be enabled, Content Distribution and a NightWatchman infrastructure. The feature is enabled during installation of PreparationNightWatchman Management Center. Please refer to Nomad Preparation for requirements.

9.1.3.18 OS deployment task sequences

Nomad can integrate with OSD strategies to maximize the efficiency of distributing large OS content across the network. It does this by providing a number of Task Sequence steps that can be integrated directly into your OSD Task Sequences.

9.1.3.19 Nomad Download Monitor

The Nomad Download Monitor tool (also known as NomadBranchGUI) is useful for administrators for troubleshooting downloads as they view the status of downloads on local and remote Nomad client devices.

9.1.3.20 Cloud Support

Nomad supports the following Configuration Manager (CM) on Azure scenarios:

Infrastructure as a Service (Iaas) - your host CM infrastructure servers are in Azure virtual machines

Cloud based Distribution Points - CM distribution points are hosted in Microsoft Azure as a cloud service

Cloud Management Gateway (CMG) - CM management points are hosted in the cloud, including support for CMG VM scale sets.

9.1.3.21 Nomad Baseline Wizard

The Nomad Baseline wizard is used to create a Configuration Manager (CM) Baseline from the Configuration Manager console for settings related to Nomad.

9.1.3.22 Nomad Download Pause

Nomad integrates with Tachyon to enable pausing or resuming Nomad downloads throughout the estate. This feature provides a safety measure for situations when a faulty or harmful deployment is made by mistake. In such situations, pausing Nomad downloads on all targeted devices can prevent or limit the potential damage.

It can also be used to facilitate troubleshooting, making it possible to pause all Nomad downloads across the network and enable IT teams to eliminate content distribution from their assessment of network bandwidth usage.

9.2 Implementing Nomad

Everything you need to know about getting Nomad installed and running in your environment. This section is structured in a way that leads you through the three phases of a typical implementation project.

Design, including requirements

Install, including preparation

Verify.

9.2.1 Design Considerations

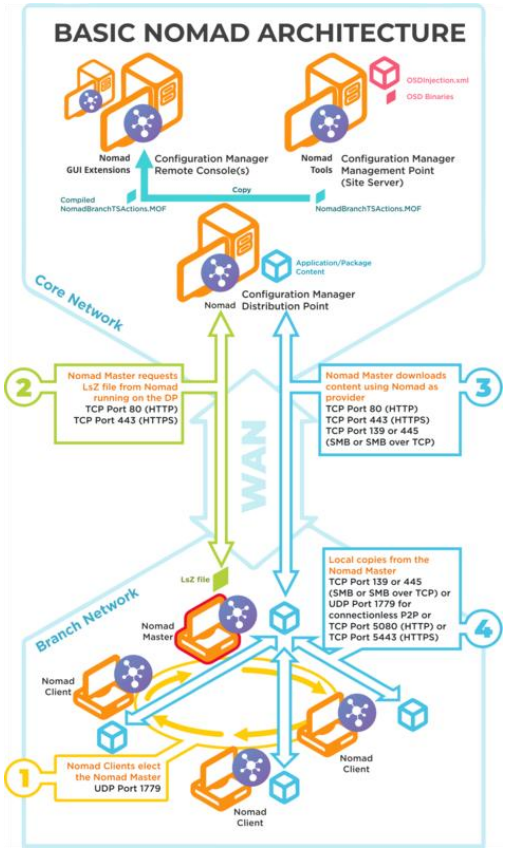
Information that will help you design and plan the implementation of Nomad in your organization.

This page is part of the design phase of implementation.

9.2.1.1 Nomad architecture

The architecture for Nomad. This describes the customer-facing components and how they connect to provide the functionality in Nomad.

> **Note**
>
> For a full description of Tachyon Platform Stacks, their components, the clients and how they connect to provide Tachyon Platform features, refer to Tachyon Architecture.



Ports	Notes
UDP 1779	**Step 1** By default, Nomad uses UDP Port 1779 to communicate during the election process for determining the master on a subnet. The Nomad installer will automatically add *NomadBranch.exe*,*NomadPackageLocator.exe* and *PackageStatusRequest.exe* to the list of excepted programs in the native Windows Firewall. The default value for the port may be changed at install time using the P2PPORT installer property or post-installation by changing the P2P_Port registry value. If you change the default port, you must ensure all Nomad clients communicate using the same port. The Nomad port (by default UPD Port 1779) must be open on all wireless access points to facilitate Nomad peer-to-peer communications. Not all vendors enable this port by default, please refer to the specific device vendor's documentation for details on how to enable ports on each WAP device.
TCP 80 (HTTP)	**Step 2**

Ports	Notes
TCP 443 (HTTPS)	Nomad Master requests LSZ file from Nomad running on the DP.
TCP 80 (HTTP)	**Step 3**
TCP 443 (HTTPS) TCP 139 (SMB) TCP 445 (SMB over TCP)	Nomad Master downloads content using Nomad as provider. This communication depends on how the DP is configured. It may be one of the following: HTTP HTTPS SMB SMB over TCP For Configuration Manager the default setting is HTTP or HTTPS.
TCP 139 (SMB)	**Step 4**
TCP 445 (SMB over TCP) UDP 1779 (used for connectionless P2P) TCP 5080 (HTTP) TCP 5443 (HTTPS)	Local copies from the Nomad master. The recommended way to facilitate Nomad cache access is to enable Windows File and Print Sharing. If this is not feasible on your network environment you can configure Nomad to use different means to access network shares, see Nomad cache for more details on configuring this option. Connections may use one of the following: SMB SMB over TCP Connectionless P2P HTTP HTTPS

9.2.1.2 Installation scenarios

9.2.1.2.1 New installation

Nomad is included with the Tachyon Platform, so you'll need to use the Tachyon setup wizard to install it. To activate Nomad, you'll need a valid license file.

1E will provide you with a **Tachyon.lic** license file that defines the products and features your Tachyon System is able to use, for how long, and how many devices it supports, this may be an evaluation or subscription license.

The license must be activated. Once activated, it may be used only by the Tachyon System that activated it.

Licenses can be renewed or updated, but if allowed to expire, then the affected products or features will not be usable.

For a new installation, the Tachyon Setup program will let you select the license file from any folder on disk.

For an existing installation, the license file is copied into the folder: %PROGRAMDATA%\1E\Licensing on your Tachyon Server.

For details of what the license file needs to contain, please refer to License requirements for consumer applications.

Before installing the Tachyon Platform, please refer to Installing Tachyon, this includes details of server sizing. The addition of Nomad does not affect sizing, as it is included with the Tachyon Platform.

9.2.1.2.2 Existing Nomad installation

If you already have Nomad configured in your environment, you can install Nomad as a local consumer application on your existing Tachyon web server, if it is Tachyon Platform 8.1

Please refer to Upgrading Nomad for guidance on:

Upgrading to the latest version of Nomad within a Configuration Manager operating environment

Additional guidance on upgrading ActiveEfficiency to Content Distribution

Upgrading Configuration Manager when Nomad is in use.

9.2.1.3 Infrastructure dependencies

9.2.1.3.1 Tachyon platform

Although not a requirement for generally using Nomad, the Tachyon Platform must be installed and available before you can use certain features.

The following features use Content Distribution and require Tachyon platform and platform features of Nomad to be enabled:

Nomad app provides visibility of content distribution activity.

Single Site Download (SSD) (SSD).

Single Site Peer Backup Assistant - SSPBA (SSPBA).

High Availability PBA (HAPBA) (HAPBA).

Get Migration Settings task sequence action used to manage computer associations.

Nomad Pre-caching.

Nomad Download Pause.

Note

Nomad versions prior to Nomad 7.1 used ActiveEfficiency to support similar features. Tachyon platform previously included ActiveEfficiency.

The following features were provided in versions older than Nomad 7.1

1E Client Health - now provided by the Guaranteed State feature of the platform.

Nomad Dashboard - now provided by Nomad app feature of the platform.

For everything you need to know about getting the platform installed and running in your network, please refer to Planning for Tachyon.

These features require the full deployment of the platform infrastructure, including Master and Response Stacks, with an optional DMZ Server for Internet-based clients.

Tachyon platform is installed using Tachyon setup, which should also be used to install the following components, included in the Tachyon platform download zip.

Nomad app - this consumer application replaces the legacy Nomad Dashboard.

Content Distribution - this web service is required by the Nomad app, and replaces the legacy ActiveEfficiency Server.

Please refer to:

Requirements for prerequisites.

Introducing Tachyon for details about the Tachyon platform and other optional applications and features.

9.2.1.3.2 Implementing a Tachyon Platform DMZ server

If you have internet-based clients you will need a Tachyon Platform DMZ Server to support your Internet-facing Tachyon clients. The DMZ Server is a type of Response Stack used to provide Tachyon Real-time and Inventory services to Internet-based clients. For details about installing a Tachyon DMZ Server to support Internet-facing Tachyon clients refer to Implementing a Tachyon DMZ Server.

9.2.1.3.3 Tachyon client integration with Nomad

When Tachyon and Nomad clients are both enabled in the 1E Client, then the clients and Tachyon instructions will - by default - automatically use Nomad to download content. Tachyon client uses Nomad to download content from the Tachyon Background Channel, or from any website, without any dependency on Configuration Manager.

For more information, from a Tachyon perspective, please refer to Downloading client content and Nomad integration.

9.2.1.4 Nomad components

To understand what Nomad can do for you, please refer to Nomad overview and Nomad fundamentals. Once you have decided what features you will use, then you will need to deploy relevant components to clients and servers.

In addition to the **Nomad app** and **Content Distribution** components described above, the following sections provide a brief overview of Nomad components:

1E Client

Configuration Manager Console extensions

Configuration Manager OSD Tools

Download Monitor tool.

9.2.1.4.1 1E Client

The Nomad client is the core component of Nomad and can be used on its own without any other components.

Nomad client is part of the 1E Client and is only supported on Windows devices. You must deploy the 1E Client (with Nomad enabled) to:

In-scope client devices - use 1E Client Deployment Assistant 8.1 (CDA) to help deploy 1E Client via Configuration Manager

Configuration Manager Distribution Points - use the installer transform file created by CDA edited as required to suit the type of DP, ensuring LSZ Generation is enabled (enabled by default in SpecialNetShare).

The 1E Client also includes the following clients that must be enabled to support optional Nomad features:

Tachyon client - provides real-time features required by the Download Pause feature

Shopping/WSA client - provides Windows Servicing Assistant (WSA) features

PXE Everywhere Agent - allows computers to automatically boot up into Windows PE, which then allows a Windows Operating System to be installed.

Please refer to:

Deployment and configuration options for an overview of Nomad configuration and deployment options

Requirements for prerequisites

Deploying the Nomad client using Configuration Manager for detailed steps

Introducing 1E Client for details about 1E Client and other optional client modules (Tachyon, Shopping/WSA, PXE Everywhere, WakeUp).

9.2.1.4.2 Configuration Manager Console extensions

The extensions must be installed on all computers where Configuration Manager administrators use their CM Admin Console to :

edit OSD Task Sequences

configure Nomad content download settings for applications, packages, software updates

use the Nomad Download Pause feature

use the Nomad Baseline wizard feature.

Please refer to:

Requirements for prerequisites.

9.2.1.4.3 Configuration Manager OSD Tools

The Configuration Manager OSD Tools (also known a NomadBranch Tools) must be installed on all Site Servers (except Secondary) and all SMS Provider servers. Specifically servers which Configuration Manager Consoles may connect to.

The installer copies the Nomad binaries to the ConfigMgr site installation folder .\OSD\bin\<Architecture> on the SMS Provider server. This enables the files to be injected into the OSD boot image allowing Nomad to be used during the WinPE deployment phase. The installer will also extend the Configuration Manager Site WMI namespace to include definitions of the 1E Nomad built-in task sequence steps.

Please refer to:

Requirements for prerequisites

9.2.1.4.4 Download Monitor tool

Also known as NomadBranch GUI, the Nomad Download Monitor tool is optionally installed on client devices alongside the Nomad client, and is used for troubleshooting and testing only. It should not be installed generally in your network.

9.2.1.5 Client deployment and common configuration settings

9.2.1.5.1 1E Client Deployment Assistant (CDA)

The **1E Client Deployment Assistant (CDA)** is the recommended method of deploying 1E Client to Windows computers if you have Microsoft System Center Configuration Manager, and also for deploying 1E NightWatchman Agent. 1E Client may be deployed independently using alternative software distribution methods.

The CDA creates Packages, Applications, empty Collections and Deployments with custom Windows Installer transforms to simplify the installation and initial configuration of the 1E Client and its modules. You can then simply add devices into the Collections to upgrade Nomad on those devices.

> **Note**
>
> The wizard allows you to configure commonly used settings. The template **.mst** contains many additional installer properties, but not all of them. You should review your requirements and decide which installer properties to modify or add. The full list is available in Nomad installer properties.
>
> Some less common settings are described in more detail further below.

Connection to a Configuration Manager site is required even if you only want to use the CDA wizard to create the MST transform files. The site must have software distribution features enabled.

> **Tip**

CDA helps create everything you need to deploy clients and agents in your Configuration Manager environment. If you prefer, you can use CDA in a lab or other environment to create the Configuration Manager application and/or package content (including MST transform files). Then you can copy the content to your production environment and manually create your deployments.

If you don't want CDA to create objects in Configuration Manager then you can use Microsoft's Orca to edit the base MST transform files supplied with CDA, and manually create your deployments.

Orca is a Microsoft tool for creating and editing Windows Installer packages (MSI) and merging modules (MST transforms). It is available from the Windows Installer Development Tools - https://docs.microsoft.com/en-us/windows/desktop/msi/orca-exe.

Nomad OSD tools and Nomad Configuration Manager Console extensions are both available in the **NomadBranchTools.msi** installer. The installer will automatically choose which components to install based on the server where the installer is running. For Configuration Manager sites and SMS Providers the Nomad OSD tools will be installed and if the Configuration Manager Console is present the Nomad Configuration Manager Console extensions will be installed.

So, in addition to deploying 1E Client (with Nomad client module enabled) on all computers and on Configuration Manager Distribution Points, the following locations require the **NomadBranchTools.msi** to be run:

Configuration Manager sites and SMS Providers.

Configuration Manager site servers, any other computer that has the Configuration Manager Console installed.

Note

For full documentation on the 1E Client Deployment Assistant, refer to Introducing 1E Client Deployment Assistant including:

Preparation.

Running the wizard - where you configure commonly used settings.

Configuration Manager objects.

Supported platforms.

Installer properties.

9.2.1.5.2 Nomad client settings

Nomad client installer properties are associated with each area of functionality in Nomad, and are mostly configured in the registry, it's only the enabling of Nomad and Tachyon that's completed in the 1E Client configuration file.

They can be specified during installation of the 1E Client as Windows installer properties, and must be specified in upper-case. Settings that exist in the 1E Client configuration file can be mixed-case, and can be reconfigured after installation using 1E Client command-line parameters.

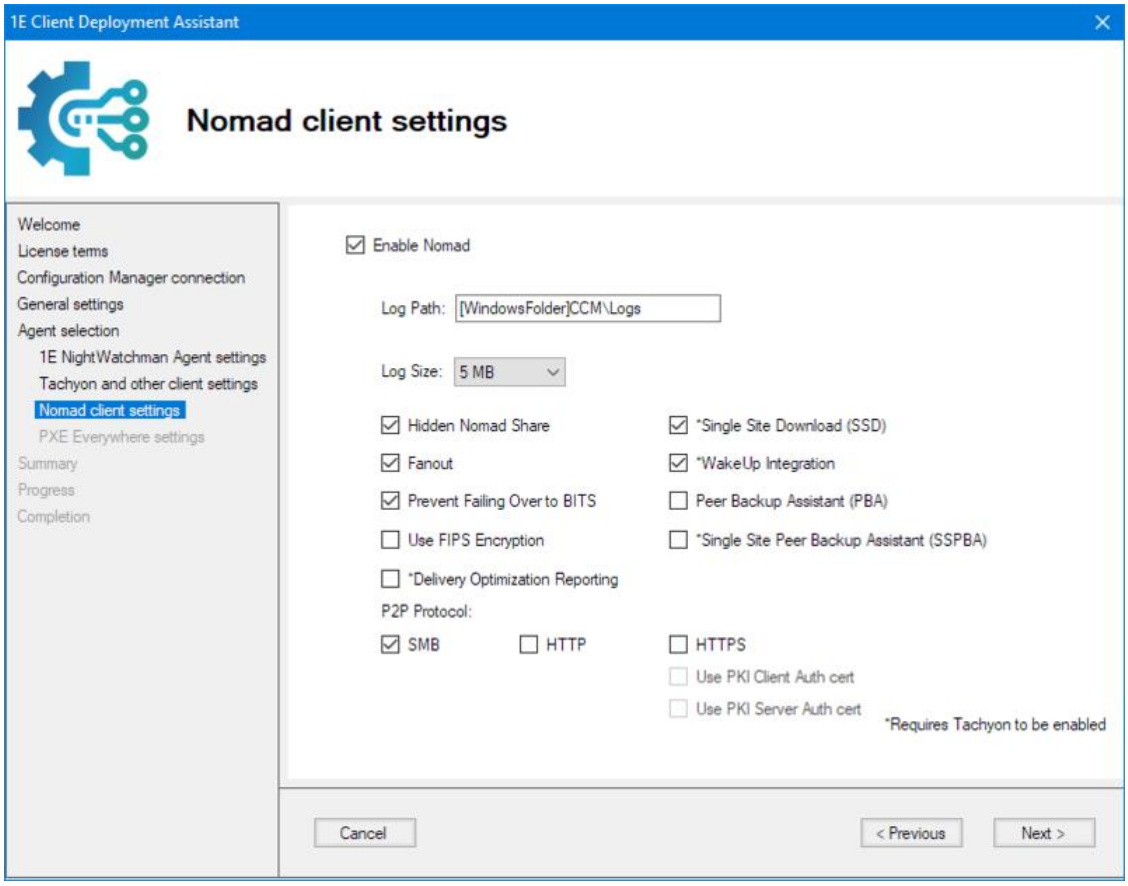
Note

For a full list of the 1E Client installer properties available for the Nomad client module refer to Nomad client alphabetic installer properties.

9.2.1.5.3 Common configuration settings

These are settings that most frequently vary between organizations, and are therefore presented as options in CDA.

9.2.1.5.3.1 Nomad client settings in CDA



9.2.1.5.3.2 Nomad client settings in 1E Client installer

9.2.1.5.3.3

Each of the following features is optional. Although not a requirement for generally using Nomad, Introducing Tachyon must be installed and available before you can use certain Nomad features.

Nomad feature	Description	Installer properties	Infrastructure requirement
Hidden Nomad Share	The Nomad cache is configured as a share that enables peer-to-peer distribution of downloaded content. Nomad provides control over the accounts that have access to the share and also provides an advanced Nomad FanOut mechanism that can overcome the connection limit to shares on workstations to ensure that content is distributed efficiently and securely.	MODULE.NOMAD.SPECIALNETSHARE	Nomad Administration Tools Microsoft System Center Configuration Manager
Single Site Download (SSD)	Nomad's Single Site Download (SSD) feature ensures a download across the WAN only happens once per site. It does this by maintaining information about which subnets are neighbors of each other (accessible on LAN rather than WAN), so that when an elected master considers a download from a DP rather than a peer in its subnet, it can discover which other local subnets already has the package. These subnets are typically at a single customer site, specifically a single geographical location. Nomad SSD uses Content Distribution. When a Nomad client downloads a package, it registers this	MODULE.NOMAD.SSDENABLED MODULE.NOMAD.CONTENTREGISTRATION	Introducing Tachyon Nomad Administration Tools Microsoft System Center Configuration Manager

Nomad feature	Description	Installer properties	Infrastructure requirement
	information with Content Distribution, enabling a profile to be created on which Nomad clients hold particular packages. **Note** When SSD is enabled in the CDA wizard, then Content registration is also enabled.		
FanOut	Windows imposes a limit on the number of concurrent connections on the Nomad share. The FanOut featurecompensates for this limitation by enabling any peer that has more content than the requester to respond to the FanOut request. It is not limited to peers that have an active connection to the master.	MODULE.NOMAD.SPECIALNETSHARE	Nomad Administration Tools Microsoft System Center Configuration Manager
Peer Backup Assistant (PBA)	The Peer Backup Assistant (PBA) feature enables files and settings data to be backed-up to a peer computer so that they can be maintained when the computer is being migrated to a new Operating System. Using PBA, you can avoid the cost of State Migration Point servers to hold the backup data, as peer computers can be used to	MODULE.NOMAD.SSPBAENABLED	Nomad Administration Tools Microsoft System Center Configuration Manager

Nomad feature	Description	Installer properties	Infrastructure requirement
	provide this storage. The risk of losing user data through the migration process is also greatly reduced in the process.		
Prevent Failing Over to BITS	If Nomad generates a return code that is not in the list, it passes a fail to the CTM component which causes the Configuration Manager client to try downloading the content itself using BITS, or use another Alternate Content Provider (ACP). This process may itself succeed or fail depending on the conditions that resulted in the original Nomad return code, and may have an undesirable impact on the network. **Note** The special code 0x9999 can be added to the list, or used on its own, to cause Nomad to always return a success to CTM. As a consequence this code is also known as "prevent failover to BITS".	MODULE.NOMAD.SUCCESSCODES	Nomad Administration Tools Microsoft System Center Configuration Manager
Single Site Peer	SSPBA can be enabled at install time using the	MODULE.NOMAD.SSPBAENABLED	Introducing Tachyon

Nomad feature	Description	Installer properties	Infrastructure requirement
Backup Assistant (SSPBA)	MODULE.NOMAD.SSPBAENABLED installer property. Post-installation SSPBA can be enabled by setting the following registry values: Update the SSPBAEnabled registry value to 1. Update the SSDEnabled registry value to 0x3 to enable Content Distribution integration required for this feature to work. When SSPBA is enabled, PBA will initially attempt to find suitable PBA data stores on the local subnet. If it does not find one, it will send the request to neighboring subnets using the information held in Content Distribution.		Nomad Administration Tools Microsoft System Center Configuration Manager
Use FIPS Encryption	FIPS encrypts the following types of Nomad data: Data sent over a network in peer-to-peer communications, including: Election communications Connectionless data transfer Nomad FanOut requests Sign-on/sign-off communication	MODULE.NOMAD.USEFIPS	Nomad Administration Tools Microsoft System Center Configuration Manager

Nomad feature	Description	Installer properties	Infrastructure requirement
	SSD Package Status Requests PBA communications.		
Delivery Optimization Reporting	Monitor and report on Delivery Optimization (DO) downloads. This feature is only supported in full versions (OS with UI) of Windows Server 2016 and Windows 10 Version 1909 onwards.		
P2P Protocol SMB HTTP HTTP(S)	If you are installing Nomad for the first time, consider how your peers are going to communicate for content transfer. You will need to make sure your clients are configured to use the same protocol. Depending on whether you use either SMB, HTTP or HTTP/S the configuration steps will be slightly different, for example if you decide to use a PKI certificate for server or client authentication HTTP/S. Nomad peer-to-peer content transfer uses SMB by default, which requires File and Print services to be enabled in order for it to share the content. For better security Nomad can be configured to use HTTP	MODULE.NOMAD.P2PENABLED	Nomad Administration Tools Microsoft System Center Configuration Manager

Nomad feature	Description	Installer properties	Infrastructure requirement
	or HTTPS for peer-to-peer content transfer, removing the requirement for file shares. When Nomad is configured to use HTTP/S, if Peer Backup Assistant is enabled it will also use HTTP/S. Refer to Peer copy over HTTP or HTTPS for more information, including: Enabling HTTP/HTTPS Authentication Certificate Selection Firewall exceptions Windows PE support Configuring use of PKI-issued certificates post-installation.		

9.2.1.6 Other configuration settings

In general, the default values using in the CDA template .mst file will suit most organizations, however you should consider the following to ensure you have the optimum configuration for your organization.

9.2.1.6.1 Maximizing download speed for high-bandwidth links using Dynamic Block Sizes

The Dynamic Block Size (DBS) feature increases block size on high-bandwidth links to get maximum efficiency, and reduces it on low-bandwidth links to reduce the impact. Using DBS, Nomad is able to automatically decide the appropriate block size for a given link bandwidth and also adjust it as needed during the download if the link conditions change. As a result, Nomad is far more efficient and faster on all types of connection bandwidths while retaining its minimal impact on other link traffic.

Note

DBS is enabled or disabled by configuring Bit 25 in the CompatibilityFlags registry. Setting Bit 25 disables DBS and clearing Bit 25 enables DBS.

In Nomad 7.0 onwards, the DBS feature is turned off by default for new installations, and not changed for upgrades.

Prior to v6.3 the default value of BlockSize registry setting was 32KB (0x8000). From v6.3 onwards the default is 128KB (0x20000).

The installer automatically sets this to 128KB for both fresh installs and upgrades from previous versions. The only exceptions to this are:

It will use the specified value if the BLOCKSIZE property is used in the installation command line or in a MST transform, when doing a fresh install or upgrade

It will retain the previous value of BLOCKSIZE if it was set to anything other than 32KB (the older default), when doing an upgrade.

Note

For more information click here to expand...

The following is a duplicate of the BlockSize page.

Value (in bytes) for the minimum size of each block of data Nomad copies from the package source folder.

Note

Any change to this value requires a manual service restart before it can take effect.

Registry value	Default value	Notes	Installer property
BlockSize	131072(128KB)	Must be between 4096(4KB) to 4194304(4MB) inclusive. The default block size is 128KB The maximum block size is 4MB Multicast environments can only use the	MODULE.NOMAD.BLOCKSIZE

Registry value	Default value	Notes	Installer property
		default block size. If you define a larger value for multicast environments, Nomad automatically resets it to the default. Clients use the block size defined in the registry and ignore the values from the LSZ	

The Dynamic Block Size (DBS) feature increases block size on high-bandwidth links to get maximum efficiency, and reduces it on low-bandwidth links to reduce the impact. Using DBS, Nomad is able to automatically decide the appropriate block size for a given link bandwidth and also adjust it as needed during the download if the link conditions change. As a result, Nomad is far more efficient and faster on all types of connection bandwidths while retaining its minimal impact on other link traffic.

Note

DBS is enabled or disabled by configuring Bit 25 in the CompatibilityFlags registry. Setting Bit 25 disables DBS and clearing Bit 25 enables DBS.

In Nomad 7.0 onwards, the DBS feature is turned off by default for new installations, and not changed for upgrades.

Prior to v6.3 the default value of BlockSize registry setting was 32KB (0x8000). From v6.3 onwards the default is 128KB (0x20000).

The installer automatically sets this to 128KB for both fresh installs and upgrades from previous versions. The only exceptions to this are:

It will use the specified value if the BLOCKSIZE property is used in the installation command line or in a MST transform, when doing a fresh install or upgrade

It will retain the previous value of BLOCKSIZE if it was set to anything other than 32KB (the older default), when doing an upgrade.

9.2.1.6.2 Managing stable LAN connections

Nomad provides extra stability by managing a machine's network connections as they move between a wireless and a wired LAN. Depending on the OS version or other factors, once an SMB or HTTP session is running on a wireless connection, it will remain on wireless even when a wired LAN becomes available. Nomad uses **WLanBlipSecs** to temporarily drop a wireless connection when it detects a wired LAN connection, to give time for the OS and Nomad to automatically switch to the LAN connection.

For example, if a Nomad master was initiated when a machine was on a wireless connection and a wired connection subsequently became available, Nomad disables the wireless adapter for a long enough period to enable a switchover to the wired connection. As a result of this, the IP address and the share path will change and peers will log error messages until each peer re-establishes its connection to the master and the new share location.

This feature is turned off by default.

> **Note**
>
> Other applications may be affected when switching from wireless to wired connection.

Irrespective of the **WLanBlipSecs** setting, you can also control which service set identifier (SSID) Nomad connects to by managing a list. To do this, update the NomadBranch WLanProfileList registry value with a comma-delimited list of SSIDs or use the wildcard (*) character for any SSID.

> **Note**
>
> For more information click here to expand...
>
> The following is a duplicate of the WLanBlipSecs page.
>
> The duration for temporarily disabling a wireless connection when a wired LAN connection becomes available, to provide time for the OS and Nomad to switch to the LAN connection. This is useful for OS versions and drivers that do not automatically switch to a preferred wired connection.
>
> | Registry value | Default value | Notes | Installer property |
> |---|---|---|---|
> | WLanBlipSecs | 0 | The value must be 20 seconds or more. | MODULE.NOMAD.WLANBLIPSECS |
>
> Nomad provides extra stability by managing a machine's network connections as they move between a wireless and a wired LAN. Depending on the OS version or other factors, once an SMB or HTTP session is running on a wireless connection, it will remain

on wireless even when a wired LAN becomes available. Nomad uses **WLanBlipSecs** to temporarily drop a wireless connection when it detects a wired LAN connection, to give time for the OS and Nomad to automatically switch to the LAN connection.

For example, if a Nomad master was initiated when a machine was on a wireless connection and a wired connection subsequently became available, Nomad disables the wireless adapter for a long enough period to enable a switchover to the wired connection. As a result of this, the IP address and the share path will change and peers will log error messages until each peer re-establishes its connection to the master and the new share location.

This feature is turned off by default.

Note

Other applications may be affected when switching from wireless to wired connection.

Irrespective of the **WLanBlipSecs** setting, you can also control which service set identifier (SSID) Nomad connects to by managing a list. To do this, update the NomadBranch WLanProfileList registry value with a comma-delimited list of SSIDs or use the wildcard (*) character for any SSID.

Examples:

```
WLanProfileList REG_SZ WIFIGAP,GUEST
WLanProfileList REG_SZ *
```

9.2.1.6.3 Setting intra-day work rates

Nomad allows hourly variable work rates to be set throughout the day enabling organizations to use different maximum percentage of available bandwidth during the working day and in the evenings. Intra-day work rates are set on the client using the *MaxWorkRates*registry value. If the intra-day work rate is less than that defined on the command-line, it will override the command-line value. If the intra-day work rate is higher than that defined on command-line, the command-line value is used in preference.

Note

Work rates only apply to transfers from a DP not to P2P transfers within a LAN.

Note

For more information click here to expand...

The following is a duplicate of the MaxWorkRates page.

MaxWorkRates is a registry key, that must be created, to hold registry values for each day of the week (Day0 to Day6) where the hourly maximums for the variable work rates are set.

Registry values	Default value	Notes	Installer property
MaxWorkRates\Day#		Hourly variable workmates can be set throughout the day. The days of the week are labelled: **Day0** to **Day6** where **Day0** = Sunday, **Day1** = Monday etc. Each day value is REG_SZ string set as a comma separated list of 24 hourly work rates for that day. Each value can be set from 1-100. The following is an example for setting for the Day# values where on Sunday, a maximum work rate of 20% will be used. On	None.

Registry values	Default value	Notes	Installer property
		Monday, the max work rate between 0:00-05:59 is 80%, between 06:00-17:59 is 20% and between 18:00-23:59 is it 80% again. For the rest of the week, the work rate specified on the command-line is used. If neither work rate is specified, the default is 80%.	

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\1E\NomadBranch\MaxWorkRates]
"Day0"="20,20,20,20,20,20,20,20,20,20,20,20,20,20,20,20,20,20,20,20,20,20,20,20"
"Day1"="80,80,80,80,80,80,20,20,20,20,20,20,20,20,20,20,20,20,80,80,80,80,80,80"
```

Registry values	Default value	Notes	Installer property
		"Day2"="" "Day3"="" "Day4"="" "Day5"="" "Day6"=""	

Nomad allows hourly variable work rates to be set throughout the day enabling organizations to use different maximum percentage of available bandwidth during the working day and in the evenings. Intra-day work rates are set on the client using the *MaxWorkRates* registry value. If the intra-day work rate is less than that defined on the command-line, it will override the command-line value. If the intra-day work rate is higher than that defined on command-line, the command-line value is used in preference.

Note

Work rates only apply to transfers from a DP not to P2P transfers within a LAN.

Work rate override arguments

The intra-day work rates can be overridden using the --wro and --wr Nomad command-line arguments.

If these two arguments are combined, the value for the --wr switch is used in preference to the intra-day work rate set in the registry

If only the --wro argument is used, any intra-day value is overridden with a default maximum of 80%

If using intra-day work rates and the --wr argument only, the lower of the two values is used.

9.2.1.6.4 Inhibiting subnets and sites

You can define subnets and AD sites where machines will download from the DP (these machines will not relay download status messages) and not participate in Nomad elections. This feature only supports IPv4 subnets and is useful for sites that have a:

Local DP

VPN without isolation. Typically, VPN solutions isolate each client using single-node subnets (i.e. each client is in its own subnet with a 32-bit subnet mask) to prevent broadcast traffic between VPN clients that are typically geographically dispersed and not on the same local network. If the VPN solution is not configured in this manner and clients get an IP address with a subnet mask less than 32 bits, broadcasts can be exchanged between the VPN clients enabling Nomad to elect a master that is not on the same local network.

The Nomad additional setting *++pr* will not override the download priority.

The Nomad NomadInhibitedSubnets or NomadInhibitedADSites registry values can be set with a comma separated list of sites or subnets in which Nomad functionality should be inhibited. If the client machine exists

in either an inhibited subnet or an inhibited site, peer functionality is disabled, the agent will not participate in elections and will download from the DP.

9.2.1.6.4.1 Inhibit files and formats

You can append the inhibited subnet and AD site lists with content from text files to make it easier to manage if there are many sites and subnets to be defined. Inhibited sites or subnets are defined in text files with a *.inh* extension and must reside in the *%INSTALLDIR%\Inhibits* directory.

Each file should contain a list of the inhibited subnets in a classless inter-domain routing (CIDR) format, or a list of inhibited AD sites. Each site or subnet must be on a separate line or be separated by commas. For example, the following defines two subnets and one AD site to be inhibited:

```
192.168.0.0/24, 192.168.1.0/24
ACMEDOM1
```

When the Nomad service starts or is reset, any .inh files in the Nomad *%INSTALLDIR%\Inhibits* directory are read in. Both the registry values and the contents of these files are used together to determine the list of inhibited subnets and sites.

A service reset occurs when the Nomad registry is updated or there is a change of subnet. So, if a laptop moves to another subnet half way through a download, the Nomad service will reset and check the current subnet against its list of inhibited subnets. If the check determines that the new subnet is an inhibited subnet, Nomad's peer-to-peer functionality is disabled – the service stops downloading from the peer and will instead download from the local DP.

9.2.1.6.5 Support for IPv4 and IPv6

Nomad supports IPv4 by default, and optionally supports IPv6, which is commonly required when clients connect to the corporate network using the DirectAccess.To configure support for IPv4 and/or IPv6, update the Nomad SpecialNetShare registry value:

Bit 1 - 0x0002 - Enable IPv6

Bit 2 - 0x0004 - Disable IPv4

9.2.2 Requirements

A checklist of typical infrastructure prerequisites and dependencies to install Nomad.

This page is part of the design phase of implementation.

Review Design Considerations first if you need to design and plan the implementation of Nomad in your organization.

9.2.2.1 Installation account permissions

Installer	Rights required
Nomad client is now part of the 1E Client. Please refer to Introducing 1E Client for details of how to deploy the 1E Client with the Nomad client enabled.	Local Administrator to install.

Installer	Rights required
The 1E Client should be installed on all Windows clients. You must use the correct installer file according to the Windows architecture of the device: **1E.Client-x64.msi** is for 64-bit architectures **1E.Client-x86.msi** is for 32-bit architectures You must also deploy the 1E Client (with Nomad enabled) to Configuration Manager Distribution Points.	
Download GUI tool installer for optional installation on clients: **NomadBranchGui.msi.** **Note** This is a troubleshooting, testing, and administrative tool only. It should not be installed generally on devices in your network.	Local Administrator to install.
ConfigMgr console extensions: **NomadBranchAdminUIExt.msi** ConfigMgr administrators use console extensions to configure Nomad content download, custom task sequence steps and Nomad Download Pause features. **Note** The installer should be run on all Windows workstations and servers that have Configuration Manager Console installed, including Site servers.	Local Administrator to install.
ConfigMgr OSD Tools: **NomadBranchTools.msi** The installer copies the Nomad binaries to the ConfigMgr site installation folder .\OSD\bin\<Architecture> on the SMS Provider server. This enables the files to be injected into the OSD boot image, allowing Nomad to be used during the WinPE deployment phase. The installer will also extend the ConfigMgr site WMI namespace to include definitions of the 1E Nomad built in task sequence steps. **Note** The installer must be run on all Site Servers (except Secondary) and all SMS Provider servers. Specifically, servers which Configuration Manager Consoles may connect to.	Local Administrator to install.

9.2.2.2 Server requirements

9.2.2.2.1 Tachyon Platform

Although not a requirement for generally using Nomad, the Tachyon Platform must be installed and available before you can use certain features.

The following features use Content Distribution and require Tachyon platform and platform features of Nomad to be enabled:

Nomad app provides visibility of content distribution activity.

Single Site Download (SSD) (SSD).

Single Site Peer Backup Assistant - SSPBA (SSPBA).

High Availability PBA (HAPBA) (HAPBA).

Get Migration Settings task sequence action used to manage computer associations.

Nomad Pre-caching.

Nomad Download Pause.

> **Note**
>
> Nomad versions prior to Nomad 7.1 used ActiveEfficiency to support similar features. Tachyon platform previously included ActiveEfficiency.

The following features were provided in versions older than Nomad 7.1

1E Client Health - now provided by the Guaranteed State feature of the platform.

Nomad Dashboard - now provided by Nomad app feature of the platform.

For everything you need to know about getting the platform installed and running in your network, please refer to Planning for Tachyon.

9.2.2.2.2 Nomad Administration Tools

Please refer to Supported Platforms - Nomad Administration Tools for a list of all the platforms supported by Nomad, and the software required to allow Nomad to be installed or to work.

9.2.2.3 Client requirements

9.2.2.3.1 1E Client

Please refer to Supported Platforms - Nomad client for a list of all the platforms supported by Nomad, and the software required to allow Nomad to be installed or to work.

9.2.3 Preparation

What you will need to prepare in advance of implementing Nomad in your network. Typically, these are tasks that may take some time, depending on how your organization works. A more complete checklist of tasks is provided in Requirements.

9.2.3.1 Nomad preinstallation checks

If you are upgrading, please refer to Upgrading Nomad. You must upgrade in the following order to avoid potential forward compatibility issues:

Upgrade all site servers and Distribution Points first. Old and new clients can then be sure to connect to the latest version on servers

Upgrade all Nomad clients running on a single subnet at the same time. This avoids potential issues with older clients attempting to peer connect with new clients on the same subnet, even if the client configuration remains the same.

Ensure DNS is working properly

Ensure client side firewalls have exceptions in place for *NomadBranch.exe*, *NomadPackageLocator.exe* and *PackageStatusRequest.exe*

Ensure local broadcasts are enabled on each subnet that Nomad operates in

> **Note**
>
> Some wireless access points may be configured to prevent broadcasts, which will prevent Nomad peer-sharing features from working. See the Wireless Access Points prerequisite for details on WAP configuration.

Ensure the Configuration Manager client is healthy and functioning properly

The latest version of Tachyon Platform should be installed to support certain features, please refer to the Tachyon Platform section

If you want **Nomad integration with WakeUp** then you will need the following:

Tachyon Platform

The Nomad app must be installed on the latest version of Tachyon Platform, and the single-site download feature enabled as described in Single Site Download.

NightWatchman Management Center with WakeUp Server infrastructure

NightWatchman Management Center 7.0 or later must be installed

> **Note**
>
> During installation, you must tick the **Enable ActiveEfficiency** checkbox on the **1E ActiveEfficiency** server screen, and enter the base FQDN:port of the Tachyon server that hosts the Content Distribution service. For example: tachyon.acme.local:443

WakeUp Server 7.0 or later must be installed

1E Client 7.0 or later (with the WakeUp component enabled and reporting turned on) must be deployed to all the clients on the required subnets.

> **Note**
>
> You will need a valid NightWatchman Enterprise license to use these components.

On Nomad peers:

Content Registration must be enabled on all machines where the WakeUp feature is to be used.

On Nomad devices requesting the download:

Enable the 1E Client WakeUp component

Enable Single Site Download if you require site-wide wake-up.

On the devices where you use wake-up:

The BIOS on each client must be configured to support wake from off

The network adapter on each client must be configured to support wake from sleep (1E Services can help configure this using vendor utilities and scripts).

To support enhanced package consistency checking, the Nomad client must be installed on each Configuration Manager DP. This client enables file-level consistency checking by creating a manifest file on the DP for every version of each package created, enabling Nomad to verify that each file it downloads is consistent with the version available on the DP.

> **Note**
>
> LSZ generation using HTTP/HTTPS is automatically configured only on DPs that are also Site servers. For standalone DPs (those not on a site server), enable the following on the Nomad client running on the DP either during installation or by updating the Nomad registry:

Installer property	Registry value	Description
SIGSFOLDER	SigsFolder	Nomad is able to leverage Configuration Manager's binary differential replication (BDR) if the Windows remote differential compression

Installer property	Registry value	Description
		feature is installed on the DP server using the Windows Server Manager. On the Nomad side, set this registry value on the DP to point to the Configuration Manager RDC signatures folder.
SPECIALNETSHARE	SpecialNetShare	The 0x4000 bit must be set to enable the Nomad client to handle LSZ file generation requests coming from HTTP/HTTPS enabled clients.
PERMITTEDLSZSHARES	PermittedLSZShares	When installed on a standalone DP (not on a site server), ensure that this registry value contains the local share names used on the server (e.g. *SMSPKGF$*; *SMSPKGG$*; etc) to host

Installer property	Registry value	Description
		Configuration Manager packages. The default value satisfies the default locations used by Configuration Manager.

If you are using the **BIOS to UEFI** feature, ensure you meet its prerequisites described in BIOS to UEFI 1.4 - Requirements.

9.2.3.2 Accounts needed to install Nomad

9.2.3.2.1 Tachyon Server Installation Account

The server installation account has the following requirements on the server.

Local admin rights on the Tachyon Server. It must be an Directory domain user account that is a direct or indirect member of the Administrators local group on the server where Tachyon Server will be installed.

Can be disabled (not deleted) in Directory after additional Tachyon admin users have been created in Tachyon, and installation has been verified.

In addition, the server installation account requires SQL rights as described in SQL Databases and SSAS Databases.

The server installation account is granted the following permissions as a Tachyon user, configured during installation of the Tachyon Server.

It is the first Tachyon user account and is a System Principal, which means it cannot be deleted or assigned any other rights

It is assigned to the Tachyon system role of Installer

It should be used to add additional Tachyon users and administrators, assign them to Tachyon roles, which should then be used for ongoing use and management of Tachyon.

It may be included in any AD security group assigned to a Tachyon system or custom role.

Refer to Roles and Securables for a complete reference of Tachyon system roles, custom roles, securables and operations.

9.2.3.3 Tachyon

The following features require Tachyon platform, and Nomad features of 1E Client to be enabled:

Nomad app provides visibility of content distribution activity

Single Site Download (SSD) (SSD)

Peer Backup Assistant - PBA (SSPBA)

High Availability PBA (HAPBA) (HAPBA)

Get Migration Settings task sequence action used to manage computer associations

Nomad Pre-caching

Nomad Download Pause.

9.2.3.4 Nomad Download Pause

Nomad Download Pause is available if you implement a Tachyon server infrastructure, including enabling the **Tachyon client** features in 1E Client in addition to the Nomad client. It also requires Single Site Download.

9.2.3.5 NightWatchman Enterprise

Nomad integration with WakeUp is available if you enable this feature when installing NightWatchman Management Center. You should install the Tachyon Platform first and then install NightWatchman Management Center.

In summary, you require the following:

Tachyon Platform

NightWatchman Management Center server

WakeUp Server installed on each Configuration Manager site server

WakeUp client module enabled in the 1E Client on all client computers

Wake-on-LAN enabled on all client computers.

Please refer to Integrating Nomad with WakeUp.

PXE Everywhere

If you are also implementing a PXE Everywhere solution using Nomad, ensure you meet its prerequisites. Please refer to PXE Everywhere Requirements.

9.2.3.6 Certificates

You can use digital certificates to certify the identity of entities in your network. We support the use of Public key infrastructure (PKI) based certificates or self-signed certificates. If you are using PKIs to digitally sign entities from the outset, ensure that they are deployed to all agents. Alternatively, you can deploy PKIs post-installation. Things to bear in mind when using the HTTPS protocol:

Define the certificate type using P2PSSLSETTINGS (0 – self-signed certificates or 1 – PKI certificates). By default, self-signed is enabled.

When self-signed is enabled, a self-signed certificate is created by the installer and stored in *MY* store.

Diagrams and tables with all the external Nomad communication ports. Useful, if needed, for network and device firewalls.

9.2.3.7 Networking

Due to the nature of how proxy servers can be implemented, some of which can be quite complex, you may need to consult your networking specialist to see if exceptions need to be added to enable Nomad's peer-copy over HTTP or HTTPS.

The following are the ports used by Nomad client on clients and on Distribution Points. The table does not include Configuration Manager communications, which can be found here: https://docs.microsoft.com/en-us/sccm/core/plan-design/hierarchy/communications-between-endpoints.

Ports	Notes	Configurable
UDP 1779	Default port Nomad uses for listening to elections to determine the master on a subnet, control traffic and for content transfer if you have Connectionless enabled. A firewall exception must exist for this port. Nomad will create one automatically for Windows firewall, but not for other firewall software.	Yes, during installation.
TCP 80 (HTTP) or TCP 443 (HTTPS)	Used when the Nomad master requests LSZ files from Nomad running on the DP and when the Nomad master downloads content using Nomad as provider. Communications depend on how the DP is configured. Configuration Manager is configured to use either HTTP or HTTPS. If Nomad clients and Content Distribution are configured to use HTTP/S, Nomad clients using SSD register and query for content.	No, for communications with CM components. Nomad service on startup reads the configured ports from CM client registry and uses the same for LSZ generation. Yes, for communications with Tachyon Platform using Nomad's PlatformURL setting.
TCP 5080 (HTTP) or TCP 5443 (HTTPS)	Default HTTP port to use for peer copy. If you are using a custom port, ensure that all agents use the same custom port. From Nomad 6.2, peer copy can be enabled over HTTP (default 5080) or HTTPS (default 5443). You can customize the ports for this feature in the host registry but a change to the default impacts	Yes, during installation.

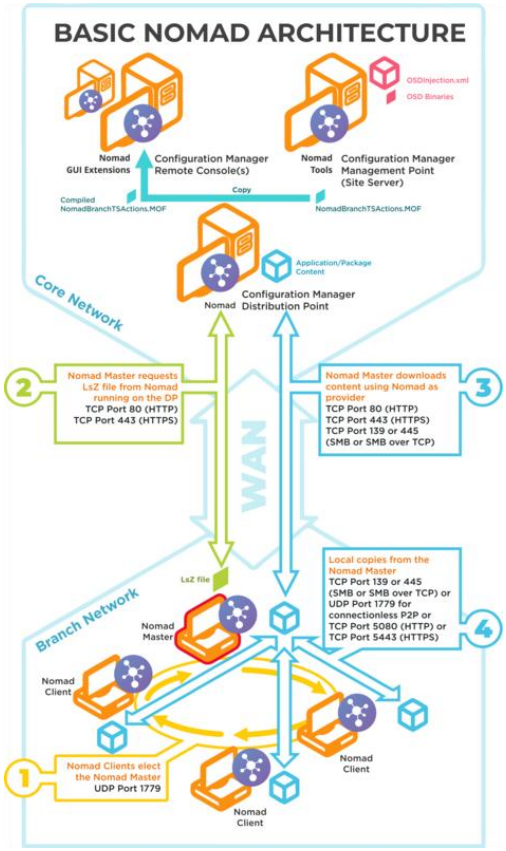
Ports	Notes	Configurable
	Nomad's peer backup assistant which is used to capture user data on remote peers during OS deployments.	
TCP 139 (SMB) and TCP 445 (SMB over TCP)	Required only if SMB is enabled. Used for peer-to-peer content transfer between the Nomad master and Nomad peers. Communications depend on how the DP is configured. That is HTTP, HTTPS, SMB or SMB over TCP. For Configuration Manager the default is HTTP or HTTPS. Windows Firewall automatically adds the exception when you enable **File and Print Sharing** but you may have to do this manually if you are using a different firewall product.	No. SMB ports cannot be configured.
TCP 137 (SMB) and TCP 139 (SMB)	Required only if SMB is enabled. Used by SMB for data transfer and related communications. It is used to resolve NetBIOS names during a transfer. UDP NetBIOS name query packets are sent to this port. Windows Firewall automatically adds the exception when you enable **File and Print Sharing** but you may have to do this manually if you are using a different firewall product.	No. SMB ports cannot be configured.

Nomad can use ephemeral ports (not discussed here). Ephemeral or high ports can either be UDP or TCP depending on the protocols used and are used to send information out. In a typical client-server communication, these are ports opened by the client on its own machine in order to send something to the server and they are closed as soon as the transmission is done, hence the term ephemeral. From a security perspective, it is not an issue.

Most firewalls will allow outgoing communications by default so in all likelihood, you will not need to do any firewall configuration. However, if your firewall blocks these outbound communications, consult the documentation for your firewall on how to enable these types of communications.

9.2.3.8 Basic Nomad architecture

Click image to enlarge.

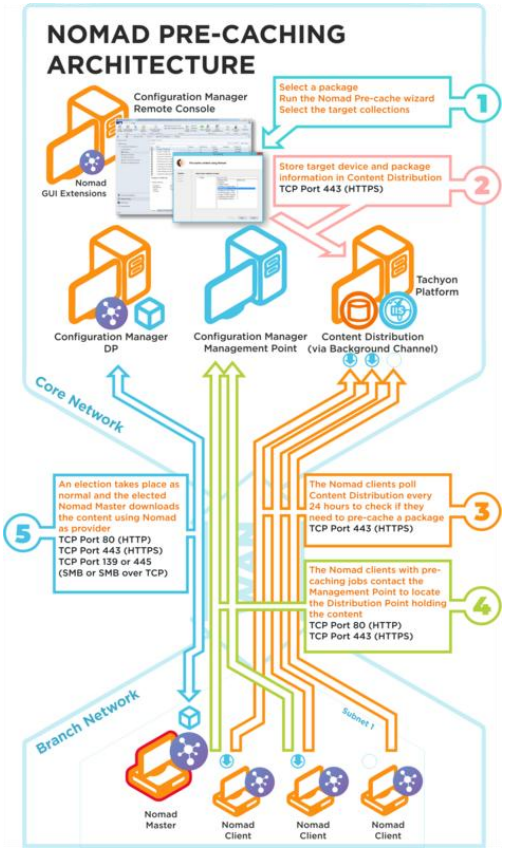


Ports	Notes
UDP 1779	**Step 1** By default, Nomad uses UDP Port 1779 to communicate during the election process for determining the master on a subnet. The Nomad installer will automatically add *NomadBranch.exe*,*NomadPackageLocator.exe* and *PackageStatusRequest.exe* to the list of excepted programs in the native Windows Firewall. The default value for the port may be changed at install time using the MODULE.NOMAD.P2PPORT installer property or post-installation by changing the P2P_Port registry value. If you change the default port, you must ensure all Nomad clients communicate using the same port. The Nomad port (by default UPD Port 1779) must be open on all wireless access points to facilitate Nomad peer-to-peer communications. Not all vendors enable this port by default, please refer to the specific device vendor's documentation for details on how to enable ports on each WAP device.
TCP 80 (HTTP)	**Step 2**

Ports	Notes
TCP 443 (HTTPS)	Nomad Master requests LSZ file from Nomad running on the DP.
TCP 80 (HTTP) TCP 443 (HTTPS) TCP 139 (SMB) TCP 445 (SMB over TCP)	**Step 3** Nomad Master downloads content using Nomad as provider. This communication depends on how the DP is configured. It may be one of the following: HTTP HTTPS SMB SMB over TCP For Configuration Manager the default setting is HTTP or HTTPS.
TCP 139 (SMB) TCP 445 (SMB over TCP) UDP 1779 (used for connectionless P2P) TCP 5080 (HTTP) TCP 5443 (HTTPS)	**Step 4** Local copies from the Nomad master. The recommended way to facilitate Nomad cache access is to enable Windows File and Print Sharing. If this is not feasible on your network environment you can configure Nomad to use different means to access network shares, see Nomad cache for more details on configuring this option. Connections may use one of the following: SMB SMB over TCP Connectionless P2P HTTP HTTPS

9.2.3.9 Nomad pre-caching architecture and ports

Click image to enlarge.



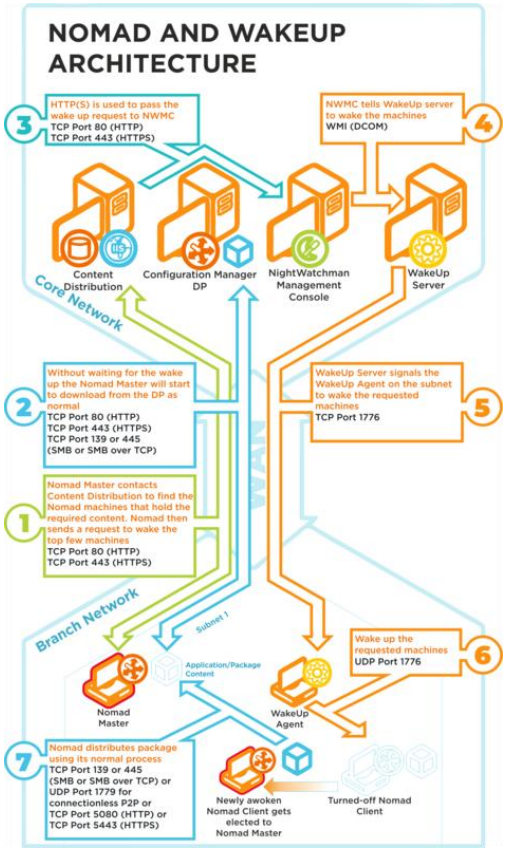
The Nomad pre-caching uses the following ports in its communications. If a site server is configured to use custom ports, pre-caching will use those ports to communicate with a management or distribution points. To ensure high-availability, pre-caching falls back to next available site server if it fails to communicate with a management or distribution point.

Ports	Description
N/A	**Step 1** Choose a package and run the Nomad pre-caching wizard, selecting the target device collection. This step does not require any port configuration but the Nomad Configuration Manager console extensions must be installed in the Configuration Manager Console.
TCP 80 (HTTP) TCP 443 (HTTPS)	**Step 2** The Nomad pre-caching wizard stores the target device and package information in Tachyon.
TCP 80 (HTTP)	**Step 3** The Nomad clients, where the pre-cache feature has been enabled, poll Tachyon every 24 hours to see if they need to pre-cache some content. This takes the form

Ports	Description
TCP 443 (HTTPS)	of pre-caching notifications that tell the Nomad clients they need to process a download job to fetch the specified content.
TCP 80 (HTTP) TCP 443 (HTTPS)	**Step 4** The Nomad clients, with pre-caching notifications, contact the Management Point to locate the Distribution Point that holds the content. This may use HTTP or HTTPS depending on how the Management Point is configured.
TCP 80 (HTTP) TCP 443 (HTTPS) TCP 139 (SMB) TCP 445 (SMB over TCP)	**Step 5** A Nomad Master election takes place and the elected master processes the job by downloading the pre-cache content using Nomad as provider. This is then distributed locally to the Nomad peers that also require the pre-cached content. This communication depends on how the DP is configured. It may be one of the following: HTTP HTTPS SMB SMB over TCP For Configuration Manager the default setting is either HTTP or HTTPS.

9.2.3.10 Nomad and WakeUp integration architecture and ports

Click image to enlarge.

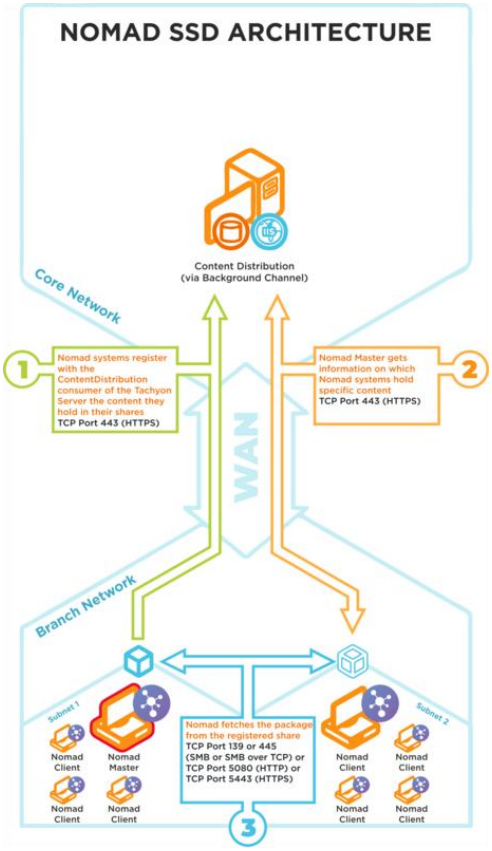


Ports	Description
TCP 80 (HTTP) TCP 443 (HTTPS)	**Step 1** Nomad Master contacts Content Distribution and gets a list of Nomad devices that hold the content it requires. Nomad sends a request to wake the top 5 devices on the list. Refer to WakeUpBatchSize for details about how you can set the maximum number of machines to wake up in a single call.
TCP 80 (HTTP) TCP 443 (HTTPS) TCP 139 (SMB) TCP 445 (SMB over TCP)	**Step 2** Without waiting for any devices to be awoken, the Nomad master starts to download content from the DP. This communication depends on how the DP is configured. It may be one of the following: HTTP HTTPS SMB

Ports	Description
	SMB over TCP For Configuration Manager, the default setting is HTTP or HTTPS.
TCP 80 (HTTP)	**Step 3**
TCP 443 (HTTPS)	Content Distribution posts the wake message from Nomad to the NightWatchman Management Center Web API.
WMI (DCOM)	**Step 4**
	NightWatchman Management Center tells the WakeUp server to wake the requested devices.
TCP 1776	**Step 5**
	WakeUp Server signals the WakeUp Agent on the appropriate subnet to wake the requested devices.
UDP 1776	**Step 6**
	The WakeUp agent on the subnet sends a wakeup request to the requested devices.
TCP 139 (SMB)	**Step 7**
TCP 445 (SMB over TCP) UDP 1779 (connectionless P2P)	As part of its standard behavior, Nomad holds regular elections (every 5 minutes) to determine the most appropriate master. If a device is found (i.e. one that has been recently awoken) that holds more of the required content, it stops downloading from the DP and fetches the content from the new device's cache. This may be via SMB or via connectionless P2P, depending on the configuration of Nomad.

9.2.3.11 Nomad SSD architecture and ports

Click image to enlarge.



Nomad SSD uses the following ports in its communications:

Ports	Notes
TCP 80 (HTTP)	**Step 1**
TCP 443 (HTTPS)	Nomad systems on the branch site register in Content Distribution the content they hold in their shares
TCP 80 (HTTP)	**Step 2**
TCP 443 (HTTPS)	Nomad Masters get information on which Nomad systems hold specific content
TCP 80 (HTTP)	**Step 3**
TCP 443 (HTTPS)	Nomad Master fetches a package from the registered Nomad share on a neighboring subnet
TCP 139 (SMB)	
TCP 445 (SMB over TCP)	

We recommend that the latest version of Tachyon Platform is installed to support this feature, please refer to Requirements for more details.

9.2.4 Installing Nomad

How to install Nomad.

9.2.4.1 Installing Nomad overview

Nomad installation requirements including installers and installation order.

9.2.4.1.1 Nomad installers

Before installing Nomad, make sure your infrastructure meets the Requirements.

Nomad requires the installation of:

1E platform.

1E Client (with the Nomad client module enabled) installed on Windows devices.

1E Client (with the Nomad client module enabled) installed on Configuration Manager Distribution Points.

For full details, refer to:

Installing Tachyon

Installing the 1E Client for Nomad

Deploying the Nomad client using Configuration Manager.

9.2.4.1.1.1 Nomad Branch Tools

Note

You can download the 1E Content Distribution Tools from the **Releases** page for your platform version at https://support.1e.com/.

NomadBranchGui.msi	Installer for a useful troubleshooting tool to monitor Nomad activity. It has no dependency on Configuration Manager. For information about using this tool, please refer to Nomad Download Monitor.
NomadBranchTools.msi	Installer for 1E NomadBranch Tools (for OSD) on Configuration Manager site servers

	1E Nomad Branch Admin Extensions on Configuration Manager consoles (previously *NomadBranchAdminUIExt.msi*) For information about installing these tools, please refer to Installing Nomad Branch Tools.
Scripts\CDPurgeSettings.ps1	A sample PowerShell script to view or update Purge Configuration in the Content Distribution Service defined in the ContentDistribution PurgeSettings table if it is configured. For details of how to use this script, please refer to Content Distribution purge configuration script.
Scripts\ExampleSitesAndSubnets.ps1	Sample script that provides two functions to update sites and subnets in the Content Distribution locations table: DeleteAllLocations and AddLocation(). For details of how to use this script, please refer to Example Single Site script.
Scripts\LocationDiscovery.ps1	Sample script to enable and disable the location discovery feature, along with the option to run it and load site, subnet and information in Content Distribution. For details of how to use this script, please refer to Example Location Discovery script.
Scripts\PostADSitesandSubnets.ps1	Sample script that scans the Active Directory (AD) environment for all sites and subnets and stores the information in the Content Distribution locations table. For details of how to use this script, please refer to Example Active Directory Single Site script.

Note

The sample PowerShell scripts can be used to populate the Content Distribution database, to support the following Nomad features:

Single Site Download (SSD)

Single-site Peer Backup Assistant (SSPBA)

High Availability Peer Backup Assistant (HAPBA).

1E Client

Note

You can download the 1E Client from the **Releases** page for your platform version at https://support.1e.com/.

1E.Client-x86.msi	Installer for computers that have a **32-bit** platform architecture.
1E.Client-x64.msi	Installer for computers that have a **64-bit** platform architecture, including **Distribution Points**.

Note

The Nomad client is a client module in the 1E Client, which also includes Tachyon and client modules for Shopping/WSA and WakeUp. Please refer to Introducing 1E Client for installation and configuration details.

Please refer to Introducing 1E Client Deployment Assistant for information about a wizard that assists Configuration Manager with the deployment of 1E Client and PXE Everywhere, guiding you through common settings for clients and deployments.

9.2.4.1.2 Installation Order

We recommend you install Nomad in the following order:

1	Tachyon Platform	If you have purchased a Tachyon license, then you can install and use Tachyon for additional features. To prepare for and install Tachyon, please refer to Planning for Tachyon.
2	Nomad Tools for Operating System Deployment (OSD) on Configuration site servers	Install Nomad Branch Tools for OSD on the Configuration Manager primary sites (and extra SMS Providers, if they exist) if Nomad's OSD features are required, refer to Installing Nomad Branch Tools. **Note** Configuration Manager Console should not be running on the computer when **NomadBranchTools** is installed/upgraded. **Tip** If you are also implementing PXE Everywhere, you may wish to install PXE Everywhere Central on your site

server at this point. Please refer to Implementing PXE Everywhere.

3	Install Console extensions on Configuration Manager site servers	Install Nomad Branch Toolson any computers that have Configuration Management Console installed, refer to Installing Nomad Branch Tools. **Note** Configuration Manager Console should not be running on the computer when **NomadBranchAdminUIExt** is installed/upgraded.
4	Deploy 1E Client to selected Configuration Manager Distribution Points	Install 1E Client (with Nomad client module enabled) on Configuration Manager Distribution Points. Enable Tachyon features and other client modules if required. By default, IIS is configured to prevent certain file types from being downloaded. You will need to allow Nomad to download all content as it does not use the Configuration Manager workaround to bypass this Microsoft security feature. We recommend you read Nomad post-installation tasks: IIS request filtering which describes how to update the filtering on all distribution points to enable Nomad to function as expected. You might also want to configure any virus checkers running on your network to make exceptions for the Nomad executables and support files, as described in Nomad post-installation tasks: Antivirus exceptions. **Tip** You can also optionally install PXE Everywhere Responders to selected clients if you have DHCP snooping enabled in your network. Please refer to DHCP Snooping.
5	Deploy 1E Client to selected Configuration Manager clients	Install 1E Client (with Nomad client module enabled) on Configuration Manager Distribution Points. Enable Tachyon features and other client modules if required. **Tip** You can also optionally enable PXE Everywhere Agent in the 1E Client.

6	Post-installation tasks	Verify selected clients before deploying the 1E Client to remaining Distribution Points and client devices. Deploy Console extensions to administrator workstations.

9.2.4.1.3 Licensing Nomad in 1E Client

The Nomad client module in 1E Client 4.1 and later does not require a license key. Nomad does not require input of a license key, or relicencing when upgrading or updating. Customers are legally bound to use the software within the terms of the 1E software license agreement.

9.2.4.2 Installing the Nomad app and 1E Content Distribution

An overview of the Tachyon Platform, and the interactive installation of Nomad and 1E Content Distribution using Tachyon Platform Setup, with screenshots.

9.2.4.2.1 Tachyon Platform setup

The Nomad app and 1E Content Distribution are installed through Tachyon Platform setup.

For full details on how to set up Tachyon Platform, please refer to Tachyon Setup. You choose to install Nomad on the following two screens during setup:

Select Configuration - allows you to choose whether to install Tachyon Platform

Configure Nomad - allows you to specify your Configuration Manager (CM), SQL database instance, and Nomad sync interval.

After installation, you should refer to the following:

9.2.4.2.1.1 Tachyon Platform post installation tasks

Post-installation tasks, which include verification checks and mandatory and optional configuration tasks. For details refer to Tachyon Server post-installation tasks.

9.2.4.2.1.2 Deploying the 1E Client

How to deploy 1E Client, including a guide to upgrading. 1E Client provides Tachyon client features and client modules for Nomad, PXE Everywhere, Shopping/WSA, and WakeUp. For details refer to Deploying 1E Client.

9.2.4.2.1.3 Basic verification tests

Basic verification tests that cover a single-server installation of Tachyon Server. These tests only cover Tachyon and do not verify the configuration of 1E client modules with other 1E products. For details refer to Verifying.

9.2.4.2.2 Nomad app

The Tachyon Portal website will be available after installation. You can access the Nomad app directly using a URL similar to the following:

Note

https://tachyon.acme.local/Nomad

The Nomad app will be available on the Tachyon Platform portal homepage and as an app from the left-hand navigation in the Tachyon Platform portal, under the **Switch app**.

For details about each page in the Nomad app, please refer to:

Overview page - provides a visual snapshot of download activity

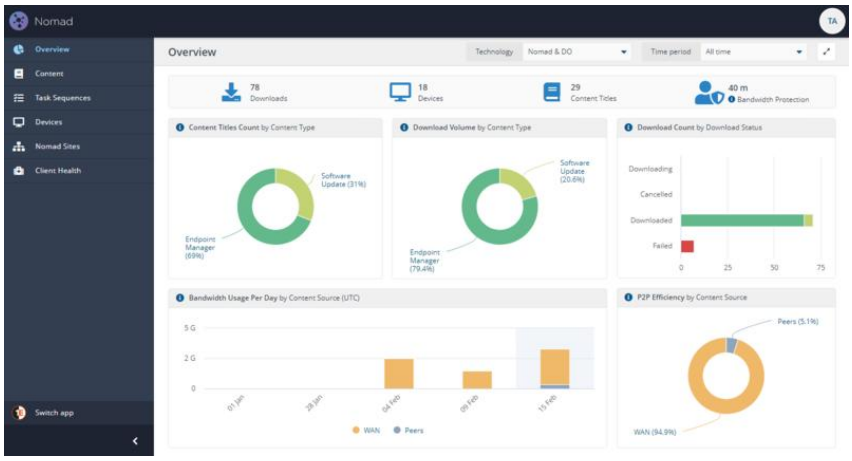
Content page - lists the unique contents synced from Configuration Manager

Task Sequences page - lists the configured task sequences

Devices page - lists every device registered to Nomad

Nomad Sites page - shows how the network is being used for content distribution in different locations

Client Health page - shows Nomad related device status information from the Guaranteed State app.



Tip

You should check each of these pages, and verify you are able to access them, and they present no issues.

For example, by default, the Client Health page will not show any data until you have completed configuration of the **Nomad Administrators** role, and uploaded the Client Health policies. Both of these tasks are described below.

9.2.4.2.3 Nomad roles and permissions

As part of the installation process, Tachyon Platform adds the **Nomad Administrator** role described in the Nomad Administrator section. The Nomad Administrator role includes permissions to view Guaranteed State and Client Health Policies and requires Configuration Manager permissions.

9.2.4.2.3.1 Nomad Administrator role

The Nomad Administrator role, allows a Tachyon user to use Nomad, manage Pre-cache jobs and view the results of related Instructions and Client health policies. As part of the installation

process, Tachyon Platform adds the **Nomad Administrator** role, with the following default permissions, viewable in the Tachyon Platform **Settings**app.

Name	Type	Permissions	Purpose
GuaranteedState	Global Permissions	Read	Allows access to Guaranteed State features, including the Client Health page.
Nomad	Global Permissions	Read, Write, Delete	Allows the Nomad app to be used.
1E Nomad	Instruction Set	Actioner	Allows instructions from the **1E Nomad** instruction set to be run. See Product Packs section below. This pack includes instructions required by Nomad Pre-caching and Nomad Download Pause features.

Typically, you would assign your Configuration Manager administrator AD group to this role, as described below in Configuration Manager permissions, to allow them access to relevant Nomad features in the Tachyon Platform.

The Nomad Administrator role can only be applied at the All Devices Management Group level, because it is defined as a non delegatable custom role.

> **Note**
>
> Delegation in Tachyon is a concept where an administrator can delegate some of their own responsibility to other users and limit the area where they can use that responsibility. In Tachyon, a Full administrator can create and modify Roles. They can also assign any Role to a Tachyon user or group using Management Groups, there are exceptions, like the **Group Administrator** Role which cannot be assigned to **All Devices**.
>
> For example, a local security administrator with the **Group Administrator** role cannot create or modify Roles, but they can assign any Role that is marked as delegatable to a Management Group they have the security permission on or any of its child Management Groups.
>
> Refer to the Permissions Menu for details about configuring Tachyon users, roles, and management groups.

9.2.4.2.3.2 Upgrading Nomad and the Nomad Administrator role

When you upgrade from a previous Tachyon version to Tachyon Platform 8.0 note the **Nomad Administrators** role has been renamed to **Nomad Administrator**.

In addition, please note that:

Before upgrading to Tachyon 8.0	Post upgrade to Tachyon 8.0
If a user had the **Nomad Administrators** role without any management group assigned.	**Nomad Administrator** role with the **All Devices** management group will be assigned to that user.
When a user has the **Nomad Administrators** role assigned with one or more management groups except **All Devices**.	**Nomad Administrator** role with**All Devices** along with all other existing management groups would be assigned to the existing user.

The only difference would be for Nomad Pause jobs which would be applicable to the **All Devices** management group in Tachyon.

9.2.4.2.3.3 Guaranteed State and Client Health Policies

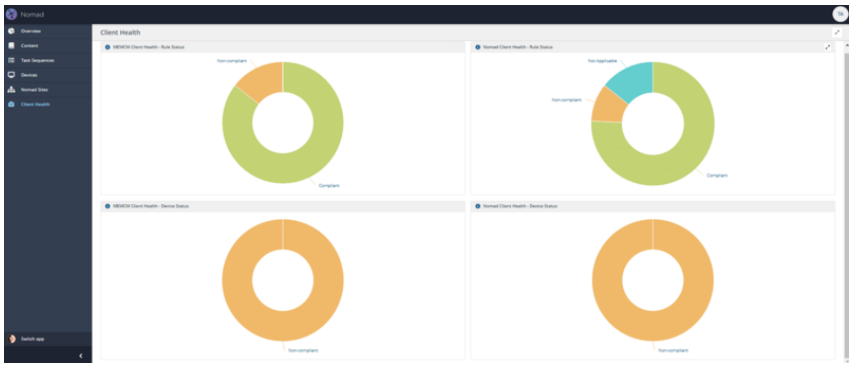
TheClient Health page shows Nomad related device status information from the Guaranteed State app.

The Nomad Administrator role allows a user to view information from Integrated Product Packs, including the two packs provided with the Tachyon Platform:

MEMCM Client Health Policy

Nomad Client Health Policy.

These Integrated Product Packs are represented on the Client Health page in the Nomad app.



Note

Guaranteed State can be reached directly using the following URL:

```
https://<tachyon DNS Name FQDN>/Tachyon/App/#/guaranteedstate/
```

where <tachyon DNS Name FQDN> is the one set up during the preparation phase, as described in DNS Names.

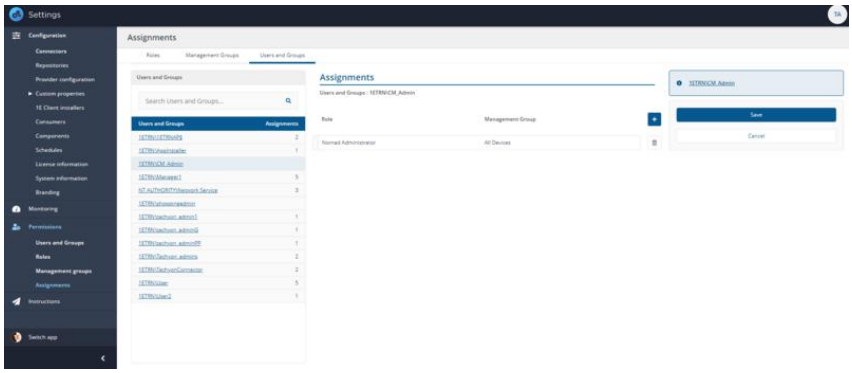
Configuration Manager administrators

If you have a single AD security group for your Configuration Manager administrators, you should assign it as a member of the **Nomad Administrator** group. This allows them to use the Nomad app, view and delete pre-cache and paused collections, and use Guaranteed State features if installed.

However, if you have decided to use different roles for Nomad app and Guaranteed State features, then you can assign the same or different AD security groups to the **Nomad Administrator** and **Guaranteed State User** roles.

For more information about these features, please refer to Nomad app overview, Nomad Pre-caching, Nomad Download Pause, and the Client Health page.

The example shows a Universal group called **CM_Admin** of which our Configuration Manager administrator account(s) are members.



Note

Active Directory security groups are strongly recommended for role-based access control (RBAC) but are not mandatory. AD security groups can be assigned to Tachyon roles after installation, they are not required during installation. They are added as Tachyon users and configured in the same way as AD user accounts.

A Tachyon user can therefore be a domain user account or a security group. Groups are not mandatory because users can be assigned to roles and managed within Tachyon instead of AD, or a combination.

9.2.4.2.4 1E Nomad product packs

Nomad feature-related Product Packs are included in the **Tachyon Platform** zip. These Product Packs are required to support various features of **Nomad**.

1E Nomad product pack - contain instructions, for use in Explorer and other Tachyon applications.

Nomad Client Health integrated Product Pack - contain policies, rules and fragments for use by Guaranteed State, and may also include instructions.

Refer to Adding Product Packs and configuring Instruction Sets for details about how to load instructions into Tachyon and create Instruction Sets for them.

9.2.4.2.4.1 1E Nomad product pack

Classic product pack used to create the **1E Nomad** instruction set in Tachyon, required by the following Nomad features:

Downloads tab on Device views - instructions used to populate details about Content download and other Nomad features

Nomad Download Pause - instructions used by the CM Admin Console extensions

Instructions to help with the following Nomad features: Nomad cache, CacheCleaner, Single Site Download, Nomad jobs, NomadBranch service.

For a full list of the instructions in the 1E Nomad product pack, including:

Associated Nomad feature

The instruction Type

Instruction description.

Refer to 1E Nomad product pack for more information.

9.2.4.2.4.2 Nomad Client Health integrated Product Pack

Nomad is included as part of the 1E Client, and as part of that integration, we offer a Nomad client health compliance policy in Guaranteed State. This verifies common Nomad requirements such as ACP registration, disk availability, firewall exceptions, crash notifications and cache monitoring.

The Nomad client health policy replaces the client health tile in the Nomad dashboard plus additional remediation steps:

Keeps content distribution services up and running on Nomad clients, so that users are secure and productive

Ensures Alternative Content Provider (ACP) registration configuration is set

Maintains optimal disk availability and monitors cache size for storage capacity planning

Enforces Firewall exceptions.

> **Note**
>
> This policy is intended for deployment to Windows devices only.

For a full list of the instructions in the Nomad Client Health Integrated Product Pack, including:

Instructions

Policies

Rules

Fragments

Trigger templates.

Refer to 1E Nomad product pack for more information.

9.2.4.2.4.3 Adding Product Packs and configuring Instruction Sets

You can either load instructions into Tachyon and create Instruction Sets for them automatically using Tachyon Setup and the **Tachyon Product Pack deployment tool**, or you can also load the product packs and create their associated instruction sets by hand.

For details about how to:

Manually load Instruction Definitions into Tachyon and then create, populate and delete Instruction sets – refer to Instruction sets page

Automatically upload instructions using the **Tachyon Product Pack deployment tool** – refer to Uploading with the Tachyon Product Pack Deployment Tool.

The **ProductPacks** folder in the Tachyon Platform zip file contains a number of **Classic** and **Integrated** product pack zip files. Reference information for Product Packs is included in the **Tachyon Platform** zip. These Product Packs are required to support various features of Tachyon.

> **Note**
>
> The **Tachyon Platform** zip is downloaded from the 1E Support Portal (1eportal.force.com/s/tachyontopicdetail). Additional Product Packs are available from Tachyon Exchange (tachyonexchange.1e.com) that are not documented here.

9.2.4.3 Installing the 1E Client for Nomad

For guidance on deploying the 1E Client onto Windows computers, including installation and uninstallation, refer to Deploying 1E Client on Windows.

9.2.4.4 Deploying the Nomad client using Configuration Manager

A step-by-step guide for using Configuration Manager to deploy the Nomad client to computers with the Nomad module enabled.

> **Note**
>
> The client component of Nomad 7.0 and later is the Nomad module of the 1E Client. This module is a direct replacement of NomadBranch used by previous versions of Nomad. The 1E Client includes modules for other 1E products, including Tachyon, Shopping and WakeUp. You can optionally enable these modules during deployment, or later by configuring the 1E Client configuration file.

9.2.4.4.1 Using Configuration Manager to deploy the Nomad client

Using Configuration Manager to deploy Nomad to all the Configuration Manager client machines is a relatively simple and efficient way of configuring all the Nomad client installations in one go. **1E Client Deployment Assistant (CDA)** is recommended as the most efficient way of creating Configuration Manager applications and deployments for clients, and packages for use in Task Sequences, or you can follow the instructions below to manually create applications. Please refer to Introducing 1E Client Deployment Assistant.

> **Note**
>
> If you are upgrading Nomad or any other client modules in 1E Client (Tachyon, Shopping, WakeUp) then please refer to Upgrading Nomad especially the note about **Application Supersedence**.
>
> **Tip**

Please also refer to Using Configuration Manager to enable and reconfigure the 1E Client after installation. The page describes how to use a **Configuration Manager Configuration Baseline**, and includes a zip file with template Configuration Items that can be imported into Configuration Manager.

9.2.4.4.2 Creating a Configuration Manager application to install the Nomad client

There are two installers for the Nomad client, one for 32-bit OS and the other for 64-bit OS:

1EClient-x86.msi is used for 32-bit OS

1EClient-x64.msi is used for 64-bit OS

The following headings show how to define an application and deployment types for each of these installers.

9.2.4.4.2.1 Creating an application with a deployment type for the 64-bit Nomad client installer

To create an application to install the Nomad client:

In the Configuration Manager console, open **Software Library**→**Application Management**.

Right-click **Applications** and choose **Create Application**.

On the **General settings** screen in the **Create Application Wizard**, select **Manually specify the application information**.

Click **Next**.

Populate the details for the application as follows:

Name: **Nomad client**

Publisher: **1E**

Software Version: **8.1**

Select the option:
Allow this application to be installed from the Install Application task sequence action without being deployed.

On the **Software Center** screen, click **Next**.

On the **Deployment Types** screen, click the **Add...** button.

From the **Type** drop-down in the **Create Deployment Type Wizard**, ensure that **Windows Installer (*.msi file)** is selected.

Ensure **Automatically identify information about this deployment type from installation files** is selected.

Set the **Location** of the **1EClient-x64.msi** installer using the **Browse...** button and locating the file from the share where the file has been stored.

Click **Next**.

On the **Import Information** screen, (assuming the import from the *msi* was successful), click **Next**.

On the **General Information** screen, set the **Name:** field to **Nomad client (64-bit)**.

Change the **Installation program** to something similar to the following:

```
> msiexec /i 1EClient-x64.msi MODULE.NOMAD.ENABLED=true MULTICASTSUPPORT=
0 LOGPATH=C:\Windows\CCM\Logs [other properties] /qn
```

In the above command line:

MULTICASTSUPPORT=0 turns off multicast (it makes the logs noisy if multicast hasn't been set up).

LOGPATH=C:\Windows\CCM\Logs sets the location of the Nomad client log files. When troubleshooting, it can be useful for Configuration Manager administrators to have the Nomad client log files in the same location as the Configuration Manager client log files.

You might also consider using a Windows Installer Transform (.mst) if there are a number of properties to define making the installer command-line long.

When the **Installation program** edit field has been set click **Next** to continue.

On the **Requirements** screen, click **Add...**

In the **Create Requirement** dialog, populate the requirements as follows:

Category: **Device**

Condition: **Operating system**

Rule type: **Value**

Operator, select **One of** from the dropdown list and then check any of the 64-bit OS you may encounter in your environment, for example **All Windows 10 (64-bit)**.

Click **OK**.

Click **Next**.

On the **Dependencies** screen, click **Next**.

On the **Summary** screen, click **Next** to start apply these settings.

You should see the heading **The Create Deployment Type Wizard completed successfully**, on the **Completion** screen of the **Create Deployment Type Wizard**. Click **Close** to close the wizard.

A new deployment type called **Nomad client (64-bit)** will have been added to the **Deployment types** field in the **Create Application Wizard**. At this point you could create another deployment type for the 32-bit version of Nomad, as described in Adding a deployment type for the 32-bit version of Nomad below.

Once you've finished creating the deployment types, click **Next** on the **Deployment Types** screen to continue.

On the **Summary** screen, click **Next** to start the creation of the application.

You should see the heading **The Create Application Wizard completed successfully**, on the **Completion** screen of the **Create Application Wizard**. Click **Close** to close the wizard

The **Nomad client** application should now be created in Configuration Manager.

9.2.4.4.2.2 Adding a deployment type for the 32-bit version of Nomad client

During or after the creation of the Nomad client application you can also add a deployment type for the 32-bit version of Nomad client using one of the following methods:

During creation: on the **Deployment Types** screen of the **Create Applications Wizard**

After creation on the **Deployment Types** tab of the application **Properties** dialog in Configuration Manager

After creation by right-clicking on the application in Configuration Manager and selecting **Create Deployment Type** from the context menu

The steps for each method are the same, to add a deployment type for the 32-bit version of Nomad repeat steps 7 to 22 under the heading Creating an application with a deployment type for the 64-bit Nomad installer - making the following changes:

At **step 10** set the location for the **1EClient-x86.msi** instead

At **step 13** on the **General Information** screen set the **Name:** field to **1E Client (32-bit)**

At **step 14** change the **Installation program** field to something similar to the following (essentially the same as the 1E client (64-bit) command line, except that the msi file name is **1E.Client-x86.msi**):

```
msiexec /i 1E.Client-x86.msi MODULE.NOMAD.ENABLED=true MULTICASTSUPPORT=t
rue LOGPATH=C:\Windows\CCM\Logs [other properties]/qn
```

At **step 17** when you set the operator check any checkboxes for the 32-bit OS you have in your environment instead, for example: **All Windows 8.1 (32-bit)** and **All Windows 10 (32-bit)**

9.2.4.4.3 Adding content to your distribution point

To add content to your distribution point:

From the **Applications** node in the **Software Library** workspace, right-click the **Nomad client** Application and from the context menu, choose **Distribute Content**.

On the **General** screen of the **Distribute Content Wizard**, click **Next**.

On the **Content** screen, click **Next**.

On the **Content Distribution** screen, click **Add** and choose **Distribution Point** from the drop-down list.

In the **Add Distribution Points** dialog, choose the distribution point.

Click **OK** to close the **Add Distribution Points** dialog and add the selected distribution points.

Click **Next** on the remaining screens of the Distribute Content Wizard to start adding the content to the selected distribution point(s).

If everything goes well you should see the message **The Distribute Content Wizard completed successfully**. Click **Close** to close the wizard.

9.2.4.4.4 Deploying the Nomad client to All Desktop and Server Computers

To deploy the Nomad client:

From the **Applications** node in the **Software Library** workspace, right-click the **Nomad client** application and from the context menu, choose **Deploy**.

On the **General** screen of the **Deploy Software Wizard**, click **Browse...** next to the **Collection:** field to open the **Select Collection** dialog.

From the drop-down list, choose **Device Collections**, then select **All Desktop and Server Clients**.

Click **OK** to return to the **General** screen.

Click **Next** to continue.

On the **Content** screen, ensure the content has been deployed to your distribution point (see step 6 under the Adding content to the Distribution Point heading). Click **Next** to continue when you have confirmed the distribution points.

On the **Deployment Settings** screen, ensure **Install** is selected on the **Action:** field drop-down list and select **Required** from the **Purpose:** field drop-down list, then click **Next** to continue.

On the **Scheduling** screen, click **Next** to accept the default deadline (**As soon as possible after the available time**).

On the **User Experience** screen, choose **Display in Software Center, and only show notifications for computer restarts** from the drop-down list.

Click **Summary** to skip to the **Summary** screen.

On the **Summary** screen, check the settings and click **Next** to start the deployment.

If everything goes well you should see the message **The Deploy Software Wizard completed successfully**. Click **Close** to close the wizard window.

9.2.4.4.5 Speeding up and monitoring the progress of the installation

To speed up and monitor the progress of the installation:

In the Configuration Manager console, select the **Assets and Compliance** workspace.

Select the **Device Collections** node, right-click **All Desktop and Server Clients** and choose **Client Notification→ Download Computer Policy**.

A dialog is displayed showing the number of resources in this collection. Click **OK**.

> **Note**
>
> This process causes each of the Configuration Manager clients to download the new deployment policy you just created rather than waiting for them to do it on their regular schedule. This may speed up the uptake of the new deployment.

Select the **Monitoring** workspace and choose the **Deployments** node.

Right-click the **Nomad client** deployment and choose **View Status** from the context menu. You can view the next task when the current one finishes.

9.2.4.4.6 Reviewing the installation on the client

To review the installation on a Windows 10 client (Previous version of Windows may differ):

Login to the client with administrative privileges.

From the **Start menu**, type services in the search box to open the **Services** app, note the **1E Nomad Branch** service is running.

Leave the Services App open, and from the **Start menu**, select **Computer Management**.

In **Computer Management**, expand **Local Users and Groups** and click **Users**. Note that the local user **SMSNomadP2P&** has been created.

Expand the **Shared Folders** node and click **Shares**, note that **NomadSHR** has been created – this is the Nomad cache.

Right-click **NomadSHR** and from the context-menu, choose **Properties**.

In the **NomadSHR** Properties dialog, note the path to the share as well as the 6 user (connection) limit.

Click the **Share Permissions** tab and note the permissions for the share.

Cancel the **NomadSHR** Properties dialog.

Leave **Computer Management** open and return to the **Services** app.

Right-click the **1E Nomad Branch** service and select **Stop**.

Return to **Computer Management** and refresh the **Shares** node, note the **NomadSHR** is deleted when the service is stops.

Switch to **Services** and start the **1E Nomad Branch** service.

Return to **Computer Management** and refresh **Shares**, note that the **NomadSHR** is recreated when the service starts.

Close **Services** and **Computer Management**.

Start Windows Explorer, and click folder **Options**.

On the **View** tab, ensure **Hidden Files and Folders** can be viewed, and uncheck **Hide extensions for known file types** and click **OK**.

Browse to **C:\ProgramData\1E\NomadBranch**, this is the folder that is shared as **NomadSHR** and is the root of the Nomad cache.

Browse to **C:\Windows\CCM\Logs** and double-click the **NomadBranch.log** to open it. Observe the **Nomadservice** startup activity in the log, note the client detected it is running on a Configuration Manager client and automatically enables the option to use HTTP and SMB.

Date/Time	Log Text
22/03/2013 19:46:26	CM 2012 client - Auto Enabling Http
22/03/2013 19:46:26	0x2000 SMB and Http

Close the log file.

From the **Start menu**, run **regedit**.

Navigate to **HKLM\Software\1E\NomadBranch**. This registry key contains all the configuration options used by Nomad.

9.2.4.4.7 Reviewing the installation on a distribution point

The installation on the Distribution Point (DP) server results in the same components being installed on the server, however the service will automatically perform the LSZ generation and RDC processing if it identifies that it is running on Configuration Manager on a Site Server and DP. For standalone DPs (distribution point not on a site server) the SIGSFOLDER and SPECIALNETSHARE installer properties will need to be correctly configured to enable the LSZ generation and RDC processing to take place, and PERMITTEDLSZSHARES may also need to be configured.

To review the installation on a site server distribution point:

Login to the server with administrative privileges.

From the Start screen, click **Services**. Note the **1E Nomad Branch** service is running. Close the **Services** console.

From the Start screen, start typing **regedit** and click **regedit** when it appears in the search results. Note the **HKLM\Software\1E\NomadBranch** registry key.

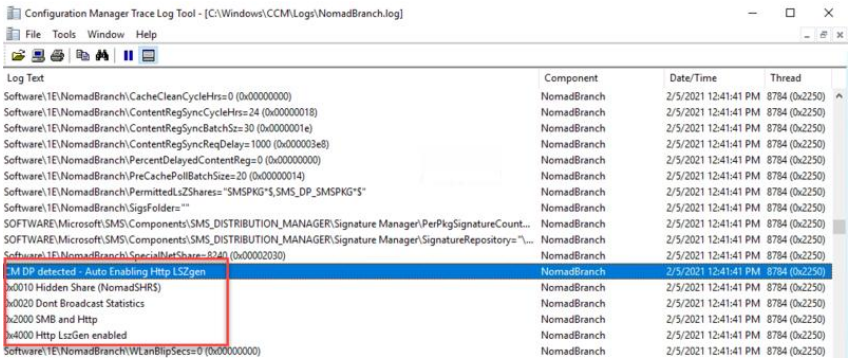
From the Start screen type **C:\ProgramData** and press Enter to open the folder. Browse to the **1E\NomadBranch** folder. Note that as this is a DP, the client has created the LSZFILES folder.

Browse to **C:\Windows\CCM\Logs** and open **NomadBranch.log** using cmtrace.exe

Near the top of the log file, notice that the computer has been identified as an SMS Site Server and an SMS distribution point.

Note

The HTTP LSZ generation option (normally set in **SpecialNetShare**) has also been enabled as Nomad has detected this is a Configuration Manager DP and will therefore be using HTTP.



The LSZFILES folder is also established as a virtual directory in IIS.

9.2.4.5 Installing Nomad Branch Tools

A step-by-step guide to installing Nomad Branch Tools which contains the Nomad Configuration Manager console extensions and Nomad OSD tools.

> **Note**
>
> If you intend using 1E Application Migration in your Task Sequences, then you will also need to install the 1E Task Sequence Tools alongside Nomad OSD Tools, as described in Using Application Migration in a task sequence.
>
> Nomad OSD Tools includes the Task Sequence action Get migration settings, which is also required by 1E Application Migration new computer (Replace scenario).

9.2.4.5.1 Before you start

Nomad Branch Tools is available as **NomadBranchTools.msi** in the NomadBranch zip. You can download this zip by clicking on the **Nomad Tools** link in the 1E Support Portal at https://support.1e.com/.

The **NomadBranchTools.msi** installer contains the following tools:

Nomad OSD tools

Nomad Configuration Manager console extensions.

> **Note**
>
> Nomad Branch Tools uses 64-bit architecture, and can only be installed on 64-bit operating systems.
>
> Previous versions of the Nomad Configuration Manager console extensions (NomadBranchAdminUIExt) supported 32-bit operating systems. However, this is no longer supported from Nomad 8.0.

9.2.4.5.1.1 Nomad OSD tools

The tools required for integrating Nomad with OSD task sequences in Configuration Manager.

Each Nomad tool executable has a corresponding .pdb file.

Nomad tool	Description
NBCacheActions.exe	Performs specific functions on the Nomad cache.
NomadBranch.exe	The Nomad service.
NomadPackageLocator.exe	Locates content in local Nomad caches.
SMSNomad.exe	The Nomad executable.
SMSTSNomad.exe	Nomad executable used in task sequences.
SnoItfPS.dll	The Nomad Enterprise COM/DCOM interface.
TSEnv2.exe	Sets environment variables in task sequences.

9.2.4.5.1.2 Nomad Configuration Manager console extensions

The Nomad Configuration Manager console extensions provide the following capabilities in the Configuration Manager Console:

Configuration Manager capability	Description
Configure Nomad settings	In software deployment and client settings policies associated with packages, applications and software updates.
Nomad Download Pause	Buttons to pause and resume Nomad downloads, monitoring report to view paused content.
Nomad Pre-caching	Menu item to start the Pre-cache Wizard, monitoring report to view pre-cached content.
Nomad Baseline wizard	Menu items to create and edit baseline configuration items.

9.2.4.5.1.3 Install permissions

All users require the following to install and use the Nomad Configuration Manager console extensions component of the Nomad Branch Tools:

Local administrator rights on the computer to install the console extensions

The Configuration Manager Console, installed on the computer to install and use the console extensions

A Configuration Manager user with **Full Administrator** rights to be able to use the Download Pause feature

Tachyon installed and working, you must know and enter the full URL for the Tachyon website in the installer.

> **Note**
>
> If you have an existing Nomad 7.0.200 installation, and you upgrade to Tachyon Platform 8.1 you should also upgrade your Nomad Configuration Manager console extensions to the current version, doing this ensures you can view your pre-existing Nomad pre-cache jobs. When you upgrade from earlier versions of Nomad to Tachyon Platform, ActiveEfficiency is upgraded to Content Distribution. As a result, if you have an earlier version of the Nomad Configuration Manager console extensions, you may not be able to view your existing Nomad pre-cache jobs until you upgrade.

9.2.4.5.1.4 Nomad Download Pause

Before installing or upgrading Nomad Branch Tools, you should consider the following:

The feature requires:

Tachyon Platform 8.x installed

Uploaded Tachyon instructions

Permissions allowing Configuration Manager (CM) administrators to execute the uploaded instructions.

These steps should be completed by a user that has Global Admin role in Tachyon, refer to Installing the Nomad app and 1E Content Distribution for details about Tachyon Platform setup, **Nomad Administrator** role and the 1E Nomad product pack.

> **Upgrading**
>
> If you are upgrading Nomad or Tachyon and you have previously installed **Nomad Download Pause** then you can continue using your existing setup, you do not need to do anything further, and you can ignore the information and steps below.
>
> However, you are recommended to rename the old instruction set from**Nomad Core Instructions**to**1E Nomad**to match the name used in the steps below for new installations. The renamed set will retain the permissions you previously configured.
>
> Prior to Nomad 7.0.200, you were advised *not* to change the name of the instruction set. This was because the **NomadBranchAdminUIExt.msi** installer uploaded the instructions into an instruction set named **Nomad Core Instructions**. From version 7.0.200 onwards, this restriction no longer applies, because the instructions are no longer in the installer, and instead are only available in the **1E-Nomad** product pack.
>
> The installation steps below use the Settings app to create the **1E Nomad** instruction set and upload instructions for a new installation. However, if you instead use the **Tachyon Product Pack Deployment Tool** to upload the **1E Nomad** product pack, the tool will create an instruction set called **1E Nomad** and place *new* instructions there. If the instruction set **Nomad Core Instructions** has not been renamed, any *existing* instructions

in it will remain or be updated if they are new versions. You may end up with two instruction sets. You can keep both sets, or you can do the following, which will retain the permissions you previously configured:

move the new instructions from **1E Nomad** to **Nomad Core Instructions**

delete the now empty instruction set **1E Nomad**

rename the old instruction set from **Nomad Core Instructions** to **1E Nomad**

The **1E-Nomad** product pack is provided in the Tachyon Platform download zip, and includes new versions of the same instructions. A list of these instructions is provided below under the heading 1E-Nomad product pack, which include the two instructions required by Nomad Download Pause.

9.2.4.5.2 Installing Nomad Branch Tools

In previous versions of Nomad, you installed Nomad Configuration Manager console extensions and Nomad OSD tools with two separate installers, now these are included in one installer, **NomadBranchTools.msi.** When you run the **NomadBranchTools.msi** installer it will upgrade any currently installed tools by removing older versions of Nomad Configuration Manager console extensions (NomadBranchAdminUIExt) and Nomad OSD tools (Nomad Branch Tools), and installing the newer versions.

Note

You will need to first upgrade your Tachyon Platform installation to 8.1 to benefit from the Nomad and Platform Integration feature of the Nomad Branch tools.

Before running the installation, you should check that you have:

Elevated Administrative privileges on the server where you're running the installation

The Configuration Manager Console installed on the server where you want to use the Nomad Configuration Manager console extensions

The Site server or SMS Provider configured on the server, so you can install and use the Operating System Deployment support (OSD Tools).

If you want to use both tools on the same server, you will need to have configured both Configuration Manager Console and Site Server/SMS Provider on that server. The installer will deploy either, or both the OSD Tools or Nomad Configuration Manager console extension depending on the above conditions.

9.2.4.5.2.1 Installing interactively

Install Nomad Branch Tools on the same device as the Configuration Manager Console, you can do this is done by running **NomadBranchTools.msi** from an elevated command prompt.

Note

The Configuration Manager Console must not be running when you run **NomadBranchTools.msi**

To install:

Download the Nomad Branch software zip. from https://support.1e.com/.

Extract **NomadBranchTools.msi** from the downloaded ZIP file.

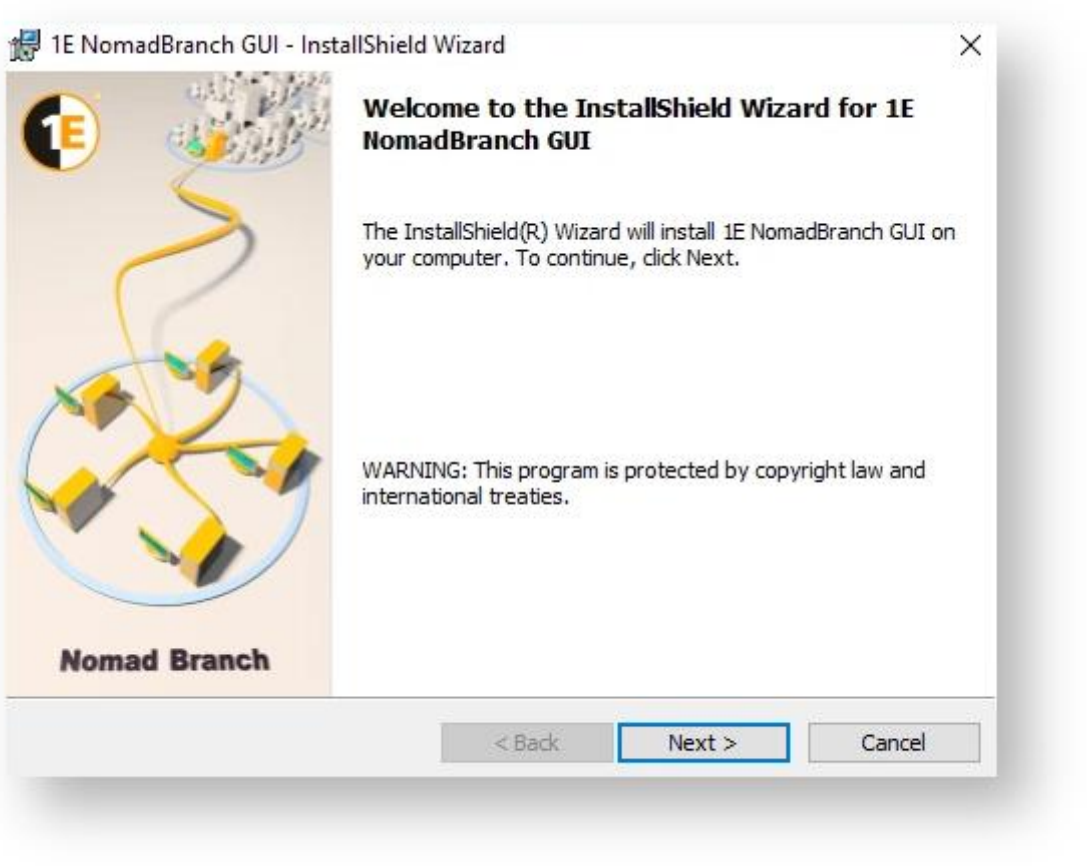
Start a Command Prompt with elevated rights, navigate to the location where you extracted **NomadBranchTools.msi** and run it with the following command-line:

```
> msiexec /i NomadBranchTools.msi /l*v NomadBranchInstall.log REBOOT=REALLYSUPPRESS
```

The following describes each of the screens in the installation wizard:

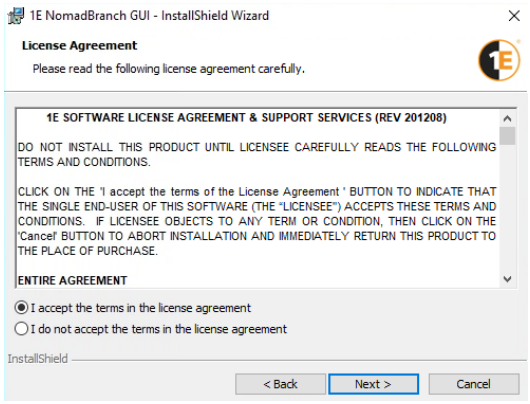
9.2.4.5.2.1.1 Welcome

The welcome screen, just click **Next** to continue.



9.2.4.5.2.1.2 License Agreement

You must read and then accept this license information by clicking the **I accept the terms in the license agreement** option before you can continue with the installation. Once this is done click **Next.**

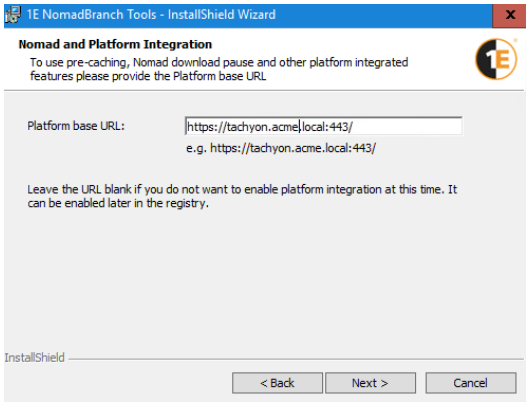


9.2.4.5.2.1.3 Nomad and Platform Integration

> **Note**
>
> Before installing this feature, please refer to Nomad Download Pause, for steps on configuring the prerequisites.

You need to supply the root URL to the Tachyon API. Which will be in the form: **https://<Tachyon DNS Alias FQDN>** using the Tachyon DNS Alias FQDN defined when you installed Tachyon.

For example if you installed Tachyon using **tachyon.acme.local** as the DNS Alias FQDN then the Tachyon API Root URL should be set to:




```
https://tachyon.acme.local
```

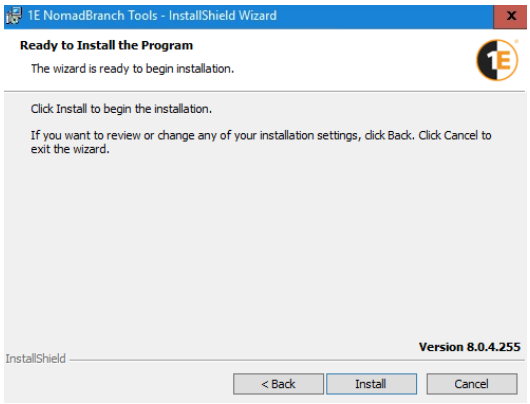
> **Note**
>
> The Tachyon API is Tachyon's Consumer API. You can learn more about Tachyon in Introducing Tachyon.

> **Note**
>
> From Nomad 8.1 there is support for providing alternate credentials to authenticate with the Tachyon Platform. If your Tachyon Platform instance resides in another domain or the cloud, you will be prompted to enter alternate credentials for that location, which get stored in the credential store for any future requests.

Click **Next** to continue.

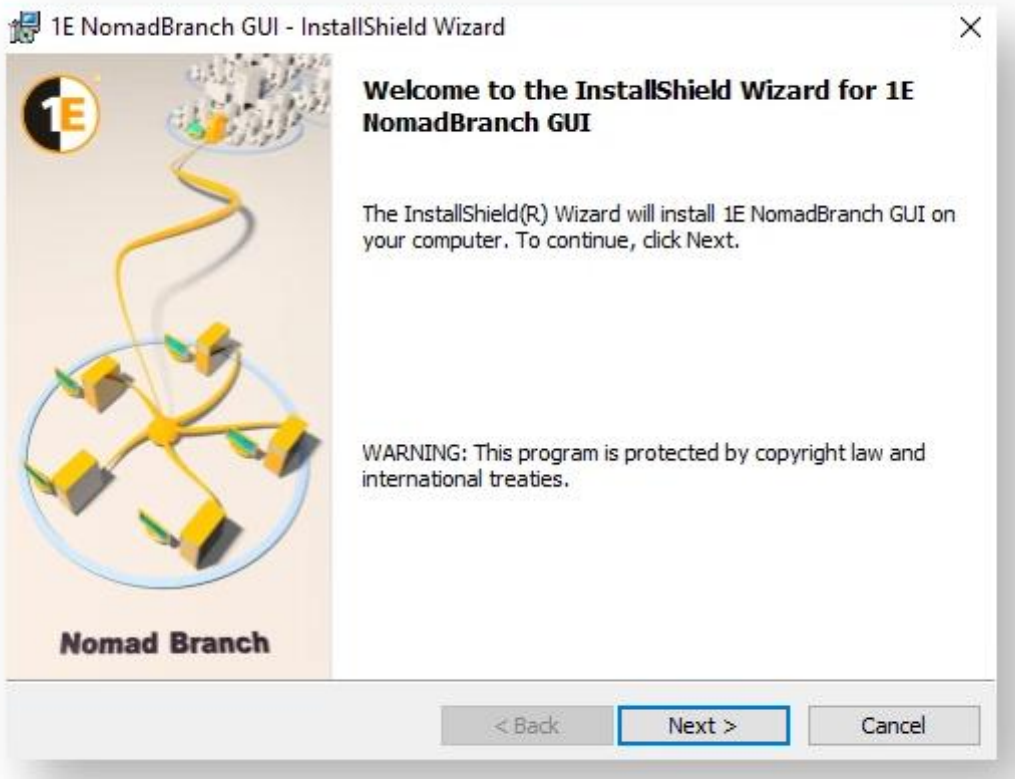
9.2.4.5.2.1.4 Ready to Install the Program

Click **Install** to start the installation process



9.2.4.5.2.1.5 Installing 1E Nomad Branch Admin Extensions

This screen shows the current progress of the installation. If a User Account Control dialog pops-up, click **Yes** to continue.



9.2.4.5.2.1.6 InstallShield Wizard Completed

If the installation has succeeded, the **InstallShield Wizard Completed** will be displayed.

Here, you can check the **Show the Windows Installer log** checkbox to view the installer log. Click **Finish** to close the installer wizard.

9.2.4.5.2.2 *Installing from the command line*

> **Note**
>
> You can download the 1E Content Distribution Tools from the **Releases** page for your platform version at https://support.1e.com/.

To install from the command line:

Extract **NomadBranchTools.msi** from the zip.

Start a Command Prompt with elevated rights, navigate to the location where you extracted **NomadBranchTools.msi** and run it with a command-line similar to the following:

```
> msiexec /i NomadBranchTools.msi /qn PLATFORMURL=https://<TCNserver> REB
OOT=REALLYSUPPRESS /l*v install.log
```

> **Note**
>
> Where <TCNserver> must be set to the DNS alias FQDN for the Tachyon server. This command-line will also enable the Tachyon integration to support the Nomad Download Pause feature.

9.2.4.5.3 Verifying installation

To confirm Nomad Branch Tools have been successfully installed, refer to:

Nomad Configuration Manager console extensions

Nomad tools for Operating System Deployment OSD.

9.2.4.5.3.1 *Nomad Configuration Manager console extensions*

To confirm the extensions have been successfully installed, start the Configuration Manager console, check Nomad extensions have been added for:

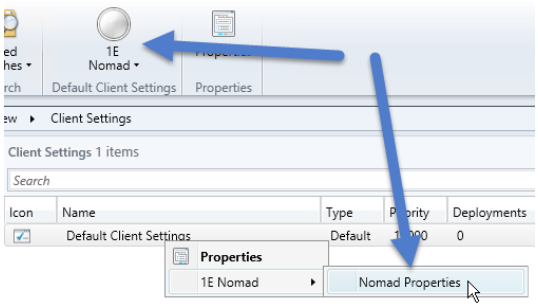
Default Client Settings

Package Properties.

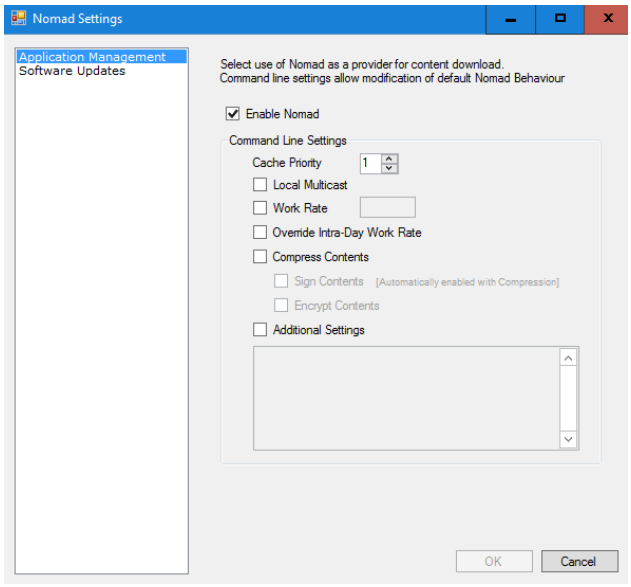
9.2.4.5.3.1.1 Default Client Settings

Open the **Administration** workspace and select the **Client Settings** node.

The ribbon has a **1E Nomad** button. Click it and choose **Nomad Properties** (as shown in the image) or, right-click the **Default Client Settings** and choose **1E Nomad→Nomad Properties**.



The **Nomad Settings** dialog allows you to configure settings for **Application Management** and **Software Updates**. Click **Cancel** to close the dialog without making any changes.

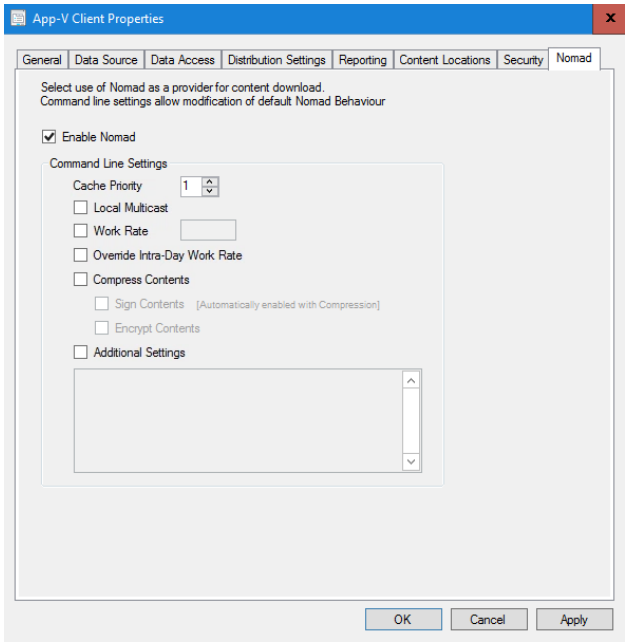


For details about the available options for setting Nomad as a download provider for applications and software updates in Configuration Manager, refer to Distributing software with Nomad and Configuration Manager and Distributing software with Nomad and Configuration Manager- Configuration Manager client settings.

9.2.4.5.3.1.2 Package Properties

Open the **Software Library** workspace and select the **Packages** node under the **Application Management** node. Right-click a package and from the context menu, choose **Properties**.

A **Nomad** tab has been added to the **Package Properties** dialog box. Click **Cancel** to close the dialog without making any changes.



For more details about the available options for setting Nomad as a content provider for Configuration Manager Packages, refer to Distributing software with Nomad and Configuration Manager - Nomad tab.

9.2.4.5.3.2 Nomad tools for Operating System Deployment OSD

If you upgrade Configuration Manager after installing the Nomad OSD tools, you will need to reinstall them as the Configuration Manager upgrade overwrites the *osdinjection.xml* and *TaskSequenceProvider.mof* files that are updated by Nomad OSD tools.

To verify that the tools have been successfully installed:

Open the Configuration Manager console.

Navigate to **Software Library→Operating Systems→Task Sequences**.

Choose an existing Task Sequence or create a temporary one. Right-click on an existing Task Sequence and click **Edit**.

In the **Task Sequence Editor**, click **Add** – note the new Nomad tasks that can be added to a task sequence.

Click **Cancel** to close the Task Sequence editor without saving any changes.

Browse to **C:\Program Files\Microsoft Configuration Manager\OSD\bin\i386** and **\x64** folders where you will find the following files:

> The page: **NMD81:@self** was not found. Please check/update the page name used in the 'multiexcerpt-include' macro.
>
> **Tip**
>
> To list the files together, you can sort by Date modified. Or you can add sort columns for Company or Product name.

Open *C:\Program Files\Microsoft Configuration Manager\bin\x64\osdinjection.xml* in Notepad.

Note

This manifest defines the files that are to be added into the Windows PE boot image when it is updated on a distribution point. The additional tools are added to this manifest, ensuring that they are included in all boot images that are updated on a distribution point from this point on.

9.2.4.5.3.2.1 Updating boot images

After installing the tools into your Configuration Manager environment, you must update any existing boot images that have been distributed to a Distribution Point or Distribution Point Group so that the tools will be included in those images.

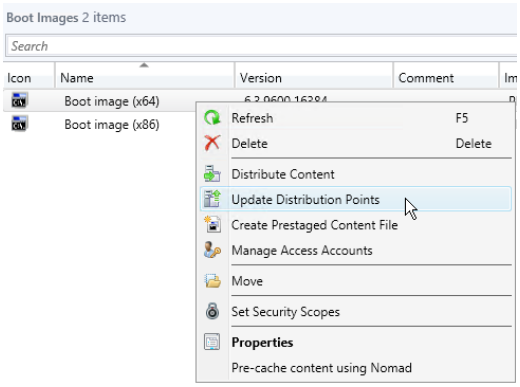
To do this:

In the Configuration Manager Console, navigate to the **Software Library** → **Operating Systems** → **Boot Images**.

Select an existing boot image.

Right-click the boot image and from the context menu, choose **Update Distribution Points**.

On the **Update Distribution Points Wizard**, click Next.



Verify that the wizard completed successfully and click **Close**. The selected boot image will now contain the latest Nomad Tools for OSD.

Repeat this process for any other boot images that are used.

9.2.4.5.4 Uninstalling Nomad Branch Tools

To uninstall Nomad Branch Tools:

Start a Command Prompt with elevated rights, navigate to the location where you extracted the ***NomadBranchTools.msi*** and run it with the following command-line:

```
> msiexec /x NomadBranchTools.msi /l*v NomadBranchToolsUninstall.log REBOOT=REALLYSUPPRESS
```

On the **Welcome** screen, click **Next**.

Click **Finish** when the uninstallation is done.

9.2.4.6 Installing the Nomad download monitor

A step-by-step guide to interactively installing the Nomad download monitor (also known as NomadBranchGUI).

9.2.4.6.1 Installing the Nomad download monitor

The Nomad branch download monitor is a tool for observing Nomad activity on either the local or a remote computer. The tool is required only for testing and troubleshooting on selected computers, and is not required or recommended for general deployment to all computers.

Generally, you only install the download monitor to administrators workstations in Advanced UI mode (UI=1) to enable them to connect any Nomad client.

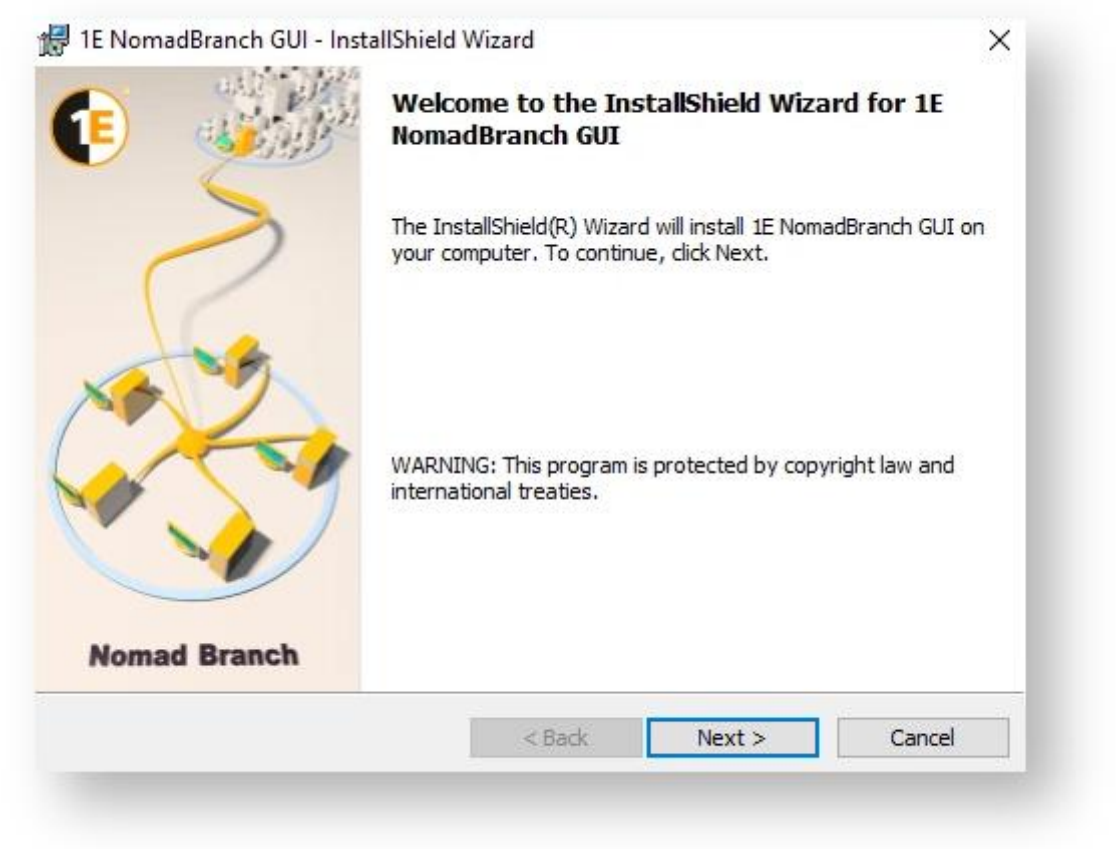
To find out more about this tool, refer to Nomad Download Monitor.

9.2.4.6.1.1 Installing interactively

The following describes each of the screens in the installation wizard, double click **NomadBranchGUI.msi**

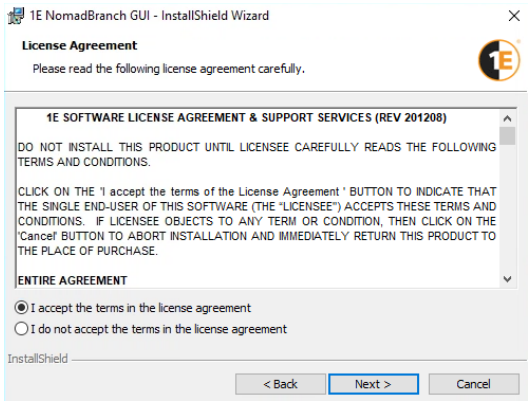
9.2.4.6.1.1.1 Welcome

The welcome screen, just click **Next** to continue.



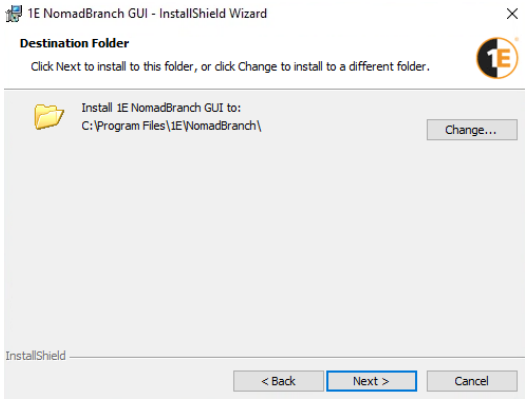
9.2.4.6.1.1.2 License Agreement

Accept the license agreement and click **Next**.



9.2.4.6.1.1.3 Destination Folder

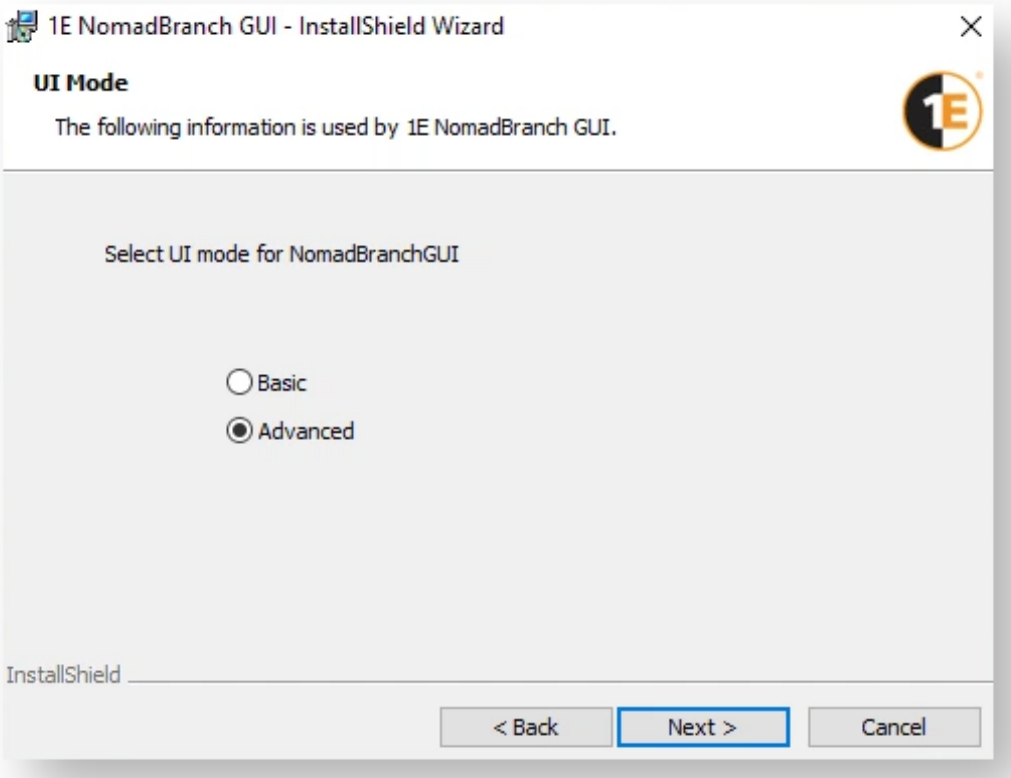
On the **Destination Folder** screen, click **Next** to accept the default location (*C:\Program Files\1E\NomadBranch* or *C:\Program Files\1E\NomadBranch (x86)*) or **Change...** to select a new location.



9.2.4.6.1.1.4 UI Mode

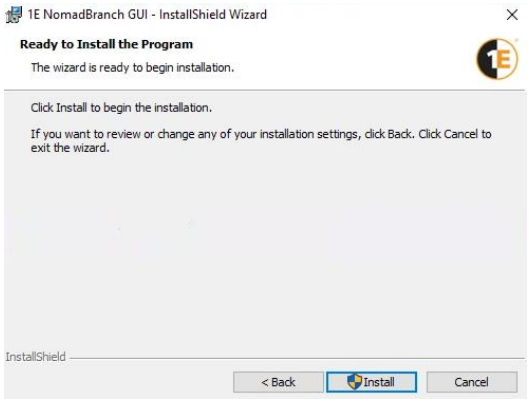
On the **UI Mode** screen, choose either **Basic** or **Advanced** mode.

Mode	Description
Basic	You will only see progress bars in the UI. Useful for those who only need to see the status of the downloads.
Advanced	You will see an extended UI – useful for administrators to troubleshooting downloads as they can connect to remote devices to view the status of the downloads, provided they have sufficient Remote Activation DCOM permissions. By default, the Download Monitor connects to the local machine.



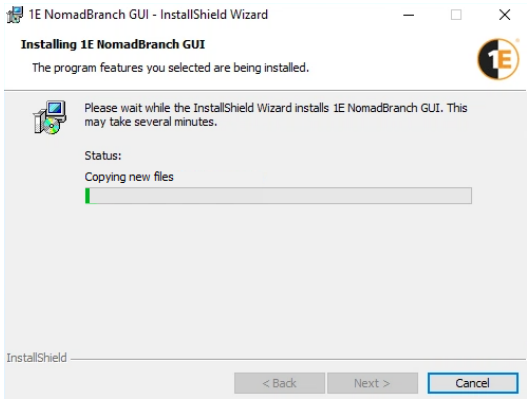
9.2.4.6.1.1.5 Ready to Install the Program

On the **Ready to install the program** screen, click **Next** to start the installation.



9.2.4.6.1.1.6 Installing 1E NomadBranch GUI

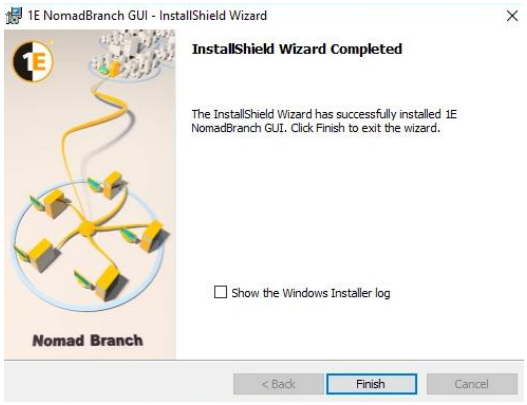
This screen shows the current progress of the installation. If a User Account Control dialog pops-up, click **Yes** to continue.



9.2.4.6.1.1.7 InstallShield Wizard Completed

If the installation has succeeded the **InstallShield Wizard Completed** will be displayed.

Here you can check the **Show the Windows Installer log** checkbox to view the installer log. Click **Finish** to close the installer wizard.



Alternatively, you can install the monitor in unattended mode. The installer has two properties which determines the behavior of the monitor:

0 – sets the UI to basic mode and is the default value

1 – sets the UI to advanced mode.

To install the monitor in basic mode in unattended mode, open a command prompt and run:

```
> msiexec.exe /i NomadBranchGUI.msi /qn
```

To install the monitor in advanced mode silently, open a command prompt and run:

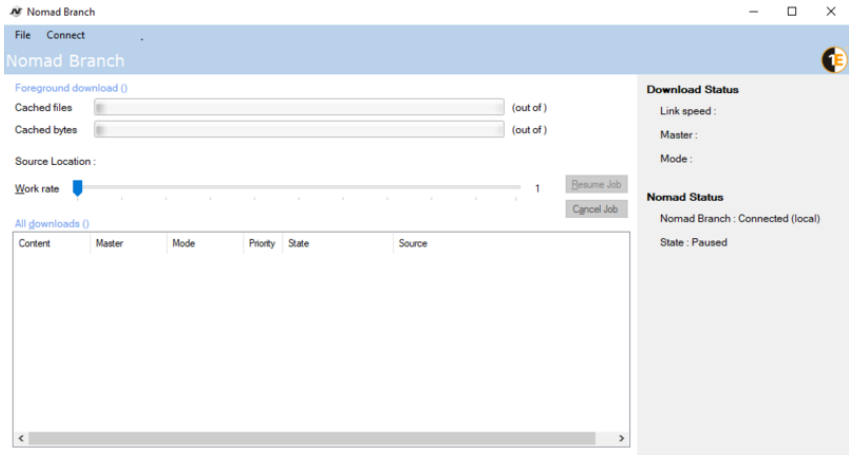
```
> msiexec.exe /i NomadBranchGUI.msi UI=1 /qn
```

9.2.4.6.2 Reviewing the installation

A status icon is added to the system tray after installation to display the download status:

Icon	Description
	Download in progress
	No downloads.

To open the download monitor, double-click the status icon. If you see the basic UI, you have installed the monitor in basic mode, if you see the expanded UI, you installed the monitor in advanced mode.

UI Mode	Displayed UI
Basic UI	
Advanced UI	

9.2.4.6.3 Changing the behavior of the monitor

You can change the behavior of the download monitor by updating its registry value after installation. The installer has two properties which determines the behavior of the monitor:

0 – sets the UI to basic mode and is the default value

1 – sets the UI to advanced mode.

To change the behavior, you can set the appropriate registry Value:

On 32-bit machines, go to *HKLM\software\1e\NomadBranch\UI*

On 64-bit machines, go to *HKLM\software\Wow6432Node\1e\NomadBranch\UI*

Note

A restart might be required when changing from advanced mode to basic mode.

9.2.4.7 Nomad post-installation tasks

Post-installation tasks that may be necessary to ensure that Nomad will work correctly in your environment.

You may need to make some post-installation configurations to your environment to ensure that Nomad works effectively. These areas may need attention.

9.2.4.7.1 Basic verification tests

For installations and upgrades:

1E Client software is installed

1E Client and **Nomad Branch** services both exist and running

Default path for Nomad Branch service is
C:\Program Files\1E\Client\Extensibility\NomadBranch\NomadBranch.exe

System PATH environment variable has been added **C:\Program Files\1E\Client\Extensibility\NomadBranch**

Open a command prompt and type the following commands (Commands are in bold, example responses below):

>**where nomadbranch**

C:\Program Files\1E\Client\Extensibility\NomadBranch\NomadBranch.exe

>**nomadbranch -version**

NomadBranch version 8.1.2.xxx (mmm dd yyyy)

Nomad registry values are as expected - using default values unless specified differently in the installer, command-line or in the MST transform file

In addition, for upgrades from Nomad 6.3.201 or Tachyon Agent 4.0 - the example is for x64 but may be for x86.

1E NomadBranch x64 / 1E Tachyon Agent x64 products are uninstalled

Tachyon.Agent service is removed

System PATH environment variable has removed **C:\Program Files\1E\NomadBranch**

After upgrade, the following Nomad registry settings are changed:

InstallationDirectory changed to C:\Program Files\1E\Client\Extensibility\NomadBranch

ProductVersion changed to 8.1.2.xxx

TachyonAgentVersionchanged to 8.1.2.xxx

9.2.4.7.2 IIS Request Filtering

By default, IIS is configured to prevent certain file types from being downloaded. You may need to configure these to allow Nomad to download all content as it does not use the Configuration

Manager workaround that Microsoft had to implement to bypass its own security feature. This is done by configuring **Request Filtering** on each website hosting the Configuration Manager DP. The example process given below does the following:

Removes file extensions from **File Name Extensions**, for example **.config**

Removes folders from **Hidden Segments**, for example **bin**

Confirms that **double escaping** is enabled, to allow files with special characters in their names, for example **+**

Microsoft introduced IIS Request Filtering in Windows Server 2008 R2 – a security feature enabling administrators to configure IIS to block requests for specific file types and URL paths that include specific folder names or special characters. By default, IIS Request Filtering blocks a number of file extensions and folder paths that may be present in normal software distribution content (packages, applications and software updates).

Although, Microsoft's documentation highlights this issue (see link below), the Configuration Manager client bypasses this security measure by using a custom method and querying for the file rather than a standard HTTP GET for it directly. Nomad does not use the same workaround but instead adheres to Microsoft's security best-practice policy of using a standard HTTP GET for the file which is filtered out by the IIS Request Filtering feature. As a result, it is necessary to remove or configure the IIS Request Filtering feature on all distribution points to allow any file extensions, paths and special characters that may exist in your Configuration Manager content.

> **Note**
>
> Microsoft IIS Request Filtering for distribution points reference - https://docs.microsoft.com/en-us/previous-versions/system-center/system-center-2012-R2/gg712264(v=technet.10)?redirectedfrom=MSDN#BKMK_RequestFiltering.

> **Note**
>
> The following examples apply to the Default Web Site. You should only configure Request Filtering at a site level or below, not at the server level.
>
> The commands also assume the Default Web Site is configured with default settings as **Allow unlisted file name extensions** and **Allow unlisted verbs** both enabled, as shown in the picture opposite.

9.2.4.7.2.1 Identifying existing restrictions

To discover files extensions and URL paths elements that are disallowed by default:

Start IIS Manager.

Locate your IIS server in the tree view and navigate to the website, for example Default Web Site.

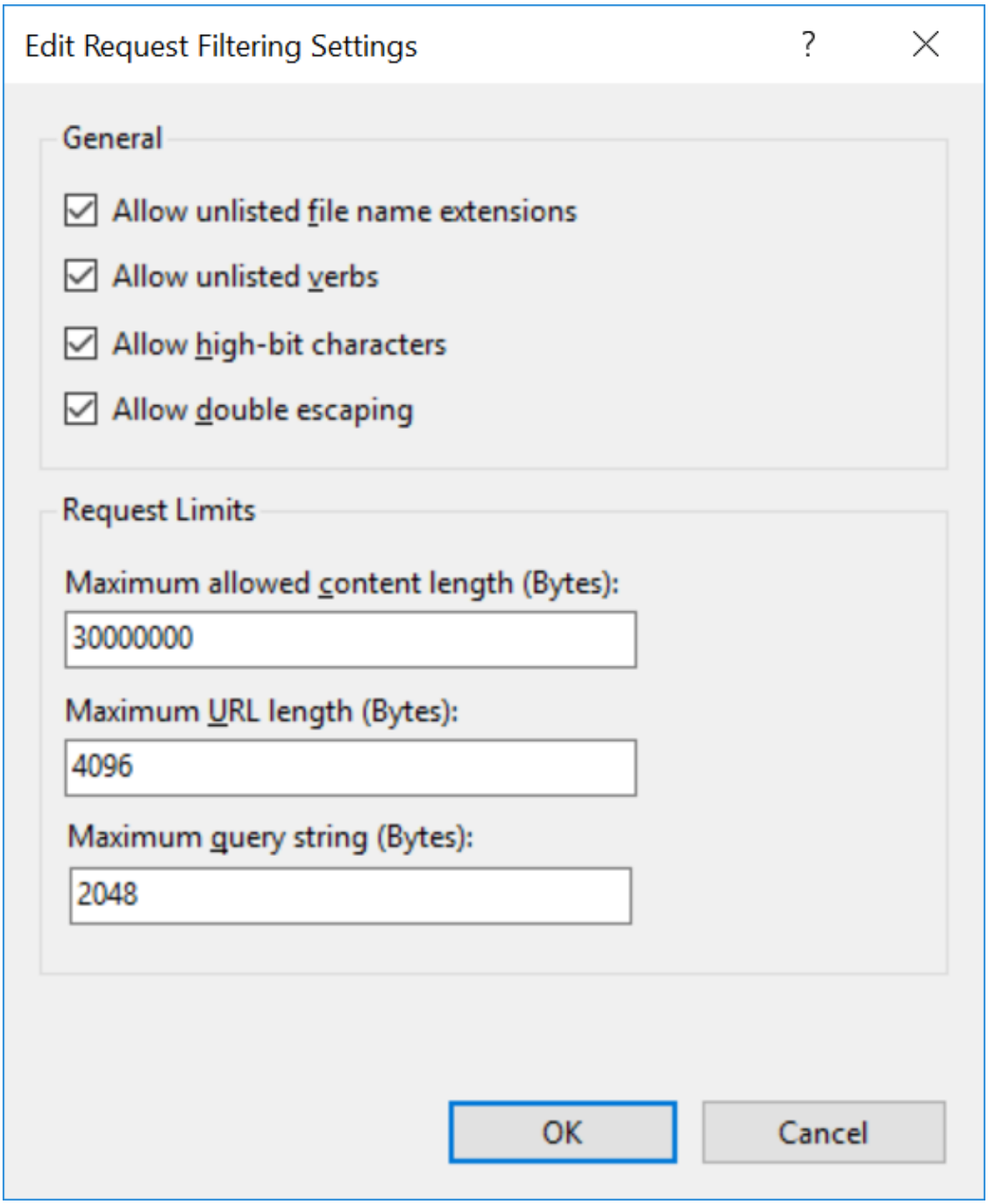
In the right pane, double-click the **Request Filtering** icon (grouped under IIS).

Click the **File Name Extensions** tab to view a list of all the file extensions that are blocked by default. Disallowed file extensions commonly found in Configuration Manager content are: *.resources*, *.mdb*, *.config*, *.java*, *.osdx*, *.skin*, *.cs*, *.vbproj*.

Click the **Hidden Segments** tab to view all the folder names that are blocked by default.

In the action pane, click on **Edit Feature Settings...**

In the **Edit Request Filtering Settings** dialog confirm that **Allow Double Escaping** is enabled.



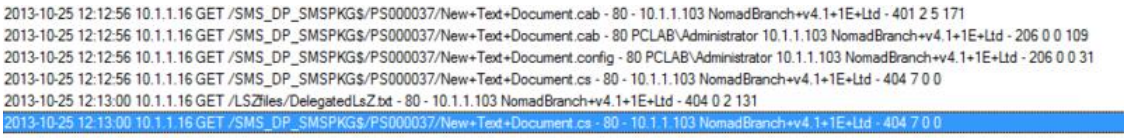
You can review the **NomadBranch.log** on clients to see details of any file types that are blocked in your download, for example:

NomadBranch.log

```
Error Reading. "path\bin\file name" - DP Path not found
TransferFiles::CopyError: "path\bin\file name" - DP Path not found
```

```
NomadBranch finished with exit code 0x205d     Job_Content_Package ID
Source : "Inaccessible DP path" Job_Content_package ID

Error Reading. "path\filename.config" - DP Path not found
TransferFiles::CopyError: "path\filename.config" - DP Path not found
NomadBranch finished with exit code 0x205d     Job_Content_Package ID
Source : "Inaccessible DP path" Job_Content_package ID

Error Reading. "path\filename++.exe" - DP Path not found
TransferFiles::CopyError: " path\filename++.exe" - DP Path not found
NomadBranch finished with exit code 0x205d     Job_Content_Package ID
Source : "Inaccessible DP path" Job_Content_package ID
```

Whilst the IIS logs for the Configuration Manager distribution points serving the Nomad download requests details the blocked files types, for example a 404.7 error:



Note

Please see http://support.microsoft.com/kb/943891 for more details about HTTP status codes, for example:

404.7 - File extension denied

404.8 - Hidden namespace

404.11 - Request contains double escape sequence.

9.2.4.7.2.2 Updating the restricted list

Now that you have discovered what file types and folders are blocked by default, you can reconfigure the filtering to allow specific the file types and folders to be used by Nomad. To update the filtering:

Start a command prompt (run as administrator).

Change directory to *C:\Windows\System32\inetsrv*

To remove a restricted file type, run:

```
appcmd set config "Default Web Site" /section:requestfiltering /-fileExte
nsions.[fileextension='.config']
```

To remove all file restrictions, run:

```
appcmd set config "Default Web Site" /section:requestfiltering /-fileExte
nsions
```

To change a file extension from restricted to allowed (change Allowed from false to true), run:

```
appcmd set config "Default Web Site" /section:requestFiltering /fileExten
sions.[fileExtension='.config'].allowed:true
```

There is more information on restricted file types at: https://learn.microsoft.com/en-us/previous-versions/orphan-topics/ws.11/hh831621(v=ws.11)

To remove a restricted folder, run:

```
appcmd set config "Default Web Site" /section:requestfiltering /-hiddense
gments.[segment='bin']
```

To remove all folder restrictions, run:

```
appcmd set config "Default Web Site" /section:requestfiltering /-hiddense
gments
```

There is more information on restricted folders at: http://technet.microsoft.com/en-us/library/hh831621.aspx#HiddenSeg

By default, any path or filename that includes special escape characters are blocked. To allow filenames or paths with special characters (double escaping) to be downloaded, run:

```
appcmd set config "Default Web Site" /section:requestfiltering /allowdoub
leescaping:true
```

There is more information on double escaping at: http://support.microsoft.com/kb/942076

Repeat the steps in Identifying existing restrictions to ensure that:

.config is not listed under **File Name Extensions**

bin is not listed under **Hidden Segments**

Note

It is likely that you may have to refresh the screen if IIS Manager is already open on the Request Filtering page.

Note

Alternatively, you can manually edit the *web.config* file for the Default Web Site normally found in *C:\inetpub\wwwroot* . It will contain only the differences between the Default Web Site and the Server configuration. IIS requires a restart for manual edits to take effect.

```
<configuration>
    <system.webServer>
        <security>
            <requestFiltering allowDoubleEscaping="true">
                <fileExtensions>
                    <remove fileExtension=".config" />
                </fileExtensions>
                <hiddenSegments>
                    <remove segment="bin" />
                </hiddenSegments>
```

```
            </requestFiltering>
        </security>
    </system.webServer>
</configuration>
```

The server configuration is stored in *%windir%\System32\inetsrv\config\applicationHost.config*.

9.2.4.7.3 Antivirus exceptions

Nomad functionality may be impaired by antivirus programs, so you may also want to configure any antivirus systems running on your network to make exceptions for the Nomad executables and support files. Although we generally advise that no malware exclusions are used, it is justifiable in certain cases to isolate specific locations and files that are used by specific software. Here is a list of exclusions that could be added for Nomad, but ensure that these are compatible with any exclusions already defined for Configuration Manager before you implement them.

9.2.4.7.3.1 Nomad installed on a DP

%SystemDrive%\ProgramData\1E\NomadBranch*.LSZ

%SystemDrive%\ProgramData\1E\NomadBranch\LogFiles\NomadBranch.log

%SystemDrive%\Program Files\1E\Client\Extensibility\NomadBranch\NomadBranch.exe

HKLM\Software\1E\NomadBranch

9.2.4.7.3.2 Nomad installed on a Configuration Manager client

%SystemDrive%\ProgramData\1E\NomadBranch*_Cache* (if the Configuration Manager cache is not excluded, do not exclude this)

%SystemDrive%\ProgramData\1E\NomadBranch*.LSZ

%SystemDrive%\ProgramData\1E\NomadBranch\LogFiles\NomadBranch.log & *.lo_

%SystemDrive%\Program Files\1E\Client\Extensibility\NomadBranch\CacheCleaner.exe

%SystemDrive%\Program Files\1E\Client\Extensibility\NomadBranch\IEMNomad.exe

%SystemDrive%\Program Files\1E\Client\Extensibility\NomadBranch\NBCacheActions.exe

%SystemDrive%\Program Files\1E\Client\Extensibility\NomadBranch\NomadBranch.exe

%SystemDrive%\Program Files\1E\Client\Extensibility\NomadBranch\NomadPackageLocator.exe

%SystemDrive%\Program Files\1E\Client\Extensibility\NomadBranch\PackageStatusRequest.exe

%SystemDrive%\Program Files\1E\Client\Extensibility\NomadBranch\SMSNomad.exe

%SystemDrive%\Program Files\1E\Client\Extensibility\NomadBranch\SMSTSNomad.exe

%SystemDrive%\Program Files\1E\Client\Extensibility\NomadBranch\TSEnv2.exe

.pdb files for each executable

HKLM\Software\1E\NomadBranch

9.2.4.8 Uninstalling Nomad

How to uninstall Nomad. Follow these recommendations if you want to reinstall Nomad instead of upgrading.

If you are uninstalling Nomad, we recommend you do it in the following order.

9.2.4.8.1 Uninstalling the Nomad app and Content Distribution

Nomad is installed and uninstalled using Tachyon setup. You can manage your Nomad installation using Tachyon setup Maintenance. You can start**Tachyon.Setup**and click directly on the**Maintenance**link in the left-hand menu. Refer to Tachyon Setup for details.

9.2.4.8.1.1 Maintenance

From this screen, you can:

Uninstall... all or part of the components deployed from Tachyon.Setup

Install, re-install or update any **Applications...**

Change the **Server certificate...** used by the Tachyon website, switches and services – or fix their bindings

Upload and apply a 1E Hotfix bundle by clicking on **Hotfixing...**

> **Note**
>
> A 1E Hotfix bundle consists of a manifest XML file containing one of commands, and hotfix files. Examples of hotfix files are MSP files and scripts.

9.2.4.8.1.2 Uninstall

From this screen, you can **uninstall** all or some of the components deployed from **Tachyon Setup**.

> **Note**
>
> **Tachyon Setup** is the recommended method of uninstalling all or individual components instead of using the Windows Control Panel.
>
> This is because Tachyon Setup can undo any changes that were done after deploying the components, which would not be undone by the standard application uninstaller.

9.2.4.8.1.3 Applications

In this dialog, you can select to install or re-install any Applications used by the Portal.

The top grid displays the Applications that are already installed and their versions.

To install or re-install applications:

Type or select a folder in the **Applications folder** field.

Click on **Show Applications**. Doing this displays all the Tachyon Applications that are found under the selected folder. The Applications are displayed using the **Name**, **Title** and **Version**.

Click on **Install Applications**. This will upload the Applications into the server:

Any new uploaded Applications are added to the server

Any uploaded Applications with a newer version number will replace the older versions

If any uploaded Application has a version number prior to an existing Application, an error message will be generated and the version will not be downgraded.

9.2.4.8.2 Configuration Manager Consoles

Close the Configuration Manager Admin Console before you uninstall the Configuration Manager Console extensions and Nomad Tools for OSD.

9.2.4.8.3 Nomad clients

If you have installed the Nomad download monitor, uninstall this before Nomad.

Ensure there are no running jobs before you uninstall 1E Client or permanently disable the Nomad client module.

Content in the cache may not be automatically deleted when you uninstall Nomad (and some MSI-based installations and files may be required for future application repairs etc). You can delete these files/folders manually or run CacheCleaner.exe -deleteall *before* you uninstall Nomad.

9.2.4.8.4 Manual uninstallation

1E Client can be uninstalled manually by using Windows Apps and Features (appwiz.cpl). A reboot is not normally required.

9.2.4.8.5 Disabling a feature or client module

Please refer to Reconfiguring 1E Client for examples of how to use the **-reconfigure** command-line to reconfigure the 1E Client.

9.2.4.8.6 Uninstallation using the Windows Installer

1E Client can be uninstalled automatically by using a Windows Installer command line, where the {product code} is dependent on the version of the 1E Client. The example below also includes switches that prevent prompting and restart and creates a log file.

```
msiexec /x {BF6F5FA9-64C8-4B72-A6B6-14A582BF96B8} /qn /norestart /l*vx C:\Windo
ws\temp\1EClient-uninstall.log
```

9.2.4.8.7 Tidy up after uninstallation

After uninstallation of 1E Client, the following is left behind. As with other Windows installers, uninstallation will leave behind any files, folders and registry entries that were created after installation.

Location	Artifacts	Recommendation
Installation folder	None.	
Logs folder	Log files remain. Please refer to Log files for log file locations of 1E Client and its client modules.	The log files can be deleted or renamed. If not deleted, then a new installation that uses the same logs folder will continue to use the old log file.
Client\Persist folder remains.	Leave this folder which contains status information about current instructions. The Persist folder should be deleted only if you do not intend re-installing the 1E Client with Tachyon enabled, or when preparing OS images.	
Tachyon client registry	HKLM\SOFTWARE\1E\Client\Persist	This registry exists if the Tachyon client feature of the 1E Client is enabled. It is used to keep a record of hash values for its persistent storage files, which includes status information about current instructions. This registry key should be deleted only if you do not intend re-installing the 1E Client with Tachyon enabled, or when preparing OS images.
Nomad Cache	%ALLUSERSPROFILE%\1E\NomadBranch	The folder should be deleted only if you do not intend re-installing the 1E Client with Nomad enabled. Downloaded content is retained so that if Nomad client is re-enabled it will be scanned and re-registered, to make it available for peer

Location	Artifacts	Recommendation
		sharing with other Nomad clients.

Note

HKLM\SOFTWARE\1E\Common and HKLM\SOFTWARE\1E\NightWatchman are used by the 1E NightWatchman Agent, previously part of the 1E Agent.

9.2.5 Upgrading Nomad

This page provides guidance on:

Upgrading to the latest version of Nomad within a Configuration Manager operating environment.

Additional guidance on upgrading ActiveEfficiency to Content Distribution.

Upgrading Configuration Manager when Nomad is in use.

Nomad 8.1 - 1E Client - Tachyon Platform

In response to customer demand to reduce the number of agents required, 1E has merged the client functionality of Nomad, PXE Everywhere, WakeUp, Shopping and Tachyon into a single 1E Client, and are merging server functionality into a single Platform.

The Nomad client is installed and enabled as a module of the 1E Client. When the 1E Client is installed with the Nomad module enabled on a device that has Nomad 6.3 or earlier installed, the previous version will be removed, and the new Nomad module will be implemented. Any custom configuration defined in the registry (for example through Configuration Baselines) will be retained. Existing Configuration Baselines will continue to work with the 1E Client. Nomad 8.1 versions of Nomad Branch Tools and Nomad Branch Admin Console Extensions are distributed and deployed in a combined installer called NomadBranchTools.

From Nomad 7.1 onward, ActiveEfficiency Server and the Nomad Dashboard are replaced by Content Distribution and the Nomad app on the Tachyon Platform.

Nomad licensing

Nomad client does not require a license key (Nomad 6.3 and earlier versions did). However, you must continue to adhere to the terms of your license agreement.

The Nomad app and Content Distribution component on the Tachyon Platform requires a Nomad license

9.2.5.1 Supported upgrade scenarios

Below is an overview of three basic upgrade and migration scenarios for customers who already have ActiveEfficiency Server.

In-place upgrade of ActiveEfficiency Server to Tachyon Platform

In-place upgrade of Tachyon Platform

Installation or upgrade of Tachyon Platform side-by-side an existing ActiveEfficiency Server

The overall objectives are:

Continued support of the following Nomad features that were supported by ActiveEfficiency Server:

Single Site Download (SSD)

Pre-caching

Single Site Peer Backup Assistant

Nomad Download Pause

ConfigMgr Computer Association.

Continued support of downlevel (old) clients during the phased upgrade of clients as CD upgrades from an existing AE.

9.2.5.1.1 Upgrading Nomad only

In this scenario, Nomad is upgraded separate from any Configuration Manager Current Branch upgrade. This is the simplest and most common scenario that typically occurs when you want to keep your software current, take advantage of new features and improvements in the latest versions, or your current version is nearing end of support. In some cases, new features in Nomad may require your ActiveEfficiency server to be upgraded or additional solutions such as Tachyon to be implemented.

> **Product Support Lifecycle**
>
> For details of the support lifecycle of each of the 1E Products, refer to https://support.1e.com/.

Upgrading Nomad involves upgrading the server, tools and console components first before upgrading Distribution Points and finally clients. Nomad is generally backward compatible and unless otherwise stated in the product documentation, existing features will be supported by the new version. 1E realizes the importance of compatibility to maintain client operations during the upgrade process.

Nomad 7.1 onward uses the Tachyon Platform to provide Content Distribution and Dashboard features. Content Distribution replaces ActiveEfficiency Server. Content Distribution continues to provide legacy features for legacy (before 7.1) Nomad clients, which function independently alongside new Nomad clients. To install or upgrade to Tachyon Platform, either from ActiveEfficiency or from Tachyon, please refer to Upgrading to Tachyon Platform. If you are currently using Active Efficiency Server it will either be upgraded to Tachyon Platform, or be decommissioned in the side-by-side scenario.

To upgrade clients, 1E recommends using the 1E Client Deployment Assistant. The CDA creates Packages, Applications, empty Collections and Deployments with custom Windows Installer transforms to simplify the installation and initial configuration of the 1E Client and its modules. You can then simply add devices into the

Collections to upgrade Nomad on those devices. CDA is required if you are installing or upgrading PXE Everywhere.

If previous versions of Nomad have been deployed as an Application in Configuration Manager, you should define supersedence on the Application that installs the new version so that it supersedes the previous versions. This is very important, as it prevents attempts at downgrading Nomad through Application Deployment Enforcement if there are still active deployments for the previous versions.

Upgrading Nomad may also require updates to existing Task Sequences. Existing Nomad Task Sequence steps will continue to work after upgrade, but it may be necessary to remove and replace them after upgrade to implement any fixes or improvements included in the new version.

Important

It is advised that before starting any Nomad upgrades, you should stop services to your CM database before you start the upgrade.

9.2.5.1.2 Upgrading Configuration Manager

Configuration Manager (CM) Current Branch (CB) is updated three times a year. In most cases, updates to Configuration Manager do not affect core Nomad functionality. 1E endeavor to test all supported versions of all products and release a support statement within 30 days of General Availability ('slow ring') of a CM CB release. If any issues are identified, 1E will endeavor to fix the issue within the 30-day period, provide a workaround or communicate when the issue is expected to be resolved. Any such fixes will usually be implemented as a hotfix (that will be rolled into future versions) rather than an upgrade.

1E Support for CM CB releases

Before upgrading Configuration Manager, refer to https://1eportal.force.com/s/support-for-msft-rapid-release-cycle to confirm your currently installed versions of Nomad and ActiveEfficiency are supported on the new CM CB version.

If your currently installed versions of Nomad and ActiveEfficiency support the version of CM that you are upgrading to, you can go ahead and upgrade CM. Even though your currently installed versions are supported, you may like to take this opportunity to upgrade to the latest versions, or at least apply the latest hotfixes, to keep your software current. In that case, upgrade CM first, then update / upgrade Nomad and ActiveEfficiency accordingly, following the process for upgrading Nomad only.

If your currently installed versions of Nomad or ActiveEfficiency do not support the version of CM that you are upgrading to, you will need to update (hotfix) or upgrade them before upgrading CM.

NomadBranchTools and OSDInjection.xml

CM upgrades are likely to overwrite the OSDInjection.xml file that defines the files that are injected into Windows PE boot images. Nomad Branch Tools updates OSDInjection.xml to include the Nomad binaries that need to be added to the boot image. After upgrading CM you should uninstall and reinstall Nomad Branch Tools on the CM site server and any remote SMS Providers to ensure the Nomad binaries are included next time the boot image is redistributed.

9.2.5.1.3 Side-by-Side Migration of Configuration Manager and Nomad

If you are implementing a new Configuration Manager hierarchy with the intention of migrating devices from a separate hierarchy to the new hierarchy. Nomad Branch Tools and Nomad Admin Console Extensions would need to be installed in the new hierarchy. If those devices to be migrated already have a version of Nomad installed that is supported on the CM version of the new hierarchy, they can be migrated to the new hierarchy with no further changes needed to Nomad. If the currently installed version of Nomad is not supported on the new hierarchy's CM version, you will need to upgrade Nomad before migrating clients to the new CM hierarchy.

If ActiveEfficiency is being used in the old hierarchy you have two options.

Reconfigure the existing ActiveEfficiency server to synchronize with the new CM hierarchy. This option has the benefit of retaining SSD site definitions and historical data for content distribution and pre-caching. If package objects have been migrated from the old hierarchy, thereby retaining their content ID, this option will also enable clients that have not been migrated to share content with those that have across subnets (using SSD). However once ActiveEfficiency is synchronizing with the new CM hiearchy, you will no longer be able to manage pre-cache jobs from the old hierarchy and the dashboard will only be updated with activity from clients reporting into the new CM hierarchy.

Implement a new ActiveEfficiency server configured to sync with the new hierarchy. As clients are migrated to the new hierarchy, they should be reconfigured to report to the new ActiveEfficiency server. Pre-caching, SSD and dashboard reporting can be managed independently from each hierarchy until all clients are migrated to the new hierarchy.

9.2.5.2 Preparing for Upgrade

You should include the following steps in your preparation for upgrading:

Step	Action	Details
1	Review how you are currently using Nomad	The new Nomad client is a module of 1E Client, which also includes clients for Tachyon, PXE Everywhere, Shopping/WSA and WakeUp. Confirm which components you have implemented and where (clients, Nomad Branch Tools, Nomad Admin Console Extensions, ActiveEfficiency) Confirm which features you are currently using (SSD, FanOut, PBA etc.) and ensure your current configuration settings are recorded. Be aware that newer versions of Nomad may change the default values of some configuration settings. In most cases the original settings will be preserved when Nomad is upgraded, however it is important that

Step	Action	Details
		new clients are deployed with a configuration that is compatible with existing (upgraded) clients. Identify any clients that have a special Nomad configuration. For example, you might consider some clients to be sensitive and consequently have adjusted their Nomad election weighting so that they never become Nomad masters. You should review whether there are any such exceptions and incorporate them in your plan accordingly If you are using PXE Everywhere, identify.
2	Familiarize yourself with the features that have been introduced and other differences between your currently installed version and the new version.	Check the Nomad features by release page in the Nomad documentation Check the Preparation and Requirements pages in the Nomad documentation as there may be new requirements and some versions of Windows, CM and SQL Server may no longer be supported. Determine how the new features can benefit your organization and then learn the details to make them effective. You may prefer to wait for the upgrade to complete and settle down before enabling new features.
3	Check if any hardware upgrades or new hardware are required for any new features you intend to implement (for example, Tachyon is required for the Nomad Download Pause feature) and plan for these sufficiently in advance.	n\a
4	Obtain the latest software versions and hotfixes from the 1E Support Portal	n\a
5	Review CM health. You will be using CM to deploy the upgrade to clients, so any effort in ensuring CM is	n\a

Step	Action	Details
	functioning well will ease the upgrade.	
6	Plan your upgrade	You should have a lab or pre-production environment that closely reflects your production environment to test your upgrade process before going into production. Document an upgrade plan and validate it in the lab or pre-production environment. Validation should include all features that you are currently using. Where practical, upgrade all clients on a subnet at the same time. This minimizes the potential for version-specific issues such as hash or election differences (specifically when taking advantage of newer Nomad features such as the Cloud DP and CMG support functionality). Nomad elections are subnet based, so any Nomad client on the subnet could respond to another Nomad client, regardless of Nomad version or Configuration Manager differences. If the Configuration Manager clients that Nomad is installed on are the same version and reporting to the same hierarchy then issues related to Configuration Manager differences are avoided. Start small. Build Collections for pilots. The wider upgrade can be deployed to a Collection of all clients with the old version installed. As clients are upgraded they will move out of the Collection. Validate each stage before progressing to the next stage. Things to check: The correct versions are now in place Configuration Manager hardware and software inventory reports can confirm this Core functionality is working – downloads over the WAN and peer-to-peer content distribution

Step	Action	Details
		Manual inspection, including log reviewing, is ideal to confirm this in the early stage The Nomad Dashboard can confirm it on a broader scale Core scenarios are working – deployment of the various content types you use, representative operating systems and hardware Nomad Dashboard can be used for this No negative side effects Thorough lab testing is important Stay alert to help desk incidents and other means of reporting anomalous behavior All components are upgraded – clients, Nomad Configuration Manager Admin Console UI components and ActiveEfficiency as appropriate to your environment Configuration Manager hardware and software inventory reports can confirm this as well Secondary functionality and scenarios are working as desired Status reporting for OSD deployments or similar efforts provides this Server workloads do not change unexpectedly, and the server performance continues to be acceptable at all times Standard server monitoring and alerting After all clients are targeted with your Nomad client upgrade, the targeting collection will become smaller (since it is targeting clients that are not the correct version). It may take some time to become empty due to clients that are offline

Step	Action	Details
		A few collections will be involved, so use manual inspection in the Configuration Manager console.
7	Follow your upgrade plan in the production environment	n\a

9.2.5.3 Upgrade Sequence

The upgrade process presented within this document implements three simple maxims

If you are upgrading Configuration Manager and your currently installed versions of Nomad or ActiveEfficiency are not supported on the new CM version, you must upgrade these before upgrading CM

If you are upgrading Configuration Manager and Nomad at the same time and your currently installed versions of Nomad and ActiveEfficiency are supported on the new version of CM, upgrade CM first then upgrade Nomad and ActiveEfficiency

Upgrade server components before clients.

The figures below describe the principal processes and the sequence of steps involved when performing an upgrade. Described, is the logical progression of an upgrade process based upon the following possible scenarios:

Nomad only upgrade

Configuration Manager only upgrade

Configuration Manager and Nomad upgrade

Side-by-side migration of Configuration Manager and Nomad.

9.2.5.3.1 Upgrading Nomad and / or Configuration Manager

If you are only upgrading CM and your currently installed versions of Nomad and ActiveEfficiency support the new version of CM, follow Microsoft documentation to upgrade CM then reinstall the Nomad Branch Tools and redistribute the boot images.

If you are upgrading CM and your currently installed versions of Nomad or ActiveEfficiency are not supported on the new version of CM, follow the process below for upgrading Nomad first, then follow Microsoft documentation to upgrade CM.

Use the following process to upgrade Nomad.

9.2.5.3.1.1 Install or upgrade Nomad server components

If you are going to introduce features that require additional infrastructure (e.g. SSD, Dashboard and Pre-caching require ActiveEfficiency, Download Pause feature requires Tachyon), install these first as you will need to specify the server names when upgrading the Nomad Admin UI extensions and 1E Client

Upgrade the existing Nomad server components as follows:

ActiveEfficiency (optional component for SSD, Dashboard and Pre-caching)

Tachyon (optional component for real-time client management)

Nomad Admin UI extensions (on Site Servers and remote CM consoles)

Nomad Branch Tools (on Site Servers and SMS Providers)

Nomad on Distribution Points. Use the 1E Client installer to upgrade to Nomad 8.1 on DPs.

Hotfix required

If you are using ActiveEfficiency, Nomad 8.1 requires ActiveEfficiency 1.10 (or later) with the latest accumulated hotfix.

9.2.5.3.1.2 Update Task Sequences

Existing Task Sequence steps will continue to work after upgrading Nomad. However, the following steps should be updated in due course after upgrading the Nomad Admin UI extensions and Nomad Branch Tools.

Current step	Changes	
Install and Configure Nomad in WinPE	Before 7.1	7.1 and onward
	ActiveEfficiency URL Legacy clients will continue reporting to the ActiveEfficiency Server. If this has been upgraded and replaced by Content Distribution, then legacy clients will use HTTP	1E Platform Background Channel URL List This is a list of URLs containing each of the Tachyon Platform Background Channels in your organization and is normally the same list as used by your 1E Client devices. Please refer to #UUID4b0c8700283e161c086960470cc47bc0_id_TachyonclientsettingsBackgroundChannelUrl. **Note** Nomad clients connect to Content Distribution via Tachyon Switches and a proxy feature of Background Channel. **Tip** Any attempt to edit and save a Task Sequence for the first time using the new version of the Admin UI extensions will fail and prompt for this field to be completed.

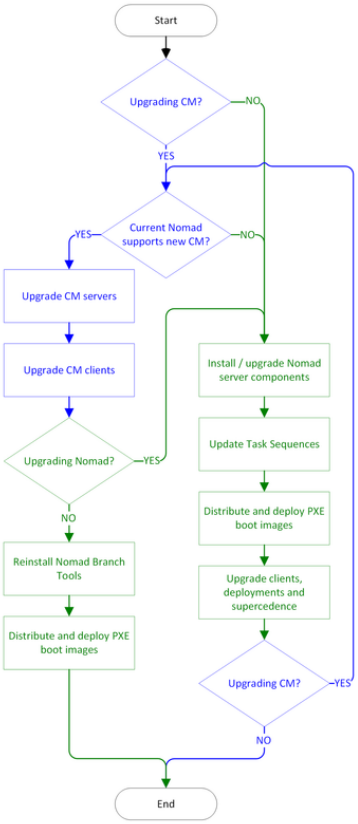
Current step	Changes	
	Redirection feature and continue to work.	
	Max. machines from ActiveEfficiency	Max. machines from 1E Platform
	WakeUp (Local only)	These settings have been removed. Content Distribution does not provide integration with WakeUp.
	WakeUp batch size	
Stage Nomad Package Only if you are upgrading from a version of Nomad earlier than Nomad 8.1	Remove the step and replace it with **Stage 1E Client Package** , and reference the 1E Client package created earlier.	
Install Nomad Only if you are upgrading from a version of Nomad earlier than Nomad 8.1	Remove the step and replace it with **Install 1E Client** . Before you remove the old step, make a note of any **Additional installation commands** in the existing step properties, and decide if you need to add them to the new step. **Installer Properties** Note that the installer property names in the 1E Client installer that relate to Nomad are different from the property names in previous versions of the Nomad installer. Generally, the original property name is prefixed with MODULE.NOMAD, but some have changed and there are new properties available since Nomad 7.0. Refer to Nomad installer properties for full details. If you are using Client Deployment Assistant to deploy the 1E Client, you should check to see if that has already configured your settings for you.	

9.2.5.3.1.3 Distribute and deploy PXE boot images

Nomad Branch Tools updates the Nomad files that are injected into Windows PE boot images. After upgrading Nomad Branch Tools, right-click existing boot images and select Update Distribution Points. CM will then generate an updated boot image, incorporating the updated Nomad files, and update it on DPs to which the boot image was previously distributed to. You will then need to deploy the updated boot image to any PXE Everywhere clients (see Preparing and deploying 1E PXE Everywhere boot images).

9.2.5.3.1.4 Upgrade clients

The 1E Client installer is used to upgrade from Nomad 6.3 to Nomad 8.1. 1E recommends using the Client Deployment Assistant (CDA) to create deployment objects (Applications, Packages, Collections and Deployments) in CM that can be used to roll out the client upgrade. The Applications and Packages created by CDA include Windows Installer transforms (.MST files) that configure the 1E Client according to options selected in the CDA.



Supported Upgrade path

The 1E Client supports upgrading from Nomad 6.3.100 and 6.3.201. Nomad 6.2 is now out of support. If you are still running Nomad 6.2, you will need to upgrade to Nomad 6.3.201 before upgrading to Nomad 8.1 with the 1E Client.

Application Supersedence

If you use Configuration Manager Applications (rather than Package) to deploy Nomad and still have active Application deployments for previous versions of the Nomad client, be sure to either:

delete those deployments

or define supersedence on the 1E Client Application such that it supersedes all Applications that install older versions of Nomad.

This will prevent Configuration Manager attempting to downgrade Nomad, which can leave the client in an unstable state.

9.2.5.3.2 Side-by-side Configuration Manager migration

When performing a sire-by-side Configuration Manager migration, you will need to perform a number of tasks in the new hierarchy to get Nomad up and running. The steps below summarize the process.

9.2.5.3.2.1 Build new CM hierarchy

Follow Microsoft documentation to build the new CM hierarchy.

9.2.5.3.2.2 Migrate CM objects as required

This is an optional step. You may choose to migrate some or all of your packages and other objects from your old hierarchy rather than recreating them manually in the new hierarchy. This has the added benefit of retaining content IDs, which means that Nomad clients assigned to the new hierarchy will be able to source content for those migrated packages from peers still assigned to the old hierarchy.

9.2.5.3.2.3 Install Nomad server components

You will need to install the Nomad server components in the new hierarchy as if installing Nomad for the first time.

ActiveEfficiency (optional component for SSD, Dashboard and Pre-caching). See Side-by-Side Migration of Configuration Manager and Nomad for options with ActiveEfficiency

Tachyon (optional component for real-time client management)

Nomad Admin UI extensions (on Site Servers and remote CM consoles)

Nomad Branch Tools (on Site Servers and SMS Providers)

Nomad (1E Client) on Distribution Points.

9.2.5.3.2.4 Distribute and deploy PXE boot images

Nomad Branch Tools updates the Nomad files that are injected into Windows PE boot images. After upgrading Nomad Branch Tools, right-click existing boot images and select **Update Distribution Points**. CM will then generate an updated boot image, incorporating the updated Nomad files and update it on DPs to which the boot image was previously distributed to.

You will then need to deploy the updated boot image to any PXE Everywhere clients (see Preparing and deploying 1E PXE Everywhere boot images).

9.2.5.3.2.5 Use CDA to create 1E Client deployment objects in new hierarchy

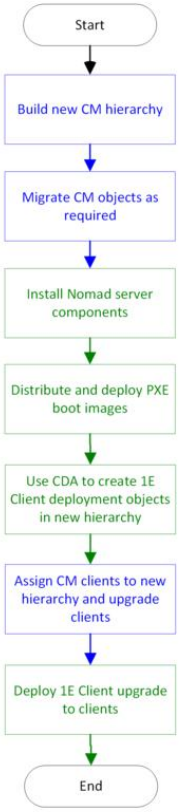
1E recommend using the Client Deployment Assistant (CDA) to create deployment objects (Applications, Packages, Collections and Deployments) in CM that can be used to roll out the 1E client to new clients in the new hierarchy and also to upgrade existing clients if they are on Nomad 6.3, and you wish to upgrade them to Nomad 8.1. The Applications and Packages created by CDA include Windows Installer transforms (.MST files) that configure the 1E Client according to options selected in the CDA. If you chose to implement a new ActiveEfficiency server in the new hierarchy, remember to specify the new server when running the CDA in this environment.

9.2.5.3.2.6 Assign CM clients to new hierarchy and upgrade clients

Follow the Microsoft documentation to assign CM clients to the new hierarchy and upgrade the CM client if appropriate.

9.2.5.3.2.7 Deploy the 1E Client upgrade to clients

If you are upgrading Nomad as you migrate clients to the new hierarchy, deploy the 1E Client application to upgrade them. If you used the CDA to create the deployment objects, simply add devices to the Collection created by CDA to upgrade them.



9.2.5.4 Upgrade FAQ

9.2.5.4.1 Client Upgrade FAQ

This section will attempt to answer some common questions related to upgrading the Nomad client.

Application Supersedence

If you use Configuration Manager Applications (rather than Package) to deploy Nomad and still have active Application deployments for previous versions of the Nomad client, be sure to either:

delete those deployments

or define supersedence on the 1E Client Application such that it supersedes all Applications that install older versions of Nomad.

This will prevent Configuration Manager attempting to downgrade Nomad, which can leave the client in an unstable state.

Question	Answer
What versions of Configuration Manager does Nomad support	Refer to Supported Platforms. **Product Support Lifecycle** For details of the support lifecycle of each of the 1E Products, please refer to the 1E Support Portal (https://1eportal.force.com/apex/ProductLifeCycleSupportMaintenance).
How do I upgrade?	Follow the process described above.
Do I need a new license key when I upgrade Nomad?	No. Old versions of Nomad required a license key, but a license key is not required to install 1E Client with Nomad enabled. However, your organization must still buy a license to use Nomad.
Why use the 1E Client Deployment Assistant during the upgrade?	The Client Deployment Assistant (CDA) was developed to allow easy installation and configuration of all 1E Client modules and the PXE Everywhere client. CDA includes all the client installation packages and is updated and released alongside new client releases. CDA is an installation wizard that guides you through the configuration creation and deployment of Applications and Packages that install the 1E Client modules (Nomad, WakeUp, Shopping and Tachyon) and the PXE Everywhere and NightWatchman clients. The CDA is designed to speed up client

Question	Answer
	deployment and ensure consistency of their configuration with the CDA providing a set of recommended configuration settings that can be changed either through the wizard or by editing the AppImport.xml file and running CDA in unattended mode. For more information on how to use the CDA, refer to Introducing 1E Client Deployment Assistant.
During an upgrade, are my customized registry settings preserved?	Yes. All upgrades will preserve the Nomad registry settings, as well as any content that exists in the Nomad Cache. However, it is recommended that users always deploy the upgrade using their desired transform (MST) in order to ensure that any existing clients that may be misconfigured are brought into line. Users should consult new release documentation in order to understand the settings related to implementing new features present in the release.
Are Nomad 8.1 clients backward compatible with previous versions?	Yes. Nomad 8.1 is backward compatible with Nomad 6.3. Older versions of Nomad are no longer supported.
Do I need to upgrade my clients at once?	It is recommended that you endeavor to upgrade clients by subnet where practical. Mobile clients moving from on-premises to Cloud DP locations should be upgraded as soon as possible. For customers not using Cloud DPs and mobile clients, it is generally not necessary to upgrade a set of particular clients at once. 1E always makes sure Nomad clients are backward compatible in terms of being able to download and share new and existing content between clients of different versions.
If you need to upgrade both the Configuration Manager and Nomad clients, which is done first?	The best practice is to upgrade the Configuration Manager client prior to the Nomad client. The exception is when the currently installed Nomad agent does not support the new version of CM. Under normal operation, Nomad is designed to instantly recognize and remediate if it is not configured as the Alternate Content Provider (ACP) for the Configuration Manager client. When upgrading the Configuration Manager client or Nomad client, no additional steps are required to make sure Nomad remains configured as the ACP.

Question	Answer
	The one exception is when the Nomad client installation is run on a host that does not have the Configuration Manager client installed. In this case, if installing the Configuration Manager client after installing Nomad, then you will need to perform a restart of the NomadBranch service for successful ACP registration. As a precaution, *if reinstalling both agents clients*, it is recommended that the Configuration Manager client is always installed/upgraded before Nomad.

9.2.5.4.2 Content FAQ

This section will attempt to answer some common questions related to Nomad content during a 1E Nomad upgrade.

Question	Answer
What happens to my existing cached content when I upgrade?	An upgrade of the Nomad client does not delete content from the Nomad cache. Similarly, an upgrade to the Configuration Manager client will not result in content being deleted from its cache. The new Cache Optimization (CO) feature introduced in Nomad 6.3 is turned off by default. CO allows content to be automatically purged from the cache based upon the last time it was copied by a peer or downloaded – whichever came last.
Does Nomad support the use of shared DPs during a side-by-side migration?	Yes, for a shared environment, provided the content version is consistent between the old and new site/hierarchy, the content locations will be supplied to the Nomad client by the Configuration Manager client and accessed by Nomad in the usual way. This is true for native Configuration Manager deployments as well as Nomad Pre-caching when the Nomad client performs its own content request. The Nomad client installed on the shared DP will continue to function as normal.
For a side-by-side migration, can existing cache content be used in the new infrastructure?	Yes. Migrating objects in Configuration Manager is performed using migration jobs and content identifiers are maintained after migration. This means all content metadata gathered by the Nomad client in the old hierarchy will be valid in the new.

Question	Answer
When performing a side-by-side migration, will Nomad reuse cached software updates?	Yes, the software update identifiers and metadata generated by Nomad in the source site remains valid in the new hierarchy.
When performing a side-by-side migration and executing Configuration Manager migration jobs, are Nomad settings preserved on migrated content?	For packages, no. Users must manually configure the Nomad settings on their migrated content in the new site. This can be automated by running a post migration script in order to set the required Nomad properties. Because of this, it is recommended that deployments are set to disabled in the package migration jobs. For applications and software updates, this is not a concern since the setting to use Nomad is made in the Configuration Manager Client Settings policy, rather than against individual pieces of content.

9.2.5.4.3 Content Distribution FAQ

This section will attempt to answer some common questions related to ActiveEfficiency and Content Distribution when upgrading Nomad.

Question	Answer
When upgrading ActiveEfficiency are custom configuration settings preserved?	No. Prior to upgrading, it is recommended to take note of any customizations. If you have customized settings such as IIS bindings or changed the *service.exe.config* file, then these will need to be reapplied after the upgrade.

9.2.5.4.4 Operating System Deployments FAQ

This section will attempt to answer some common questions related to OSD when upgrading Nomad.

Question	Answer
Is there a new version of PXE Everywhere released with Nomad 8.1?	No. PXE Everywhere 4.0 is the latest version, released earlier in 2019.

Question	Answer
Do I need to recreate my PXE boot images after the upgrade?	Unless you are upgrading the Windows ADK, you do not need to recreate your Nomad enabled PXE boot images. Admins do however need to update and deploy their boot images to include updated Nomad 8.1 program files when upgrading the Configuration Manager site server, SMS provider components, or the Nomad Branch Tools. Updating is achieved by simply redistributing the boot image package using the Configuration Manager console. The PXE boot image must then be re-deployed to your PXE Everywhere endpoint agents.
Do I need to update my OSD task sequences after the upgrade?	1E are always looking for ways to simplify and enhance our customer's OSD experience and will often release new built-in task sequence steps as part of a Nomad release. 1E recommends that whenever possible, users take advantage of any new task sequence steps and update their task sequences accordingly. If users wish to retain the configuration of their existing task sequences, then the older steps will typically remain supported, unless otherwise stated in the release documentation. Where existing steps are supported into the latest release, no action is required on existing task sequences once the Nomad Branch Tools and Configuration Manager Admin Console UI extensions have been upgraded. Configuration Manager admins are then able to open and edit their existing task sequences, and they will continue to function in the same way.

9.2.5.5 Upgrading to Tachyon Platform

Guidance for upgrading Tachyon, SLA, and ActiveEfficiency platforms to Tachyon Platform.

Before you attempt an upgrade, please ensure you thoroughly read all sections that apply to you. Combine the steps if your system matches multiple upgrade scenarios. If you cannot find a complete match, please contact 1E.

Refer to Upgrading to Tachyon Platform for full details.

9.2.5.6 Upgrading to 1E Client

Guidance for upgrading Tachyon and other legacy 1E agents to 1E Client. This page contains detailed steps for upgrading Tachyon Agent and a summary of considerations for upgrading other legacy agents. The 1E Client contains clients for 1E products and solutions, and their upgrade documentation should be consulted before upgrading their clients and agents.

For full details, refer to Upgrading 1E Client.

9.2.5.7 Nomad upgrade checklist

Quick checklist for upgrading Nomad and PXE Everywhere.

Main Step	Step Outline
Upgrade Tachyon Platform	Upgrade Tachyon Platform (or upgrade from ActiveEfficiency Server to Tachyon Platform).
Prepare 1E Client installation files	Use the1E Client Deployment Assistant 8.0 (CDA) wizard to create applications, collections, deployments and packages for the 1E Client in Configuration Manager. The Nomad client is now part of the 1E Client, and you must enable the Nomad client module of the 1E Client during installation. The1E Client 8.0 documentation also explains how to deploy the 1E Client with the Nomad client module enabled. Before running the CDA wizard, review AppImport.xml. Subject to the settings required in your organization, make changes to the file as appropriate. If the settings available in the wizard or AppImport.xml do not cover those that need to be configured within your organization, customize the automatically generated MST as described in the 1E Client Deployment Assistant (CDA) documentation. (Re)Distribute the 1E Client application and package contents to all DPs.
Upgrade Nomad on the Primary Site server	Extract the Nomad ZIP file onto the server Upgrade NomadBranchTools Upgrade NomadBranchAdminUIExt Upgrade Nomad client by installing 1E Client

Main Step	Step Outline
Upgrade Nomad on the Distribution Point server(s)	Upgrade the 1E Client with Nomad enabled on all the Distribution Point servers (before upgrading clients).
Upgrade Nomad on test client(s)	Create a test collection and deploy the 1E Client application or package to one computer – to test successful deployment.
Upgrade Nomad on all clients	Create a new deployment or use application supersedence to upgrade client computers.
Update/Create Compliance Baseline	(Optional) Update an existing Compliance Baseline, or use the new Nomad Baseline Wizard to create a new Compliance Baseline/configuration items by importing your 1E Client 5.1 MSI/MST. If you are updating an existing baseline, review specific Nomad settings (such as BLOCKSIZE=131072) making sure you only deploy this to Nomad clients.
Update 1E PXE Boot Image(s)	Update your 1E PXE Boot Image(s) by right-clicking the Boot Image and selecting “Update Distribution Points” - this will recreate the Boot Image and automatically inject the updated Nomad binary files into the Boot Image. Create a new deployment of your specific Task Sequence to pre-stage the Boot Image onto PXE Everywhere clients. Ensure you select the Rerun behavior to “Always rerun program” and the Deployment Option of “Download all content locally before starting the task sequence”. **Note** Nomad will only download the block differences (that is, deltas), so your clients won’t be

Main Step	Step Outline
	downloading the entire Boot Image all over again.
Update OSD Task Sequences (with new Nomad package) and Pre-Cache new Nomad package	If you already have OSD Task Sequences, then you'll need to update the **Stage Nomad Package** or **Stage 1E Client Package** step to point towards the new Nomad client installation package. The new 1E Client installation package will need pre-caching to remote clients, usually already setup by the Nomad Pre-cache Wizard. In the background, the content from the old 1E Client installation package to the new 1E Client installation package will automatically be cached onto clients after updating your OSD Task Sequences, but this can take up to 24 hours. You can speed this up by manually initiating the Nomad Sync (*C:\Program Files (x86)\1E\ActiveEfficiency\Service\ServiceHost.exe -NomadSyncAll* on the AE server), and then perform the *NomadBranch.exe -precache* command on remote clients.

9.2.6 Verifying

Basic verification tests that cover the installation and basic use of Nomad. Depending on the decisions you have made during the design phase of your implementation, you may need additional tests to verify your Nomad implementation.

> **Note**
>
> Please ensure you complete all verification tests. They not only confirm your system is operational, but they also introduce you to concepts and tasks that you will use later when using Nomad.

9.2.6.1 Basic verification tests

To run these tests you need, for installations and upgrades:

1E Client software is installed.

1E Client and **Nomad Branch** services both exist and running.

Default path for Nomad Branch service is
C:\Program Files\1E\Client\Extensibility\NomadBranch\NomadBranch.exe

System PATH environment variable has been added **C:\Program Files\1E\Client\Extensibility\NomadBranch**

Open a command prompt and type the following commands (Commands are in bold, example responses below):

>**where nomadbranch**

C:\Program Files\1E\Client\Extensibility\NomadBranch\NomadBranch.exe

>**nomadbranch -version**

NomadBranch version 8.1.2.xxx (mmm dd yyyy)

Nomad registry values are as expected - using default values unless specified differently in the installer, command-line or in the MST transform file.

In addition, for upgrades from Nomad 6.3.201 or Tachyon Agent 4.0 - the example is for x64 but may be for x86.

1E NomadBranch x64 / 1E Tachyon Agent x64 products are uninstalled.

Tachyon.Agent service is removed.

System PATH environment variable has removed **C:\Program Files\1E\NomadBranch**

After upgrade, the following Nomad registry settings are changed:

InstallationDirectory changed to C:\Program Files\1E\Client\Extensibility\NomadBranch.

ProductVersion changed to 8.1.2.xxx

TachyonAgentVersionchanged to 8.1.2.xxx

9.2.6.2 Platform verification tests

You should run basic verification tests If you have installed the platform as part of your Content Distribution installation.

Platform verification tests should be run in series. They start with basic server checks, then testing 1E Clients, and finally using the verification instructions from the **1E-Tachyon-Platform** Product Pack to do end-to-end tests that confirm all components are working. Depending on the decisions you have made during the design phase of your implementation, you may need additional tests to verify your implementation.

To run these tests you'll need:

Tachyon Server installed.

Remote workstation with a supported browser.

The name and password for the **server installation account**.

The AD account must be enabled.

The account may already be assigned to other platform roles either directly or using membership of an AD group role.

Two AD User accounts, **Test User 1** and **2**.

Must not be existing platform users because they will be assigned specific roles for the purpose of these tests.

Must have email addresses and be able to read emails.

The **1E-Tachyon-Platform** instruction set with two verification instructions.

The verification steps describe how to create this instruction set by uploading the 1E Tachyon Platform Product Pack.

You may have already uploaded this pack using the Product Pack Deployment Tool, either during Setup or after.

The 1E Tachyon Platform pack is included in the **TachyonPlatform zip** file that you can download from the 1E Support Portal https://support.1e.com/.

At least one test device on which the 1E Client will be installed.

1E Client installation source files and configuration details required by your platform implementation.

Basic verification tests cover a single-server installation of Tachyon Server. These tests only cover the platform and do not verify the configuration of 1E client modules with other 1E products. For details refer to Verifying.

9.3 Using Nomad

How systems administrators use Nomad to deploy software, software updates and operating system upgrades.

9.3.1 Deploying software with Configuration Manager

Scenarios for deploying Applications and Packages where Nomad is integrated with Configuration Manager.

Nomad integrates with the Configuration Manager (CM) client content download process. When Nomad is installed, it registers with the Configuration Manager client as an Alternate Content Provider (ACP), which means the CM client will use Nomad as an alternative to BITS when it requires content if Nomad is enabled for the requested content object. Nomad can be enabled on individual packages (including Driver Packages, Operating System Images, Operating System Upgrade Packages and Boot Images) and Task Sequences.

For Applications and Software Updates, Nomad is enabled on each client for all Applications and Software Updates through Default Client Settings. When the CM client requires Nomad-enabled content, it passes a request to Nomad, which in turn downloads the content, places it in the CM client cache and passes back to the CM client for execution. The 1E Client (with Nomad client module enabled) must be installed on all CM client machines and on all Distribution Points (DP).

Refer to Distributing software with Nomad and Configuration Manager for more information about how Nomad works with Configuration Manager. For example, Nomad supported CM content sources and the types of content Nomad can act as a content provider for.

To enable the Configuration Manager client to interpret Nomad settings and ensure Content Transfer Manager hands-over to Nomad to download content, we need to extend the standard software deployment and client settings policies associated with packages, applications and software updates. The additional Nomad attributes are configured through the Configuration Manger console by way of custom console extensions, which add properties pages to the standard package, task sequence and client settings dialog boxes and wizards.

To find out more, refer to Installing Nomad Branch Tools.

> **Note**
>
> You can use the Nomad app, powered by the Tachyon Platform to get a visual snapshot of download activity in your environment. The Nomad app will be available after you install the Tachyon Platform and can be accessed using the Tachyon DNS Alias FQDN, for example https://tachyon.acme.local/Tachyon
>
> The section Monitoring Nomad on this page provides an overview of how you can use the app to view download progress for large and small scale deployments.

9.3.1.1 Enabling Nomad for Application Management

Nomad is enabled or disabled for all Application deployments through the Client Settings. In our example we will enable Nomad for Application Management in the **Default Client Settings** and see how Nomad takes part in the download process and shares the content.

In our example in Configuration Manager:

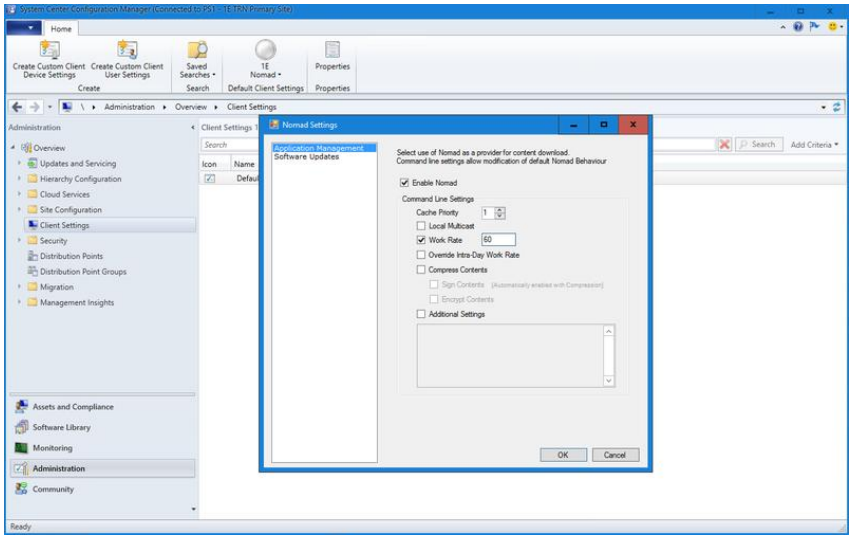
We select the **Administration** workspace and choose the **Client Settings** node.

Then click **Default Client Settings** in the right-hand pane and select **1E Nomad→ Nomad Properties** from the displayed Ribbon.

In the Nomad Properties dialog box, we select **Application Management** on the left and make the following changes.

Check **Enable Nomad**

Check **Work Rate (%)** and set the value to **6 0**.

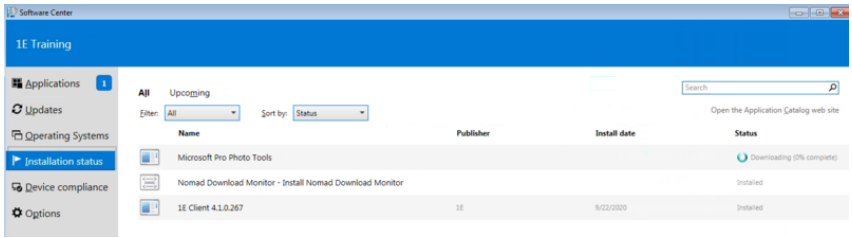


In this example, we will deploy **Microsoft Pro Photo Tools** to our collection containing our workstations called **Workstations**. Because we have enabled Nomad for Application Management, Nomad will be used to obtain the content for these clients when executing the deployment.

We then created a deployment for **Microsoft Pro Photo Tools** to our computers using the default deployment settings, but making sure on the **Deployment Settings** page we set the **Purpose** to **Required.**

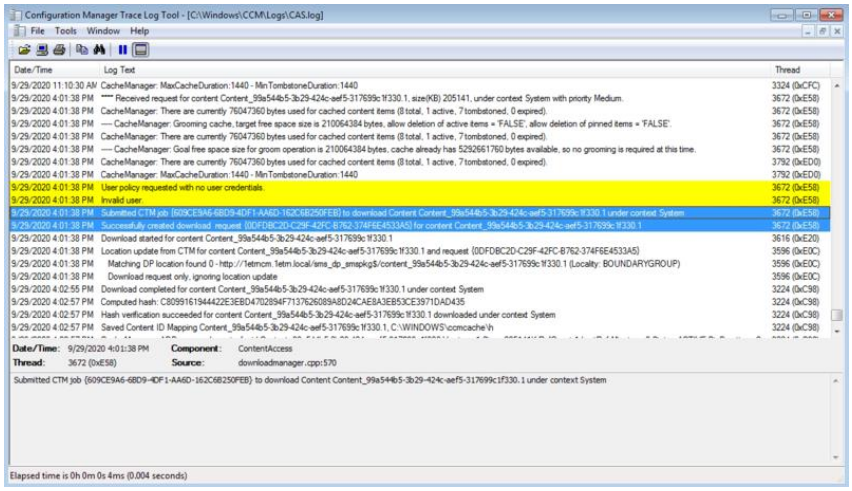
9.3.1.1.1 Tracing the Application download progress

We then observe the computers as they receive the Software Updates policy and begin to download the content. Using **Software Center** we can see the content being downloaded.

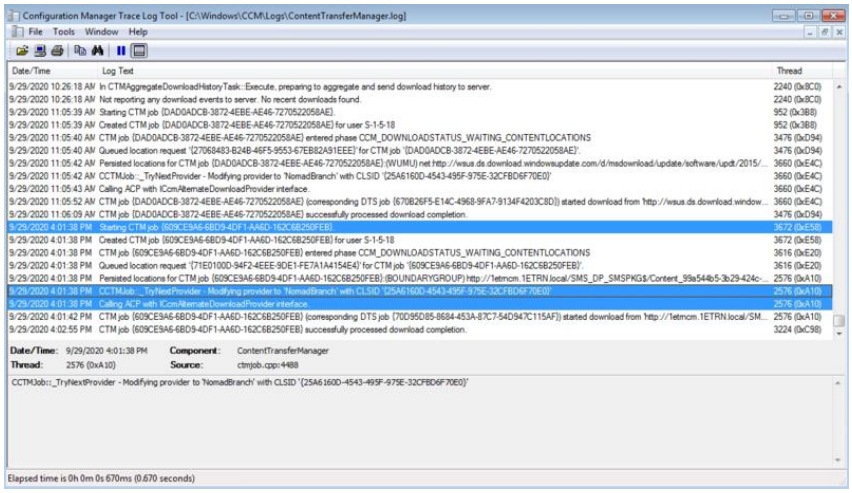


On **1ETRNW71** Using CMTrace.exe we open the **CAS.log** from **C:\Program Files\SMS_CCM\Logs** and can Identify the point when the content request is initiated.

We do this using the Application's Content ID: **Content_99a544b5-3b29-424c-aef5-317699c1f330**



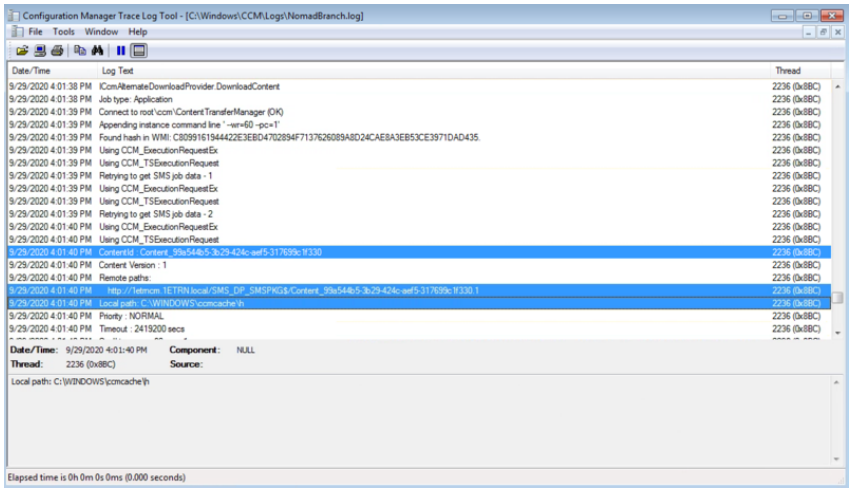
In the **ContentTransferManager.log** we can see where the CTM job started and that the Content Transfer Manager modifies the content provider to NomadBranch.



We look at the **NomadBranch.log** and identify the point where Nomad is called by the Content Transfer Manager as the Alternate Content Provider.

Note

The log extract shows the **ICcmAlternateDownloadProvider.DownloadContent** being called when the ContentTransferManager modified the provider to NomadBranch.



In the **NomadBranch.log** we can also see where the 1E Client names the Nomad options we defined in the Application Management section of Nomad settings.

We can identify the point where the list of available content locations presented to Nomad appears.

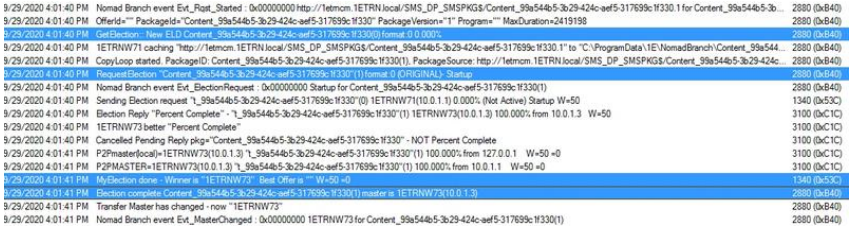
There is also a point where the election starts, and we can identify that **1ETRNW73** wins the election.

> **Note**
>
> Nomad ensures that software packages are only ever copied once per branch over the WAN, utilizing local computers as temporary file caches to distribute the software locally. This reduces the bandwidth required for delivering software updates and means that small offices or sites connected by poor network links can receive software updates more reliably.
>
> The Nomad clients with local copies of the package can themselves act as the master if the need arises. This significantly reduces the number of Configuration Manager servers required to manage a Configuration Manager hierarchy, thereby reducing initial and ongoing maintenance costs.
>
> Refer to Download once to branch for full details about Nomad elections work including:

Nomad master elections

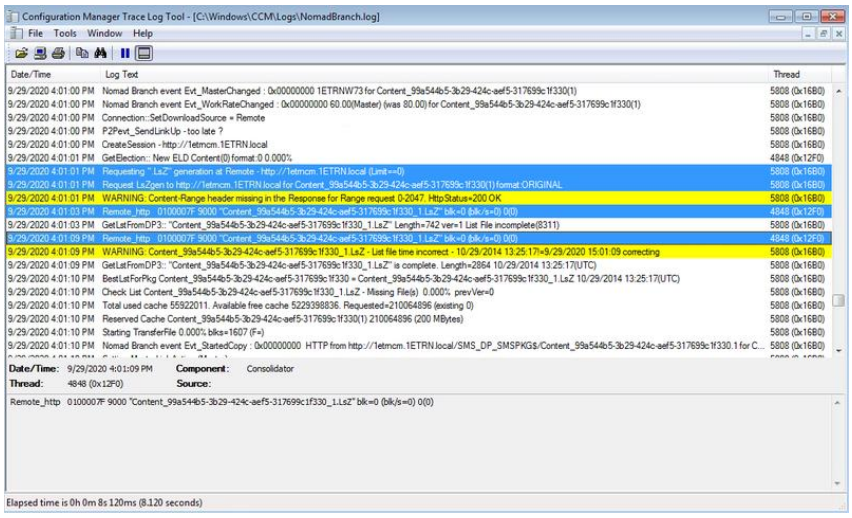
Nomad cache

Election rules and master elections.

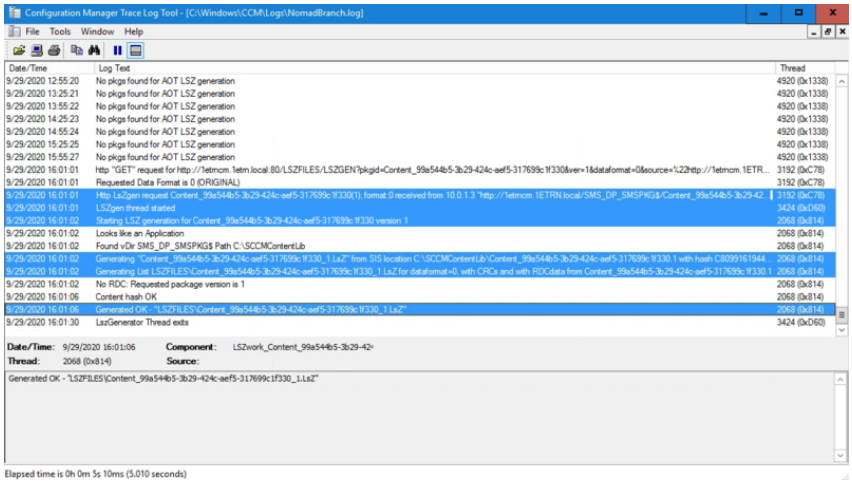


Because the elected master is **1ETRNW73** we switch to this computer and look at the NomadBranch.log, we then identify where the elected master requests the LsZ Manifest file to be generated on the DP.

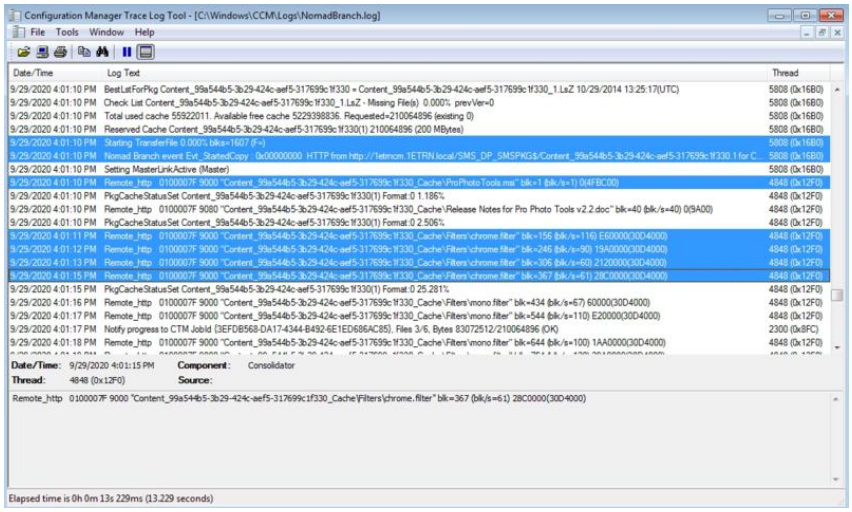
> **Note**
>
> The manifest, a *LSZ* file, is stored in the root of the Nomad cache. This lists each file, its time stamp, a CRC checksum and the Configuration Manager hash value for the content. Nomad uses this manifest to ensure that the correct files have been downloaded for each package and to enable the rapid detection of changes between versions of packages.



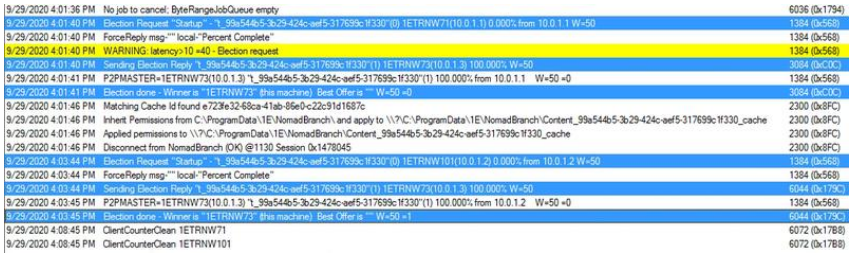
We switch to our Configuration Manager Server and open **c:\Windows\CCM\Logs\NomadBranch.log** where we can identify the point where the agent on the DP intercepts the request and generates the LsZ file.



By switching to the elected master **1ETRNW73** it's possible to track the download of content from the DP. This is highlighted by **Remote_http**.



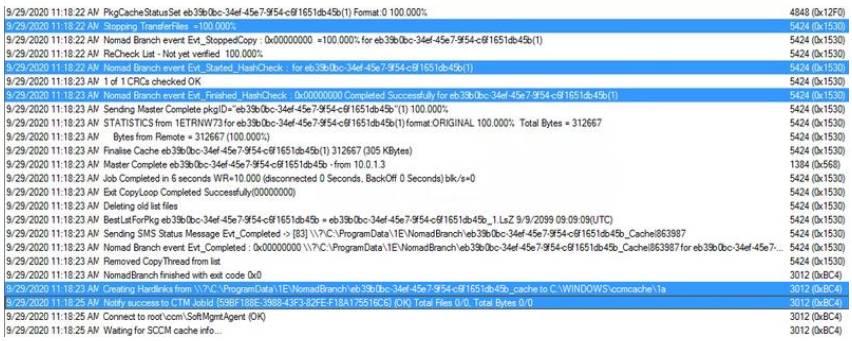
On the same computer **1ETRNW73** we can see other clients initiating an election as they process their content request.



Finally we can see the point where the master completes the download and performs the content hash check.

Note

The **STATISTICS** log entry indicates that this client (the master) got 100% of the content from the DP. The hardlinks are created shortly afterwards.



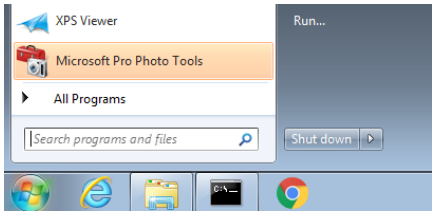
Once this process is complete **Microsoft Pro Photo Tools** is installed and available from the start menu.

Note

You can also use the Nomad app in the Nomad app to get a visual snapshot of download activity in your environment. The Nomad app will be available after you install the Tachyon Platform, it can be accessed using the Tachyon DNS Alias FQDN. For example:

https://tachyon.acme.local/Tachyon

See the section Using the Nomad app for an overview of how you can use the app to view download progress for large and small scale deployments for Content Titles and by device.



9.3.1.2 Enabling Nomad for Package Deployments

While you can use the same settings for all Applications, settings for Packages must be defined for each package you want to deploy.

Nomad can be set as a content provider for individual instances of the following types of Configuration Manager (CM) content. In the Configuration Manager Console, navigate to **Software Library**→**Overview** and then to one of the following:

CM Console node	Sub-node	Action
Application Management	**Packages**	Select a package.
Operating Systems	**Driver Packages**	Select a driver package.
Operating System Images	Select an operating system image.	
Operating System Upgrade Packages	Select an operating system upgrade package.	
Boot Images	Select a boot image.	
Task Sequences	Select a task sequence.	

Right-click and select **Properties**or click on**Create** to start a **New Wizard**. Nomad properties is then accessible on the **Nomad** tab.

In our example we will deploy a Package called **Phonebook** to the computers in our collection.

In Configuration Manager:

We select the **Software Library** workspace and choose the **Application Management**→**Packages** node.

We right-click the Phonebook package in the right-hand pane and select the**Nomad** tab from the displayed properties.

On the Nomad Properties tab, we select make the following changes:

Check **Enable Nomad**

Check **Work Rate (%)** and set the value to **10** we slow the rate to 10 to make the deployment easier to follow.

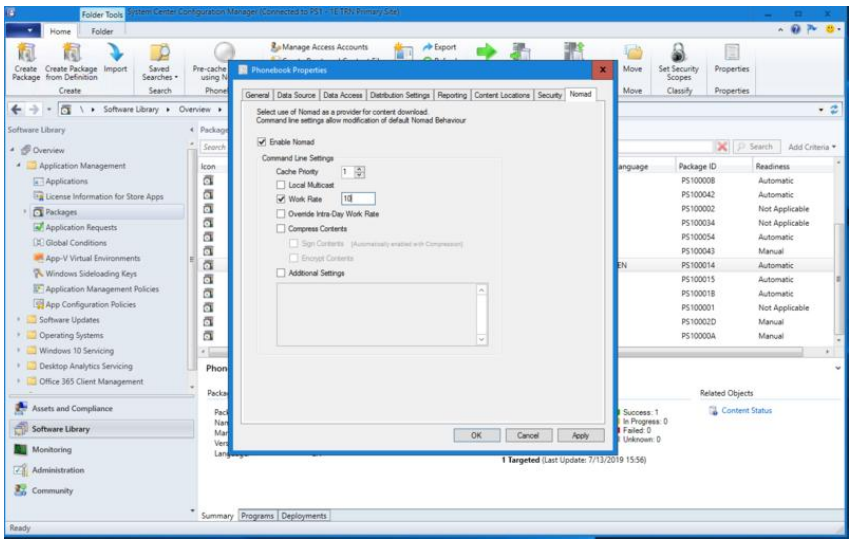
> **Note**
>
> Work Rate (%) – determines the percentage of available bandwidth to use for the download. The default value is 80%. If you have set intra-work rates, (the lower of these two values is used unless you enable the Override Intra-Day Work Rate option. Please refer to MaxWorkRates for details about intra-day work rates.

We then deploy the Phonebook Package to our workstations using the default deployment settings, but making sure we have set:

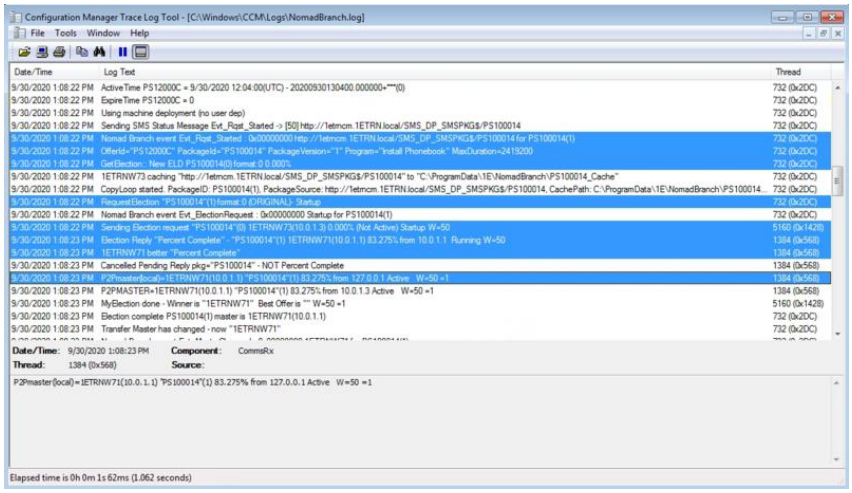
Deployment Settings - Type of deployment is **Required**

Scheduling - Create an assignment schedule of **Assign immediately after this event** with the deadline **As soon as Possible**

Distribution Points - we set both to **Download content from distribution point and run locally**.



On **1ETRNW73** Using CMTrace.exe we open the **NomadBranch.log** from **C:\Windows\CCM\Logs** and Identify the election for the Phonebook Package which has a content ID of **PS100014**.



When the master is elected the computer starts copying from the master, refer to Download once to branch for details about Nomad elections.

The method for deploying Packages is the same as for Applications and software updates, as detailed in Tracing the Application download progress.

9.3.2 Deploying software in large networks

Scenarios for deploying software in large networks, introducing FanOut and Single-Site Download (SSD).

Our environment is configured to represent two distinct locations (a datacenter and a remote office), with the servers all located in the datacenter and the computers are all located in the remote office. It just so happens that the remote office has two subnets.

In our example, we'll use Single Site Download, which enables a 1E Client to obtain content from a peer in an adjacent subnet (within the same defined location) if that content is not available on a peer in its own local subnet.

We'll then enable FanOut and watch when this feature is enabled to allow multiple 1E Clients to serve content simultaneously within the same subnet instead of relying on a single elected master. In our example computers with a name ending in an odd number are in subnet 10.0.1.0, while those with a name ending in an even number are in subnet 10.0.2.0.

> **Note**
>
> Not only is Nomad aware of the file level differences between different versions of a package so that only changed files are downloaded, it is also aware of the differences within individual files.
>
> This is sometimes known as binary differential replication or binary deltas but is more commonly known as remote differential compression (RDC) integration, for details refer

to https://docs.microsoft.com/en-us/previous-versions/windows/desktop/rdc/about-remote-differential-compression.

Note

You can use the Nomad app, powered by the Tachyon Platform to get a visual snapshot of download activity in your environment. The Nomad app will be available after you install the Tachyon Platform and can be accessed using the Tachyon DNS Alias FQDN, for example https://tachyon.acme.local/Tachyon

The section Monitoring Nomad on this page provides an overview of how you can use the app to view download progress for large and small scale deployments.

9.3.2.1 Using Single-Site downloads to deal with multi-subnet sites

Nomad's Single Site Download (SSD) feature ensures a download across the WAN only happens once per site. It does this by maintaining information about which subnets are neighbors of each other (accessible on LAN rather than WAN), so that when an elected master considers a download from a DP rather than a peer in its subnet, it can discover which other local subnets already has the package. These subnets are typically at a single customer site, specifically a single geographical location.

Nomad SSD uses Content Distribution. When a Nomad client downloads a package, it registers this information with Content Distribution, enabling a profile to be created on which Nomad clients hold particular packages.

Before enabling Nomad clients to use SSD, you need to ensure the following:

Tachyon Platform 5.2 or later is installed and running successfully

The Content Distribution database is populated with information about sites and their associated subnets

9.3.2.1.1 High-level overview of how to enable SSD

The following information applies to both new and existing installations of Nomad:

Make sure that Tachyon Platform is installed in your environment and is used as a content location metadata repository, for more information refer to Introducing Tachyon

Within Content Distribution, populate the SSD sites and subnet information. A sample PowerShell script called **PostADSitesandSubnets.ps1** is included in the Nomad installation files, which reads sites and subnets from AD

Nomad captures a list of background channels from the 1E Client in the BackgroundChannelUrl and uses the first working URL as the PlatformURL by appending /Proxy/ContentDistribution/ if this PlatformURL is unreachable it attempts to connect to the next BackgroundChannelUrl, for details about BackgroundChannelUrl refer to Nomad architecture

Enable SSD on all Nomad agents, by modifying **HKLM\Software\1E\NomadBranch\SSDEnabled** to 3, this enables SSD for both "Provide" and "Consume" modes, specifically Nomad will provide content to other peers and consume content from other peers

If you already have Nomad installed and are only now enabling SSD, then ensure **HKLM\Software\1E\NomadBranch\Platform\ContentRegistration** is set to 1, in other words, Nomad will register downloaded content with Content Distribution, this is automatically enabled for new installations of Nomad and SSD.

Tip

If you have clients on networks where broadcasts are disabled (for example wireless) then enable local SSD by setting SSDEnabled=7. Also set ContentProviderOnWifi=1.

9.3.2.1.2 Building a subnet profile in Content Distribution

For Content Distribution to build a subnet profile for SSD and the peer backup assistant feature, Nomad must communicate with its web service. When the Nomad service starts, it connects and registers the hosting device by name with Content Distribution, which returns a device ID in the form of a GUID that enables it to uniquely identify the Nomad client and its default subnet. If it is unable to communicate with Content Distribution, it retries every 5 minutes until it succeeds (as long as SSD is enabled). An attempt to communicate with Content Distribution is also made prior to a package download to register its status.

Please refer to Enabling SSD in WinPE to make use of Nomad SSD in OS Deployment.

The following points should be noted:

On a multi-NIC host, only one NIC gets registered, and a wired interface takes precedence over a wireless interface during registration

If Nomad fails initially to register an adapter, it retries every 5 minutes (for as long as SSD is enabled) until it succeeds

Wireless adapters can be configured to act as SSD content providers and consumers. Use the ContentProviderOnWiFi registry setting to do this

If the initial device registration was successful when the Nomad service started, but Content Distribution later becomes unavailable, when Nomad subsequently downloads and caches a package it will not be able to register the package with Content Distribution (see below for details). Nomad does not re-attempt package registration, so Content Distribution will not know that this particular Nomad host has the package.

9.3.2.1.3 Example PowerShell scripts

You can get information about sites and subnets from AD, or by other means. Example PowerShell scripts can be used for retrieving information about sites and their associated subnets from the AD and updating the Content Distribution database.

Example Active Directory Single Site script — Sample script that scans the Active Directory (AD) environment for all sites and subnets and stores the information in the Content Distribution locations table.

Example Single Site script — Sample script that provides two functions to update sites and subnets in the Content Distribution locations table: DeleteAllLocations and AddLocation().

Example Location Discovery script — Sample script to enable and disable the location discovery feature, along with the option to run it and load site, subnet and information in Content Distribution.

Content Distribution purge configuration script — Sample script to view or update Purge Configuration in the Content Distribution Service defined in the ContentDistribution PurgeSettings table if it is configured.

9.3.2.1.4 Enabling a Nomad package for Single-Site downloads

Nomad is enabled or disabled for each Configuration Manager package in**Configuration Manager**, **Software Library** workspace, **Packages** node. In our example we will enable Nomad for legacy package and see how Nomad takes part in the download process and shares the content.

> **Note**
>
> If you enable Single Site Download when you install the 1E Client, you only need to define the **SSDENABLED** and **PLATFORMURL** installer properties. However, if you enable the feature after installation through modification of the registry, you must also explicitly set the **ContentRegistration** value to 1.

In this example, we will configure a legacy package to use Nomad and then deploy it to our example Workstations Collection.

Before deploying our package, we are going to amend the Work Rate for our deployment. The Work Rate determines the percentage of available bandwidth to use for the download.

In this example we have changed this from the default 80% of available bandwidth to 10% to slow down the deployment and so making it easier to monitor.

For more details about the Nomad tab, and how you can use Work Rates, refer to Distributing software with Nomad and Configuration Manager - Nomad taband Design Considerations: Setting intra-day work rates.

In our example in Configuration Manager:

We select the **Software Library** workspace and choose the **Packages** node.

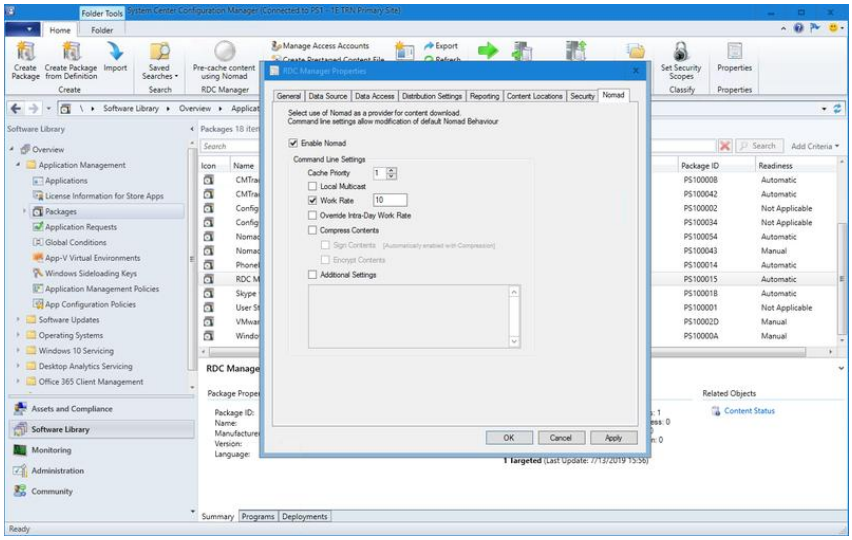
Then right-click the **Remote Desktop Connection Manager (RDCMan)** package in the right-hand pane and select the **Nomad** tab.

In the Nomad Properties dialog box, we check:

Enable Nomad

Work Rate (%)and set the value to**10**.

Once this is done, we force a policy update on the collection containing our workstations called **Workstations**.

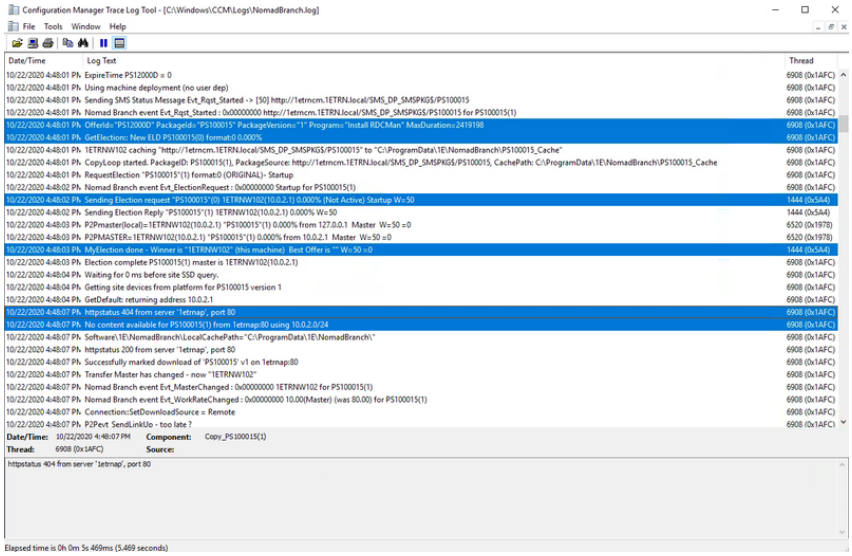


9.3.2.1.5 Deploying a legacy package with Nomad

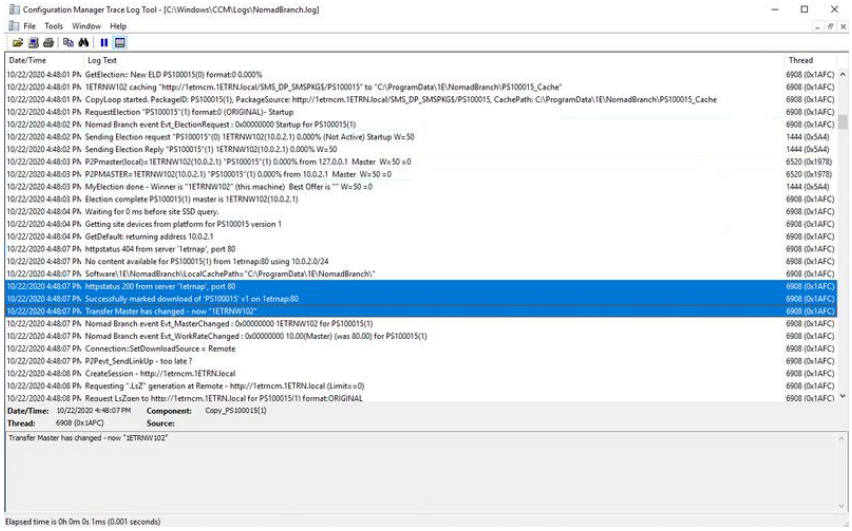
We then deploy the updates to our workstations using the following Deploy Software Wizard page settings:

Deploy Software Wizard Page	Setting
General	Selected the **Workstations** Collection
Content	Made sure the content is present on the DP
Deployment Settings	Set the **Purpose** to **Required**.
Scheduling	Created a new assignment schedule to run at the current time
User Experience	Checked **Allow users to run the program independently of assignments**
Distribution Points	Selected both Deployment Options to **Download content from distribution point and run locally**

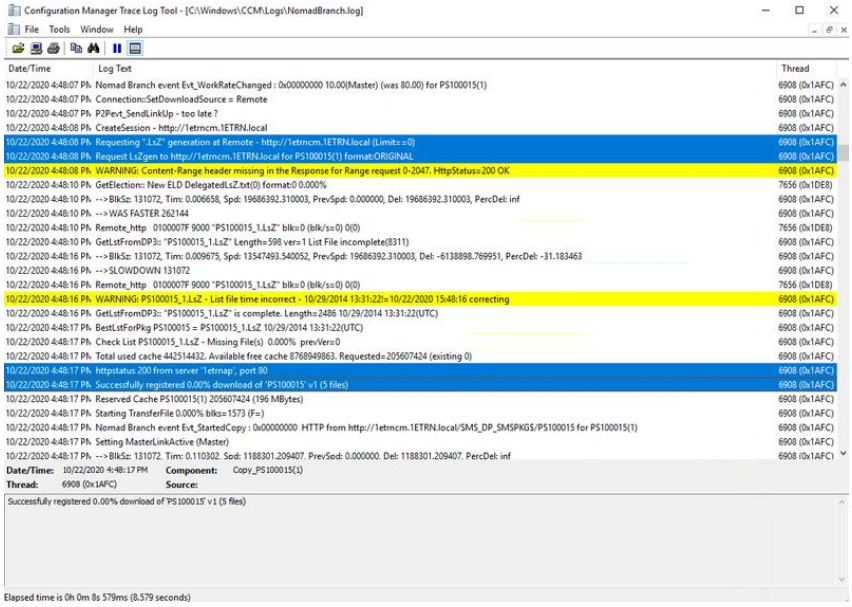
Our elected master is 1ETRNW102 in subnet 10.0.1.0 in the **C:\Windows\CCM\Logs\NomadBranch.log** we can see the normal election process. This is followed by a request for content for the **RDCMan** package but there is no content available.



From this point onwards 1ETRNW102 will be returned by the Content Distribution Consumer as a content source for other clients in its subnet within the same location.

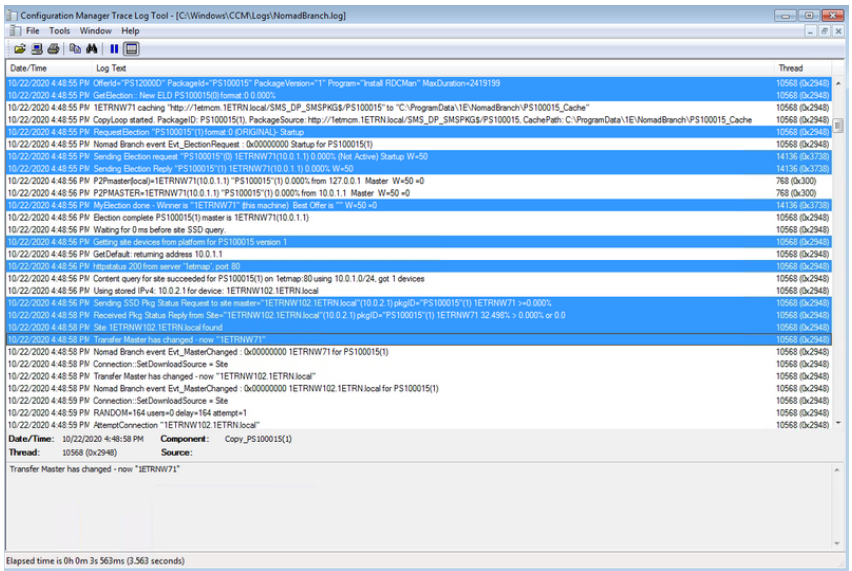


We can see 1ETRNW102 downloading the .LsZ file from the DP and updates the Content Distribution Consumer to indicate the download has started.



If we now look at the other subnet in our example, 10.0.2.0 and identify the first election request from this subnet which is from 1ETRNW71.

In the **NomadBranch.log** we see the normal activity where 1ETRNW71 is elected as the master.



Following this 1ETRNW71 queries the Content Distribution Consumer to see if the content is available on and adjacent subnet. The query returns 1ETRNW102 as a potential candidate, Nomad then sends a Package Status Request to the returned client and selects it.

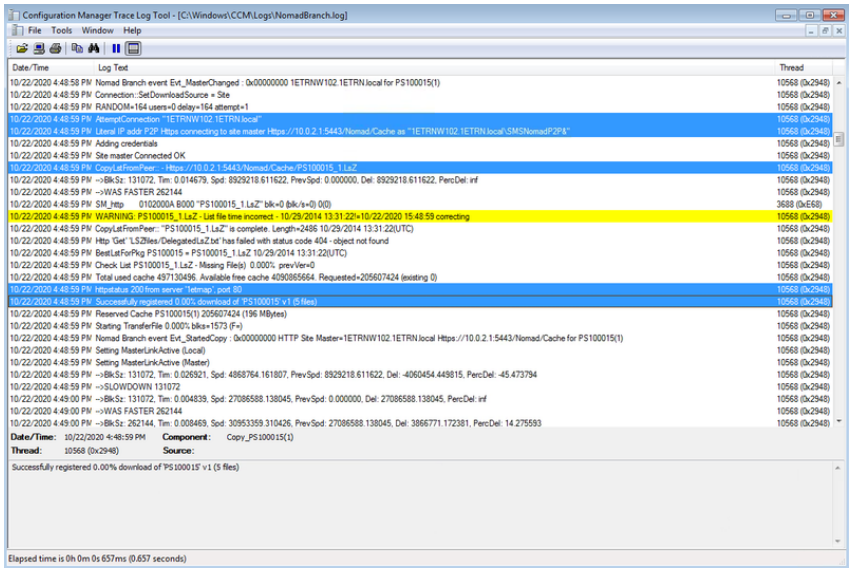
> **Note**
>
> If more than one client had been returned, the client with the most content already cached becomes the Site Master.

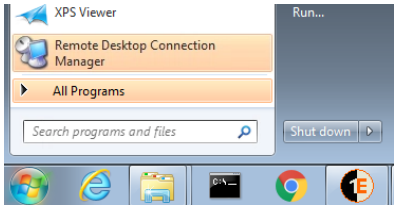
The elected subnet master starts to download content starting with the .LsZ file and the agent registers with the Content Distribution Consumer that it's now started the download. Every client

with ContentRegistration enabled will update the Content Distribution Consumer in this way whenever it starts to download content.

The **Remote Desktop Connection Manager (RDCMan)** package is then installed on our computers.

We have seen that Single Site Download allows you to deploy content to a large network, for example where you have a datacenter and a remote office and the computers are located in the remote office on two different subnets. Using Single Site Download allowed the 1E Client to obtain content from a peer in an adjacent subnet (within the same defined location) when that content was not available on a peer in its own local subnet.





9.3.2.2 Using FanOut for large subnets

Windows imposes a limit on the number of concurrent connections on the Nomad share. The FanOut featurecompensates for this limitation by enabling any peer that has more content than the requester to respond to the FanOut request. It is not limited to peers that have an active connection to the master.

The Nomad cache share (NomadSHR$) is created with a connection limit of six, this also applies for HTTP(S) transfers. This means that up to six Nomad peers can get content from the master at a time. If a 1E Client tries to connect to the master and all six connections are in use on the master, that agent would back off and retry later. The Fanout feature enables the 'rejected' agent to ask for an alternative peer in the same subnet that has the content it needs. Any other peer on the subnet can respond to this request, but will only do so if it has:

More content than the agent requesting it

Available connections and is not already be connected to a Fanout peer.

To find out more about how FanOut works refer to Nomad FanOut - How FanOut Works.

9.3.2.2.1 Enabling FanOut

To use FanOut, the Nomad*SpecialNetShare*registry value must be updated to include bit 6 (*0x40*or 64 decimal) on all computers hosting Nomad. To do this in our example, we imported a Configuration item and used Configuration Manager Settings Management to update our 1E Clients using a configuration baseline.

> **Note**
>
> The Nomad Baseline wizard is used to create a Configuration Manager (CM) Baseline from the Configuration Manager console for settings related to Nomad. Refer to Nomad Baseline wizard for more information.

In our example, we'll reinstall the RDC Manager package we installed in Using Single-Site downloads to deal with multi-subnet sitesusing two computers, 1ETRNW71 and 1ETRNW73 in our 10.0.1.0 subnet to prompt Nomad to re-download the content when the NomadSHR connection limit (1) is reached on the elected master which should be 1ETRNW101 as it has the content in its cache. For the purpose of this example we have reduced the connection limit to 1 to demonstrate FanOut behavior with a couple of clients. This is not something we recommend you do in a production environment.

> **Note**
>
> In our computers with a name ending in an odd number are in subnet 10.0.1.0, while those with a name ending in an even number are in subnet 10.0.2.0.

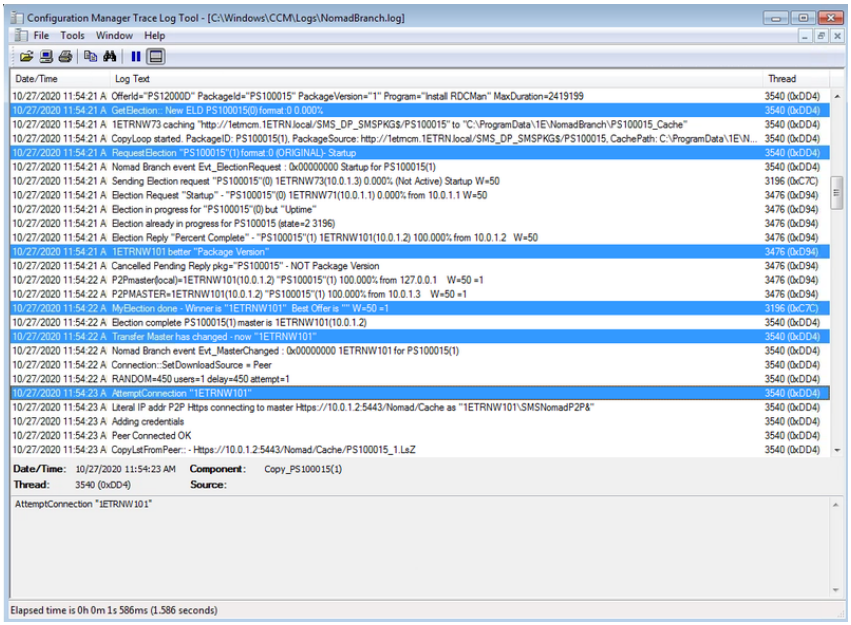
On both 1ETRNW71 and 1ETRNW73 we reinstalled RDC Manager using Software Center.

When we open **NomadBranch.log** on 1ETRNW73 there's an election where 1ETRNW101 wins as it has 100% of the content in its cache.

The elected master does not change for 1ETRNW71, but as there is only one connection available on **NomadSHR** which is being used by 1ETRNW73, 1ETRNW71 would fail to connect to the master. 1ETRNW71 then polls for a FanOut and receives a reply from 1ETRNW73 and then starts downloading the content from 1ETRNW73.

In this example we saw how FanOut can be enabled to allow multiple peers within a subnet to serve content to others in the situation where there are insufficient connections available on the elected master. This feature will typically enable faster distribution of content in larger subnets compared to the behavior seen in Using Single-Site downloads to deal with multi-subnet , where a maximum of six clients (in addition to the master) can be simultaneously obtaining content within the subnet.

> **Note**
>
> We recommend using Configuration Baselines as the best way to manage the configuration of your 1E Clients in a production environment. Refer to Nomad Baseline wizard for more information.



9.3.3 Deploying software updates using Configuration Manager

Nomad integrates with the Configuration Manager (CM) client content Distribution Point (DP) download process, and can be enabled on individual packages (including Driver Packages, Operating System Images, Operating System Upgrade Packages and Boot Images) and Task Sequences. For Applications and Software Updates, Nomad is enabled on each client for all Applications and Software Updates through Default Client Settings in Configuration Manager.

In addition, Nomad can also download content from Windows Update / Microsoft Update (WUMU). Starting in CB version 1806, software updates can be deployed to devices without first downloading and distributing content to Distribution Points, instead clients download updates directly from Microsoft Update.As a system administrator, we'll show how you can use Nomad to deploy software updates with CM from a CM Distribution Point or directly from Microsoft Update. While Nomad is enabled or disabled for all Software Update deployments through CM Client Settings, downloading from Microsoft Update is enabled by default. The settings are defined inCompatibilityFlags and you will need to ensure the relevant bits remain set if you are using that registry value to configure other options.

For details about the types of updates enabled by default in the Nomad client (1E Client 4.1 and later), refer to Downloading content for CM Software Updates from Microsoft Update.

> **Note**
>
> You can use the Nomad app, powered by the Tachyon Platform to get a visual snapshot of download activity in your environment. The Nomad app will be available after you install the Tachyon Platform and can be accessed using the Tachyon DNS Alias FQDN, for example https://tachyon.acme.local/Tachyon
>
> The section Monitoring Nomad on this page provides an overview of how you can use the app to view download progress for large and small scale deployments.

9.3.3.1 Enabling Nomad for Software Updates

Nomad is enabled or disabled for all Software Update deployments through the Client Settings. In our example we will enable Nomad for Software Updates in the **Default Client Settings** and see how Nomad takes part in the download process and shares the content.

Before deploying our software updates, we are going to amend the Work Rate for our deployment. The Work Rate determines the percentage of available bandwidth to use for the download.

In this example we have changed this from the default 80% of available bandwidth to 10% to slow down the deployment and so making it easier to monitor.

For more details about the Nomad tab, and how you can use Work Rates, refer toDistributing software with Nomad and Configuration Manager - Nomad tabandDesign Considerations: Setting intra-day work rates.

In our example in Configuration Manager:

We select the **Administration** workspace and choose the **Client Settings** node.

Then click **Default Client Settings** in the right-hand pane and select **1E Nomad→Nomad Properties** from the displayed Ribbon.

In the Nomad Properties dialog box, we select **Software Updates** on the left and make the following changes.

Check **Enable Nomad**

Check **Work Rate (%)** and set the value to**10**.

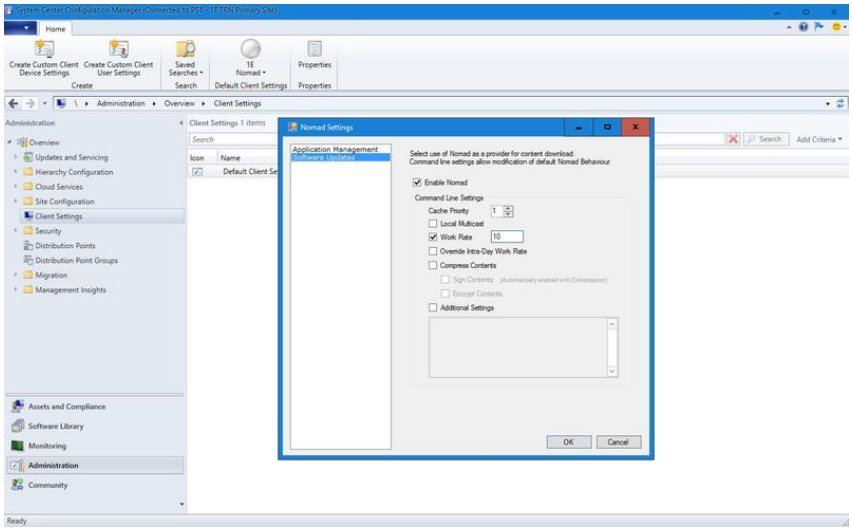
Once this is done, we force a policy update on the collection containing our workstations called **Lab Workstations**.

> **Note**
>
> As Windows 10 cumulative updates get very big, very quickly (often in excess of 1GB a few months after any given Feature Upgrade), Microsoft started publishing express installation files for these updates in addition to the traditional full update files. Configuration Manager introduced support for Windows 10 Express Installation File updates in Current Branch 1802 hotfix KB4163547.
>
> Express installation files are a much larger payload on the Distribution Point compared to traditional software update files, but the feature enables clients to download delta byte-ranges from these files, so each month the amount of data a client has to download is typically much smaller. Configuration Manager Current Branch can be configured to support express installation files (refer to https://docs.microsoft.com/en-us/configmgr/sum/deploy-use/manage-express-installation-files-for-windows-10-updates for more details).
>
> With the release of Windows 10 1809, Microsoft replaced express update files with a new way of managing deltas within software updates. In Configuration Manager 1902 the **Enable installation of Express installation files on clients** option in Software Update Client Settings was replaced with
> **Allow clients to download delta content when available**.

Note

Nomad supports the download of Express installation files and delta content for updates.

Refer to Windows 10 Express Installation Files and Delta Content for Updates for more details.



9.3.3.2 Deploying Windows updates from a DP

We have created a **Software Updates** group called **Windows 7 Updates** containing three updates for the Windows 7 computers on our network:

2018-05 Security Only Quality Update for Windows 7 for x86-based Systems (KB4103712)

2018-07 Security Only Quality Update for Windows 7 for x86-based Systems (KB4338823)

Security Update for Windows 7 (KB3000483).

We then deploy the updates to our workstations using the default deployment settings, but making sure we have set:

Deployment Settings - the Purpose is **Required**

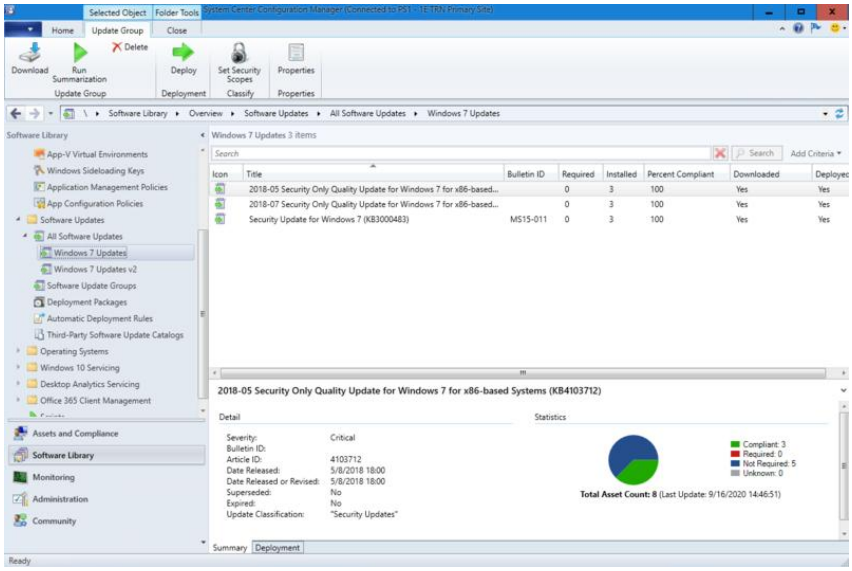
Scheduling - Installation deadline is **As soon as Possible**

Download Settings - we selected both **Download** options.

Note

Software Update Deployments always download the required content and install it from the local cache. By default, clients connected within a boundary defined by an administrator as slow or unreliable will not download the content and therefore the update will not be deployed to those clients.

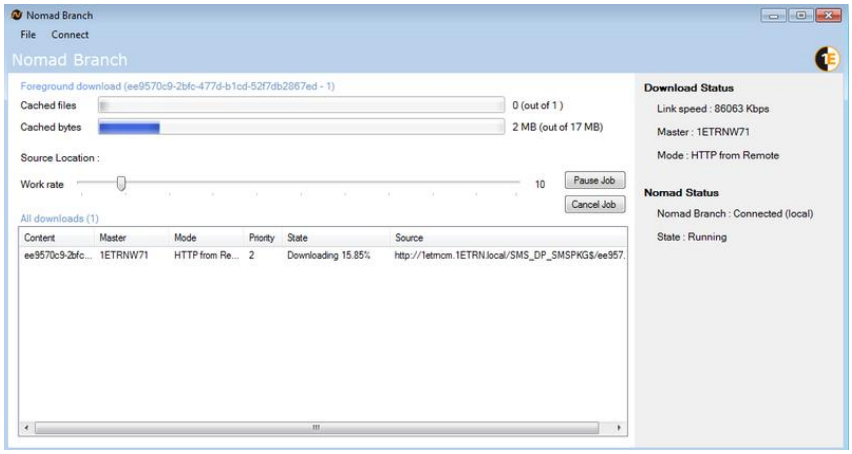
Because we are using Nomad to distribute the content, we always want the content to be downloaded, as we are not concerned about the bandwidth when using Nomad.

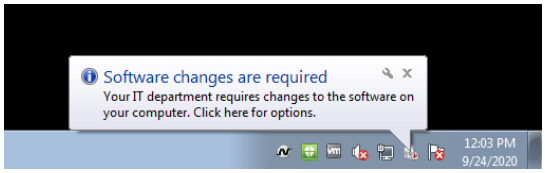


9.3.3.2.1 Tracing update download progress

We then watch the computers in our as they receive the Software Updates policy and begin to download the content. Using the Nomad download UI we can see the content being downloaded. We can also see that the 1ETRNW71 computer has been elected as Master.

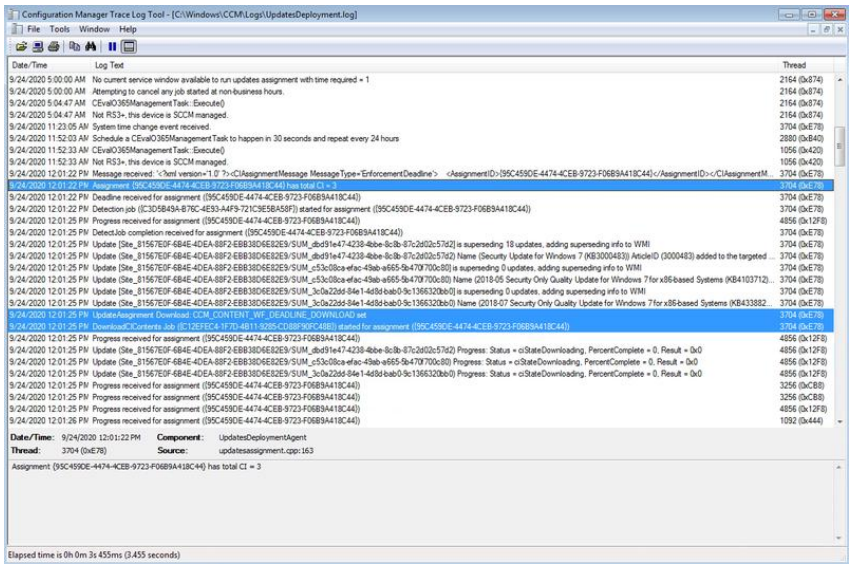
> **Note**
>
> Nomad ensures that software packages are only ever copied once per branch over the WAN, utilizing local computers as temporary file caches to distribute the software locally. This reduces the bandwidth required for delivering software updates and means that small offices or sites connected by poor network links can receive software updates more reliably.
>
> The Nomad clients with local copies of the package can themselves act as the master if the need arises. This significantly reduces the number of Configuration Manager servers required to manage a Configuration Manager hierarchy, thereby reducing initial and ongoing maintenance costs.
>
> Refer to Download once to branch for details.



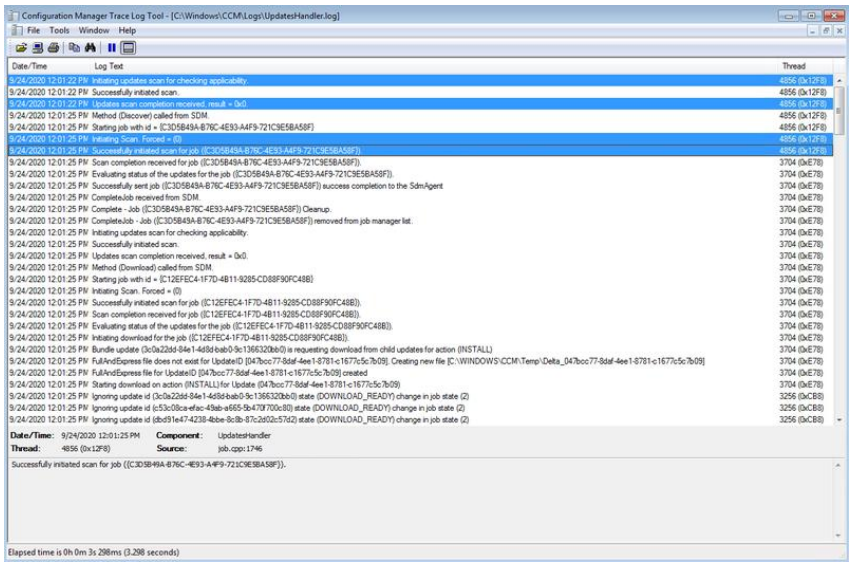


Using CMTrace.exe we open the **UpdatesDeployment.log** from **C:\Program Files\SMS_CCM\Logs** and can Identify the point when the Configuration Manager client receives the software updates assignment. We can also see log entries indicating that each of the updates have been added to the targeted list and that the **DownloadCIContents** Job has started.

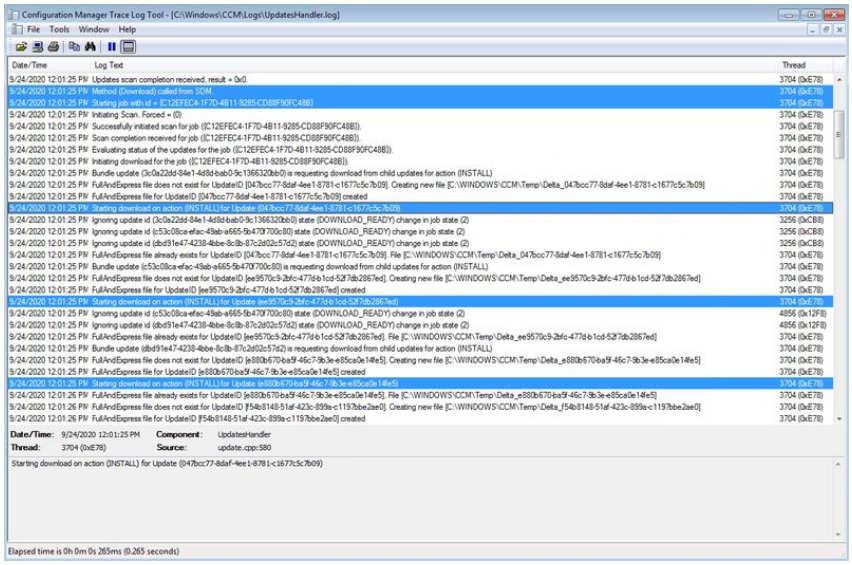
In our example we can see this process for Security Update for Windows 7 (KB3000483).



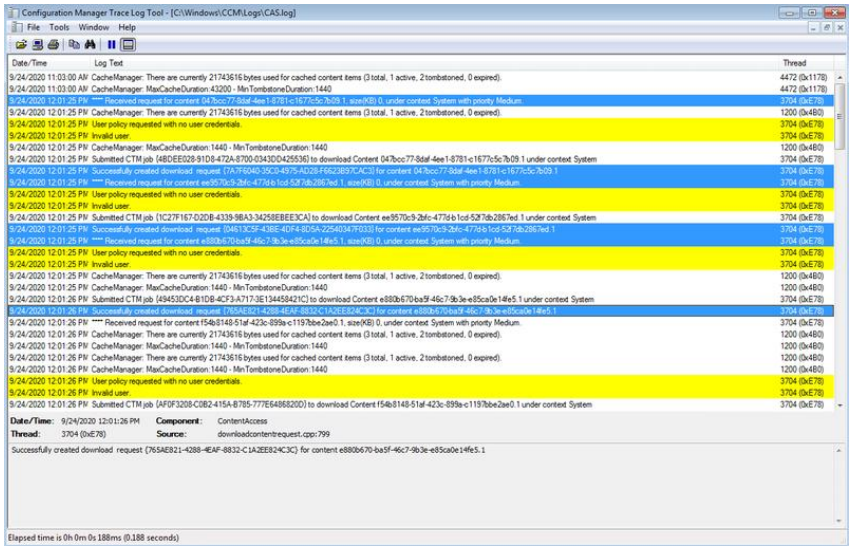
We then open **UpdatesHandler.log** and identify the point where the updates handler initiates a scan to determine which of the updates included in the deployment are applicable.



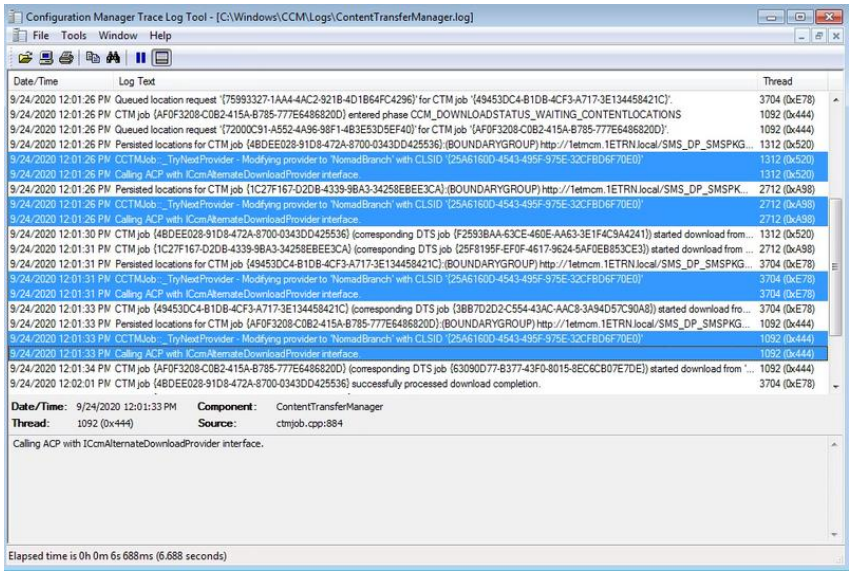
Eventually the scan determines the required updates and initiates download.



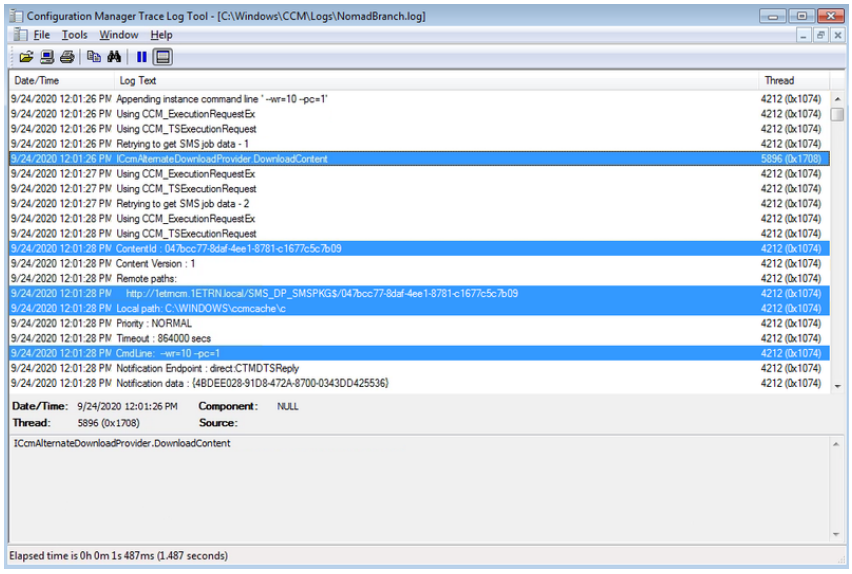
We then open **CAS.log** and identify the point where the Content Access Service requests the content for the requested updates in the deployment.



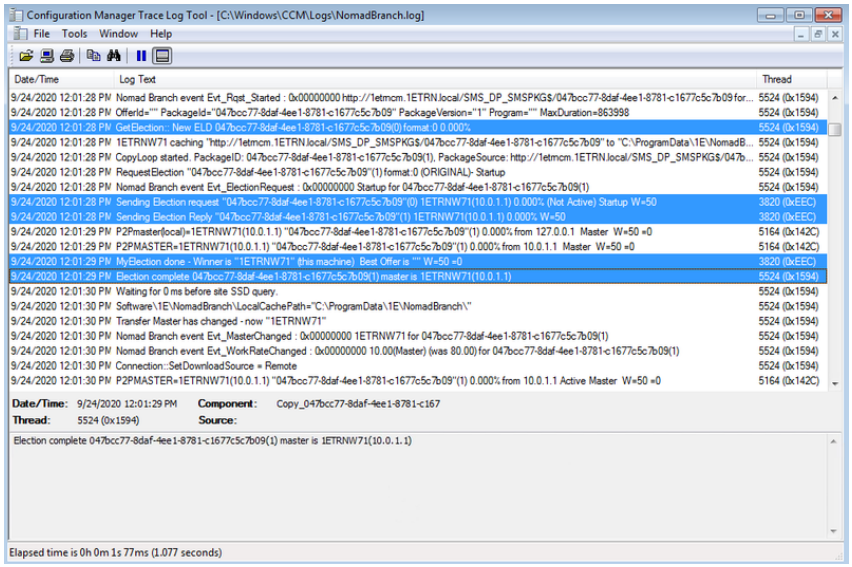
In the **ContentTransferManager.log** we identify the points where CTM calls the NomadBranch provider for each of the required updates.



We look at the **NomadBranch.log** from C:\Windows\CCM\Logs and identify the point where Nomad is called by the Content Transfer Manager as the Alternate Content Provider.

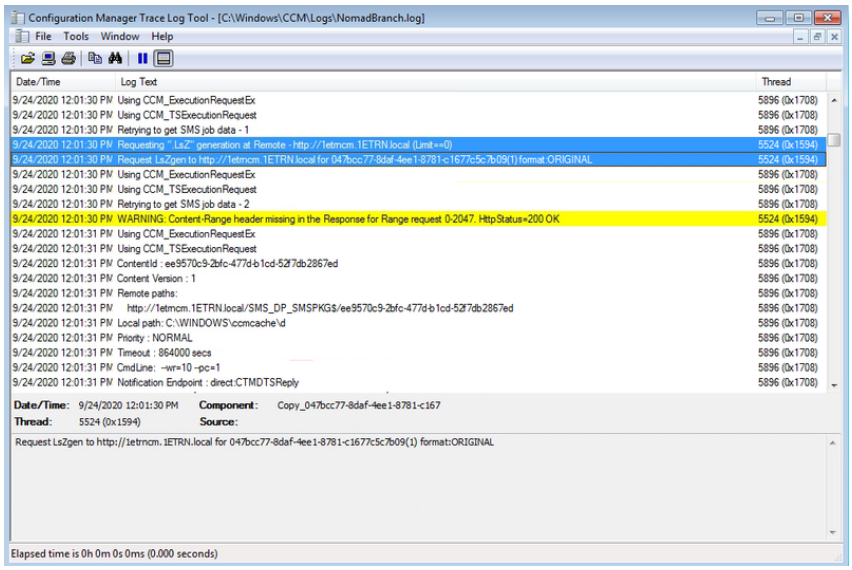


We locate the point where Nomad initiated the election for the content associated with the first update. From the log entries, we can then see which computer became the master.

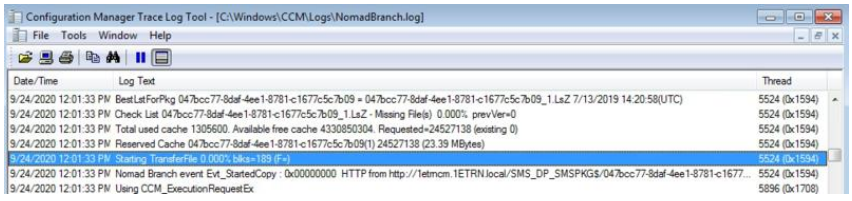


Then we locate the point where the client gets the **LsZ** file. As we are looking at the **NomadBranch.log** file on the master, we see the LsZ generation request (as this is the first time the content has been requested from the DP) and the LsZ file will then be downloaded from the DP.

> **Note**
>
> If we looked at the log file on one of the other clients, the LsZ file will be downloaded from the master.



Finally we identify the point where the client downloads the content for the first update (either from the DP or from the master). The client will then complete the hash check and create the hard-link to the Configuration Manager cache.



We have seen that each update is identified as an individual piece of content, resulting in an election for each Software Update. Because all computers on our network might not need the same updates, every update will have its own election, and different masters may emerge for different updates.

9.3.3.3 Deploying Windows updates directly from Microsoft Update

In this example, the source of our updates are from Microsoft Update and Nomad shares the content as it would if the content was available from Configuration Manager.

9.3.3.3.1 Configure and confirm settings

We have created a **Software Updates** group called **Windows 7 Updates v2** containing two updates for the Windows 7 computers on our network:

Security Update for Windows 7 (KB3004375)

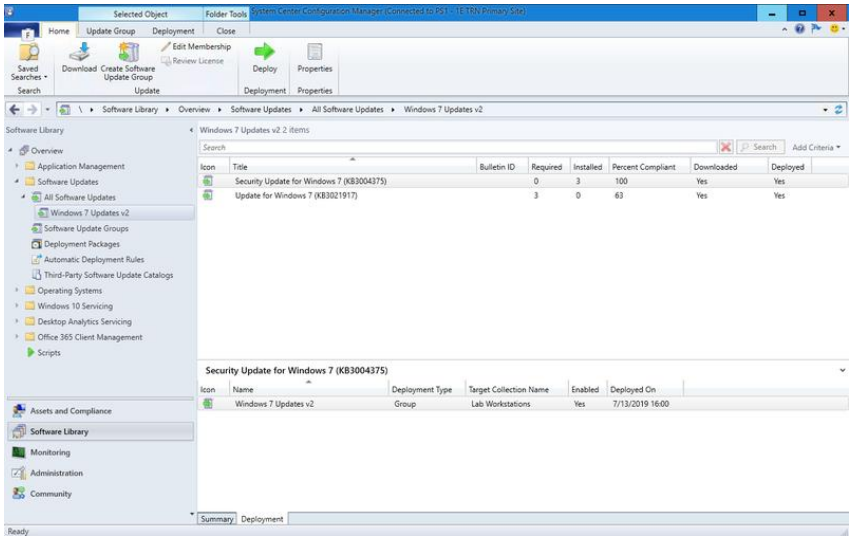
Update for Windows 7 (KB3021917).

We then deploy the updates to our lab workstations using the default deployment settings, but making sure we have set:

Deployment Settings - Type of deployment is **Available**

Download Settings - we selected both **Download** options and checked
If software updates are not available on distribution point in current, neighbour or site boundary groups, download content from Microsoft Updates.

We then install the update using **Software Center→Updates** on our Windows 7 computers.



We open the **NomadBranch.log** on our computer 1ETRNW72 and see the start of the download from Windows update and the calls for an election with this computer winning.

1ETRNW72 wins the election because it is the only targeted device the subnet.

Note

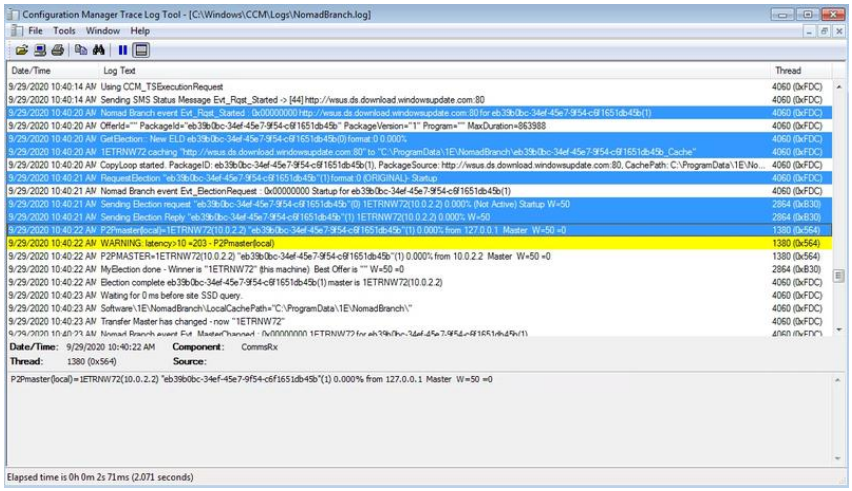
Nomad ensures that software packages are only ever copied once per branch over the WAN, utilizing local computers as temporary file caches to distribute the software locally. This reduces the bandwidth required for delivering software updates and means that small offices or sites connected by poor network links can receive software updates more reliably.

The Nomad clients with local copies of the package can themselves act as the master if the need arises. This significantly reduces the number of Configuration Manager servers required to manage a Configuration Manager hierarchy, thereby reducing initial and ongoing maintenance costs.

Refer to Download once to branch for details.

In this example, we have seen how Nomad can be used to download Software Updates content. From both a Config Mgr deployment where content is available and when it is not and connecting to Microsoft Update has been allowed.

In addition, we have seen that Nomad is enabled within the Software Updates Client Agent settings rather than in the individual Software Update Deployments, so once enabled Nomad is used for all Software Update Deployments. The process of getting content is the same as with Applications and Packages – the Content Transfer Manager invokes Nomad as an Alternate Content Provider, which downloads the content then passes back control to CTM.



9.3.4 Deploying updates for Office 365

Configuration Manager introduced support for Office 365 updates in Current Branch 1602, and Nomad introduced support in version 6.1.100. This section describes how Office 365 deployments differ in terms of ACP requirements and how Nomad behaves during the download.

Downloading the following types of updates is enabled by default in the Nomad client (1E Client 4.1 and later). Downloading from Microsoft Update is also enabled by default.

The settings are defined in CompatibilityFlags and you will need to ensure the relevant bits remain set if you are using that registry value to configure other options, refer to Downloading content for CM Software Updates from Microsoft Update - Configuration for more details.

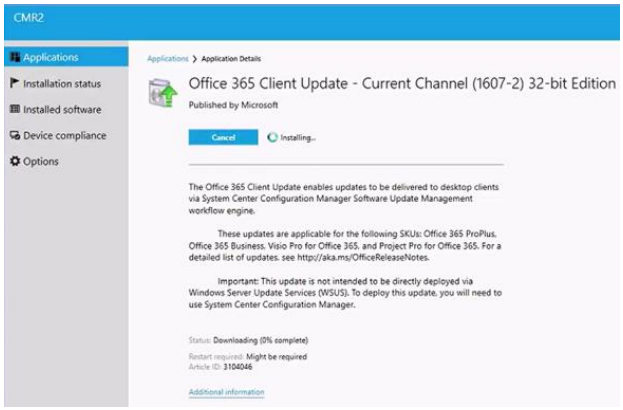
Refer to Deploying Office 365 updates for details about Nomad and Office 365 including, how it works, Nomad app integration for Office 365 and other supported Nomad features.

> **Note**
>
> You can use the Nomad app, powered by the Tachyon Platform to get a visual snapshot of download activity in your environment. The Nomad app will be available after you install the Tachyon Platform and can be accessed using the Tachyon DNS Alias FQDN, for example https://tachyon.acme.local/Tachyon
>
> The section Monitoring Nomad on this page provides an overview of how you can use the app to view download progress for large and small scale deployments.

9.3.4.1 Deploying Office 365 updates

We will start by installing an update that is not cached locally on one Nomad client and therefore all download activity is from the Distribution Point. After that, we initiate an installation of the update on the second Nomad client and walk through the download from the first Nomad client's cache.

From Software Center, the Installation of the Office 365 update is initiated. During the download, its status is displayed at the bottom of the screen.



Browsing to the NomadBranch.log location (typically, located with Configuration Manager agent logs). When Nomad receives the download request (job) and manifest file from the Configuration Manager agent:

It checks its query results store (QRS) to see if any peer has broadcast that it is already downloading the content.

If the broadcast is not found, an election (network query) is initiated in an attempt to obtain the content from a peer.

If no peer responds, a download is initiated from a DP (4).

Once the download is complete, the data is copied into the location described in the manifest file.

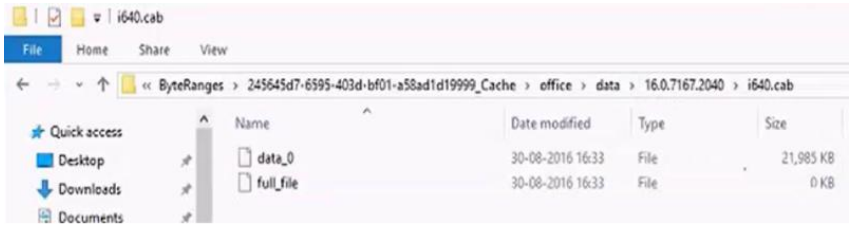
The log extract below shows all five events with the successful download (i641033.cab) from a DP. Office 365 downloads can be either a file or part of a file (byte-range). Our example illustrates a download for an entire file.

The downloaded data is copied to the CTR location described in the manifest and is also retained in the Nomad cache. Our example illustrates the location of the Nomad cache with the file downloaded and a marker (full_file) to indicate that this is not a byte-range.

For an Office 365 Update deployment, multiple jobs are passed to Nomad by the Configuration Manager agent. Once the downloaded job is completed, another BEGIN JOB appears in the log for the same update deployment.

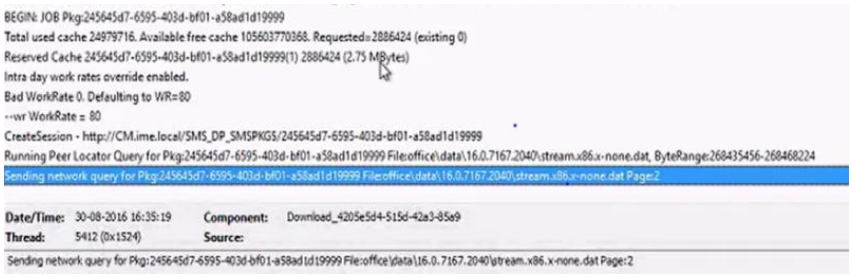
The same process is followed in the attempt to obtain the content locally. Our example illustrates a larger i640.cab file being downloaded.

And the Nomad cache when the job completes.

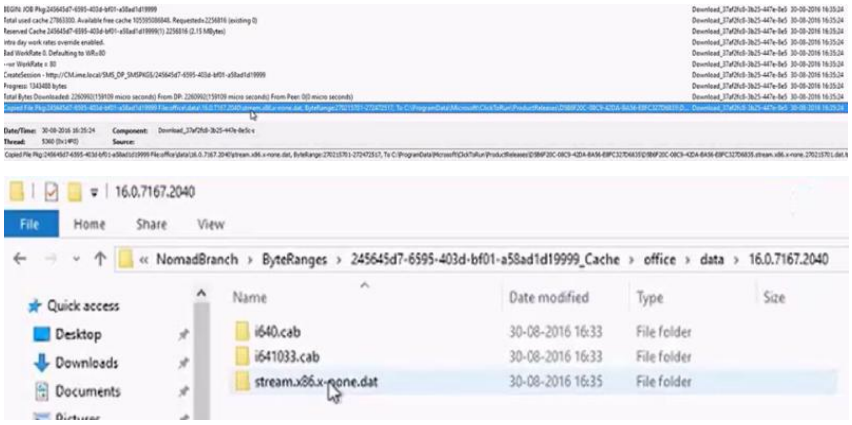


The third job to be passed to Nomad contains an instruction to download a byte-range for Stream.x86.x-none.dat.

An entry in the log describes the range (the byte-range is 268435456-268468224, a 32KB chunk that must reside in the second page file. Update files are broken down into 128MB page files.) and the subsequent election request attempting to locate it.



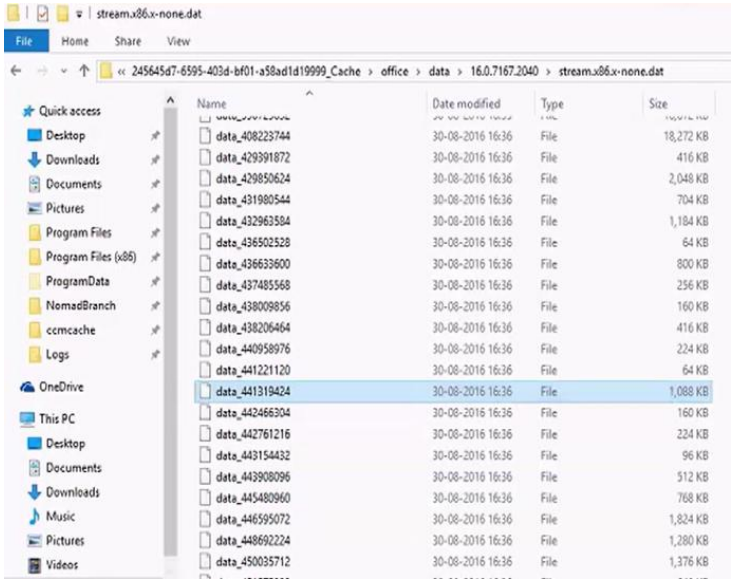
When the download completes and copied to the CTR location, more byte-range jobs related to the same file are logged.



Successive byte-range jobs are passed to the Nomad client, downloaded into the cache and copied to the CTR location.

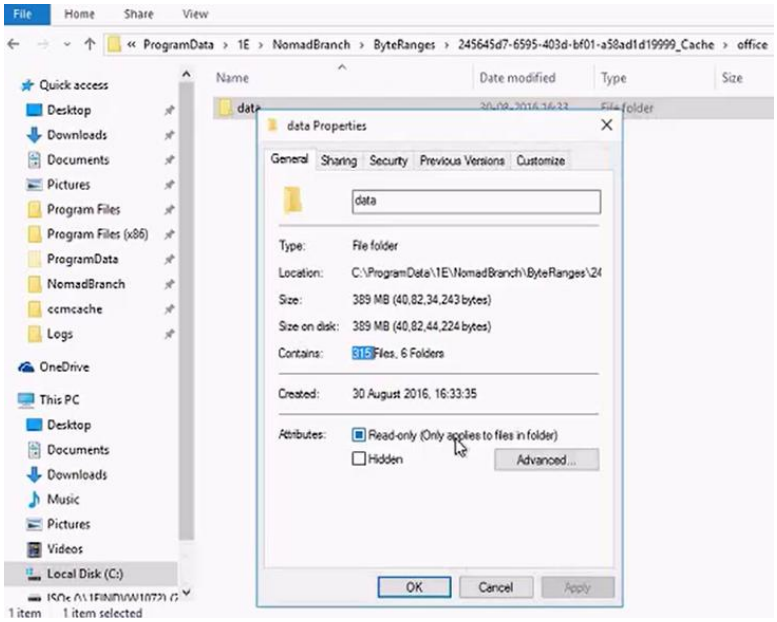
Once byte-range downloads are complete, Nomad copies them into the CTR update location at:

C:\ProgramData\Microsoft\ClickToRun\ProductReleases\<ProductCode>\<ProductCode>.<FileName>.tmp



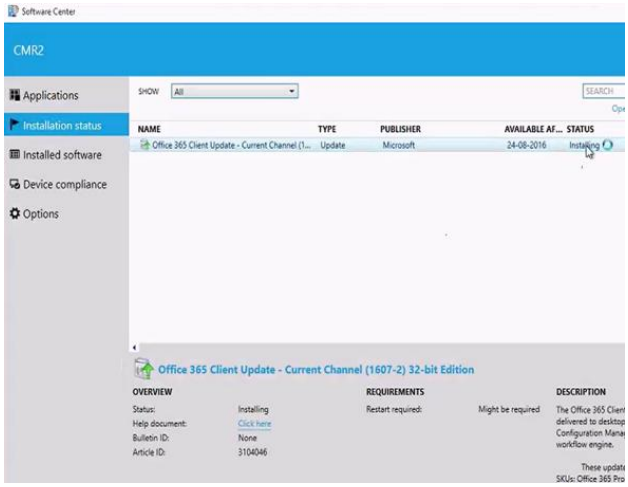
It will be likely that hundreds of jobs are passed to Nomad for a single Office 365 update download.

In our example, a total of 315 download jobs were requested by the Configuration Manager agent.

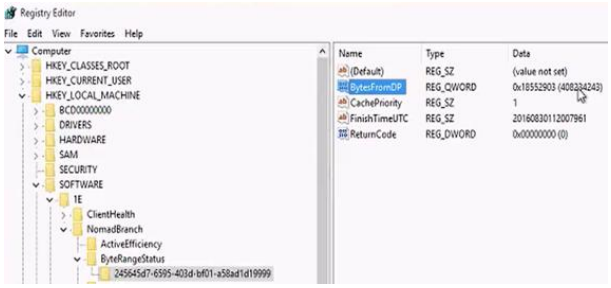


When a job completes, Nomad monitors the CTR agent interface to determine if actual update installation is successful. Once the CTR agent has all the files and byte-ranges that it needs, it merges the byte-ranges, performs a hash check on the contents and attempt to install the update.

The status indicates **Installing** at this point and changes **Installed** when it is done.

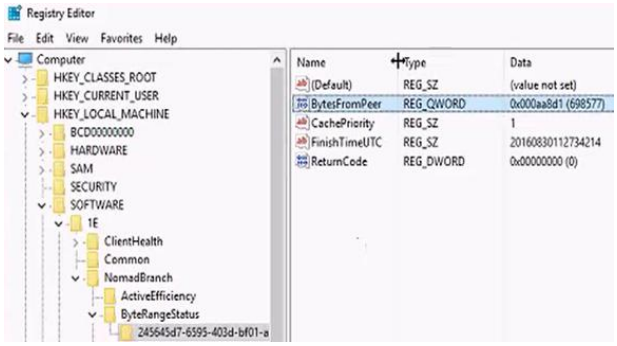


For an Office 365 Update download, you can verify the total amount of data downloaded from the DP by inspecting the registry. If you do not see a BytesFromPeer value, it means that all your downloads were from the DP.

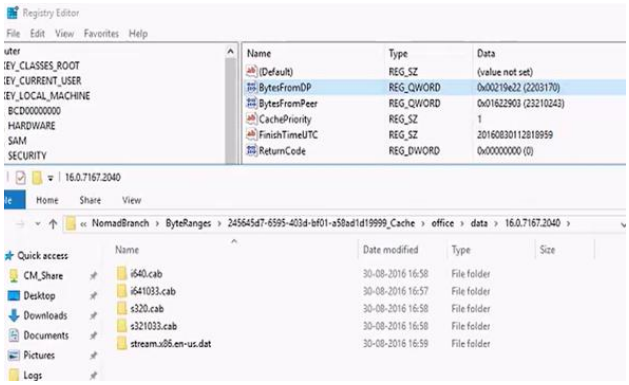


Log on to the second Nomad client and initiate the update installation from Software Center.

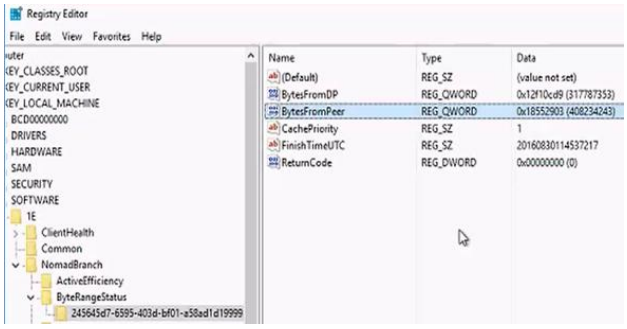
Browse to NomadBranch.log. The Standard P2P connecting to... and SMB Connected OK log entries indicates that it is initiating a download from the first Nomad client. Initially, the Nomad client registry does not display BytesFromDp as the second Nomad client is able to obtain content from the first Nomad client.



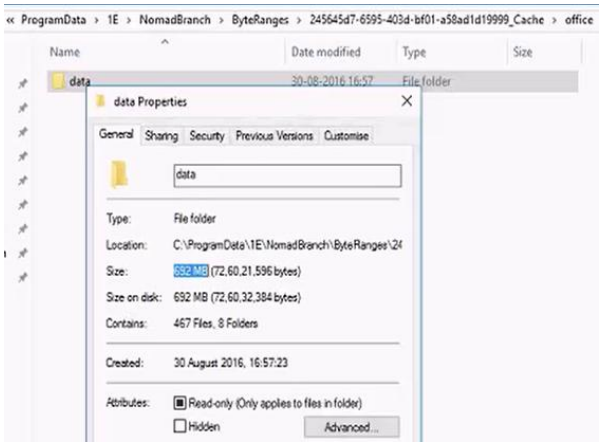
Due to differences in the state of the Office 365 installation on the second host, the CTR agent requested content that is not present on the first Nomad client. Consequently, it switches to download from the DP. Our example illustrates this event in the second Nomad client's registry.



When the download is complete, the values in the registry are updated.



We can see the extent of the differences in the update installation on the two Nomad clients if we inspect the total downloads on the second Nomad client; 467 downloads compared to 315 on the first Nomad client.



9.3.5 Using Nomad with Operating System Deployment OSD

Nomad can integrate with Operating System Deployment (OSD) strategies to maximize the efficiency of distributing large OS content across the network. It does this by providing a number of Task Sequence steps that can be integrated directly into your OSD Task Sequences.

As a system administrator you can use Nomad for OSD refresh. In the following scenario we'll show how you can use Nomad to integrate with the ConfigMgr OS Deployment process to refresh workstations in remote locations that do not have a local server. This will involve:

Preparing the boot image to allow content to be sourced from a local peer

Preparing the deployment Task Sequence to use Nomad

Deploying the modified task sequence to target clients.

OSD integration requires both **NomadBranchTools.msi** and **NomadBranchAdminUIExt.msi** to be installed:

NomadBranchTools.msi - are installed on the CM Site server(s) and SMSProvider server(s) and install the Nomad files that get injected into a boot image

NomadBranchAdminUIExt - is installed wherever the ConfigMgr console is installed. It adds the custom Task Sequence steps, among other ConfigMgr console extensions.

Refer to Installing Nomad Branch Toolsfor more details about installing the Nomad OSD tools.

> **Note**
>
> You can use the Nomad app, powered by the Tachyon Platform to get a visual snapshot of download activity in your environment. The Nomad app will be available after you install the Tachyon Platform and can be accessed using the Tachyon DNS Alias FQDN, for example https://tachyon.acme.local/Tachyon
>
> The section Monitoring Nomad on this page provides an overview of how you can use the app to view download progress for large and small scale deployments.

9.3.5.1 Preparing a task sequence to use Nomad

In this scenario, we will use an pre-existing example Task Sequence we have called **Nomad Windows 10 Ent** to upgrade a device to Windows 10, and make modifications to integrate Nomad. This will ensure that content is obtained from a local peer whenever available or downloaded from the Distribution Point in a bandwidth controlled manner using Nomad. Additionally, we will add actions to store the captured User State on a local peer and retrieve the User State after the new operating system is in place.

> **Note**
>
> For details beyond the scope of this example about using Nomad to carry out an OSD refresh including task sequence deployments, refer to OS deployment task sequences - Using Nomad for an OSD Refresh.

9.3.5.1.1 Set Nomad as the Download Program

To support an Alternate Content Provider in a Task Sequence, Microsoft introduced the SMSTSDownloadProgram task sequence environment variable. The SMSTSDownloadProgram task sequence environment variable contains the path to the download program's executable file.

In the case of Nomad, this file will be **SMSTSNomad.exe** , the Nomad OSD Tools use a custom task sequence action that we use in this task to set the SMSTSDownloadProgram variable to**SMSTSNomad.exe**.

To set Nomad as the **Download Program**, we can:

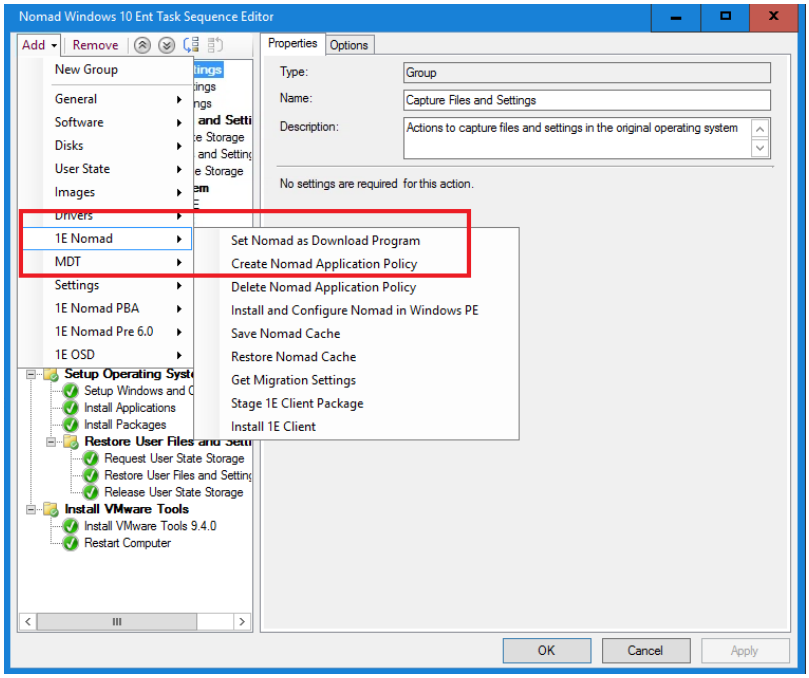
Right-click our **Nomad Windows 10 Ent** task sequence from **Software Library**→**Operating Systems**→**Task Sequences** and select **Edit**.

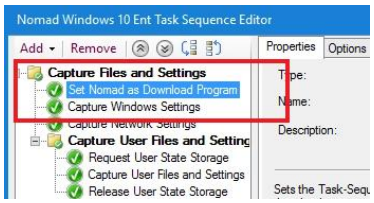
Select the **Capture Files and Settings** group.

Select the **Add** dropdown we select **1E Nomad** and select **Set Nomad as Download Program**.

Right-click the **Set Nomad as Download Program** task and select **Move Up**. We then make sure the **Set Nomad as Download Program** task now appears above the **Capture Files and Settings** group at the top of the Task Sequence before any content is needed.

Click **Apply** to save the change.





9.3.5.1.2 Install and Configure Nomad in Windows PE

We install and configure Nomad in WinPE so that Nomad is used to download content during the Windows PE stage of a task sequence.

The NomadBranchTools updates the OSDInject manifest with the Nomad files to be added to the boot image. The process of updating the boot image on Distribution Points injects them into the boot image, When the boot image is loaded the Nomad files are there but the Nomad service is not installed.

> **Note**
>
> This manifest defines the files that are to be added into the Windows PE boot image when it is updated on a distribution point. The additional tools are added to this manifest, ensuring that they are included in all boot images that are updated on a distribution point from this point on.

We set this step up by:

Selecting the **Restart in Windows PE** step in the *Install Operating System* group.

Clicking **Add > 1E Nomad** and select **Install and Configure Nomad in Windows PE**.

Changoing the **SpecialNetShare** value to **8240** (0x2030).

Setting the **Compatibility Flags** value to **538443786** (0x2018000A).

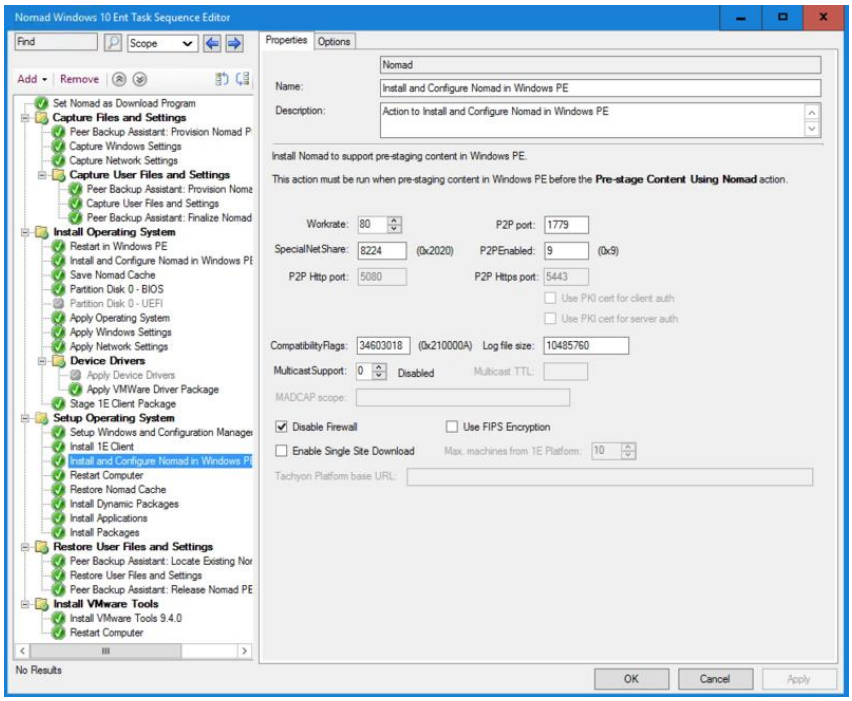
Setting the **P2PEnabled** value to **73** (0x49).

Clicking **Apply**.

Selecting the **Install and Configure Nomad in Windows PE** step, click **Add→1E Nomad** and select the **Save Nomad Cache** task. The **Operation** value will be **Move** and the **Wipe CCM Cache** option is selected.

Clicking **Apply** to save the task sequence.

> **Note**
>
> The settings we used for **SpecialNetShare , Compatibility Flags** and **P2PEnabled** match those on the Nomad clients installed in our environment, the settings for your environment may be differant. If there is a mismatch in certain settings between clients, Nomad may might not work as expected.



9.3.5.1.3 Install the 1E Client in the New Operating System

Once the ConfigMgr client is installed in the new operating system, we need to install the 1E Client so it can register as the Alternate Content Provider (ACP) and retrieve the content for all the other packages, applications and software updates to be installed in the new operating system. We achieve this by:

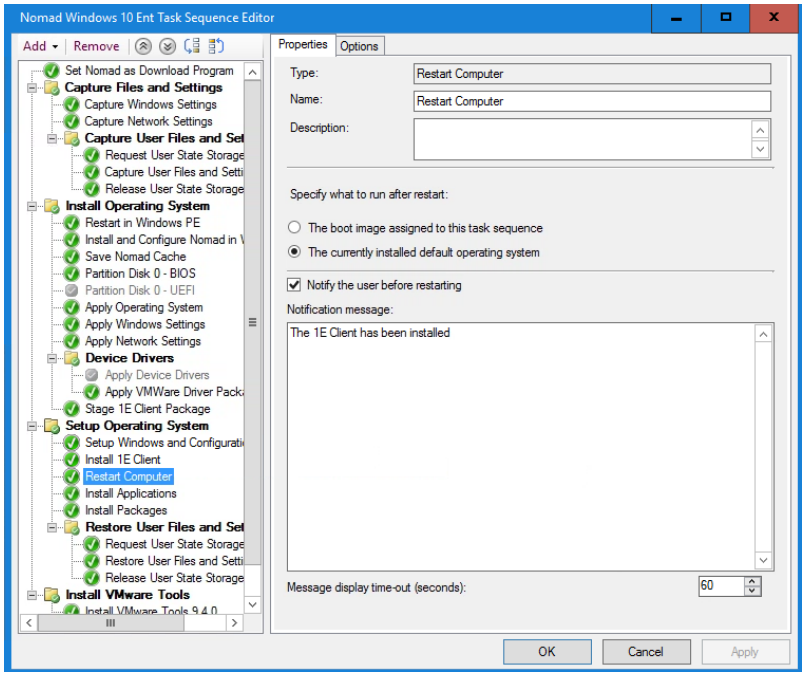
Selecting the **Setup Windows and Configuration Manager** task In the *Nomad Windows 10 Ent* Task Sequence Editor and from the **Add** dropdown selecting **1E Nomad→Install 1E Client**.

Clicking **Add→General→Restart Computer** with the **Install 1E Client** step selected.

Choosing **The currently installed default operating system** in the *Specify what to run after restart:* section. We ensure the **Notify the user before restarting** check box is checked and change the **Notification message** to **The 1E Client has been installed**. We then click **Apply**.

Note

A reboot is required after the Install 1E Client task to ensure the system path is properly updated so the Nomad tools (like, **NBCacheActions**) can be located by the operating system.



9.3.5.1.4 Restore the Nomad Cache

Once Nomad is installed, we want to restore the content that was used during the build into the Nomad cache of the newly built OS.

In the Install and Configure Nomad in Windows PE section the added Save Nomad Cache is used to save the Nomad cache either in WinPE or a full Microsoft Windows operating system. The **Save Nomad Cache** step copies, links or moves previously downloaded content to the protected task sequence runtime folder so that it is not deleted by the standard **Apply Operating System** task sequence action.

We now do this by:

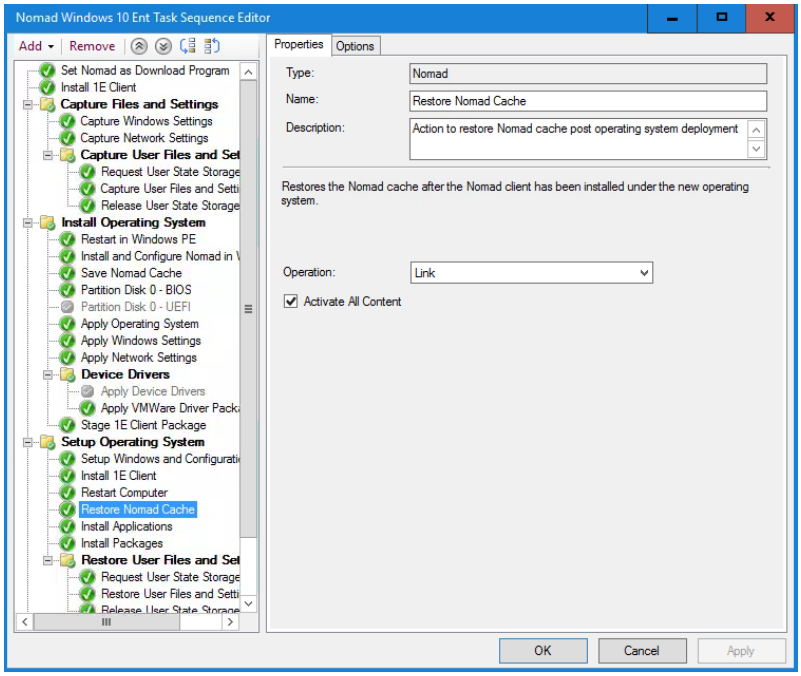
Selecting the **Restart Computer** task and from the **Add** dropdown select **1E Nomad > Restore Nomad Cache**.

In the **Properties** tab, ensuring **Link** is the operation and selecting **Activate All Content** then click **Apply** to save the task sequence.

Note

This task will restore the Nomad cache from the persisted **_SMSTaskSequence** folder to the newly installed Nomad cache. The option to Link the content (i.e. create a link from the folder in _SMSTaskSequence to the Nomad Cache folder) is optimal in this scenario; copying would take a long time and moving it may prevent subsequent tasks (such as MDT tasks) from completing properly.

The Nomad cache is essential to Nomad's download once to branch feature. The cache enables Nomad to hold its downloaded content so that it can be distributed locally to other Nomad peers. The Nomad cache contains downloaded content (such as packages, applications, and software updates) which can vary in size from relative small patches to rather large OS image files. For more details refer to Nomad cache.



9.3.5.2 Working with Dynamic Packages

We now add a package to be installed using a variable. We will manually set the variable to demonstrate the behavior, but any means of populating the variable will give the same result. Nomad will be called by the task sequence by SMSTSNomad.exe being specified as the default task sequence download program.

9.3.5.2.1 Add the dynamic package to the Task Sequence

We will add an Install Package task to the *Nomad Windows 10 Ent* task sequence that uses a variable name to define the Package and Program to be executed at runtime. For the purpose of this example, we will define this variable directly within the task sequence to demonstrate how Nomad handles dynamic packages. We do this by:

Selecting the **Restore Nomad Cache** task in the Setup Operating System group.

Clicking **Add** and selecting **Software→Install Package**.

In the Properties tab, entering **Install Dynamic Packages** as the name.

Selecting **Install software packages according to dynamic variable list** and entering a Base variable name of **NOMADOSD**. Select **If installation of a software package fails, continue installing other packages in the list** and click **Apply**.

Selecting the **Restore Nomad Cache** task again, clicking Add and selecting **General→Set Task Sequence Variable**.

In the Properties tab, naming the task **Set NOMADOSD001.** Enter **NOMADOSD001** as the Task Sequence Variable and set the Value to **PS10001B:Install Skype**.

Clicking on the **Options** tab on the task, and checking the **Continue on error** box.

Clicking **Apply**. The task sequence now looks like image on the right, we click **OK** to save the updated Task Sequence.

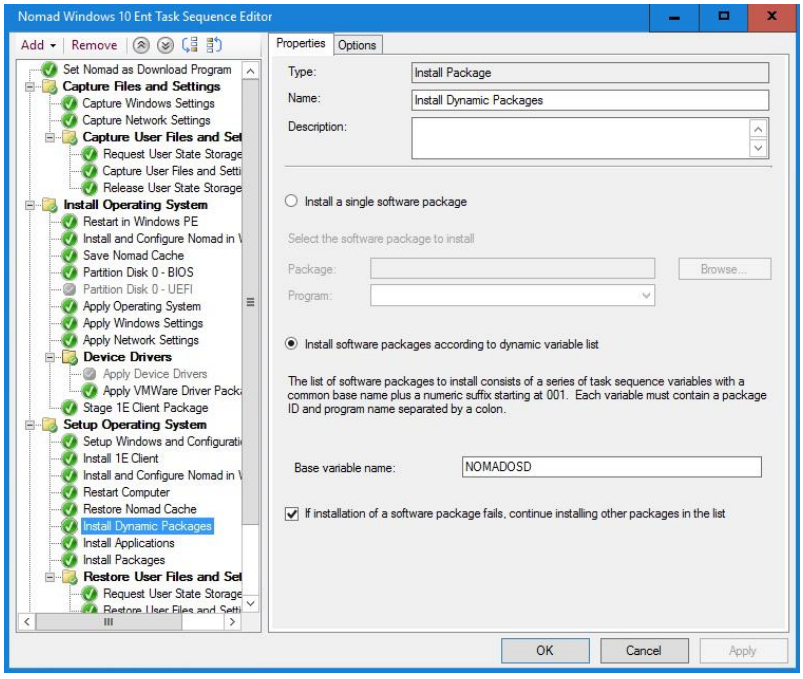
Note

In this step we are defining the first (and only, in this case) dynamic package through the NOMADOSD001 Task Sequence variable before the Install Dynamic Packages task executes. The value of this variable is in the format **<PackageID>:<Program Name>**. The Skype Package has a Package ID of PS10001B.

In a production environment, variables associated with dynamic packages are commonly set by scripts or other processes that determine what applications are required at runtime.

Note

Packages deployed in a task sequence using a dynamic variable will not be listed on the references tab of a task sequence. For that reason, we must initiate a separate pre-cache job for any packages deployed using a dynamic variable. In the **Nomad Windows 10 Ent task** sequence, the Skype package is installed using a dynamic variable.



Now we return to the CM console and select **Packages** from the **Application Management** folder in the **Software Library** node of the ConfigMgr console, then we:

Right-click on the **Skype for Windows 7** package, select **Properties** and go to the **Nomad** tab.

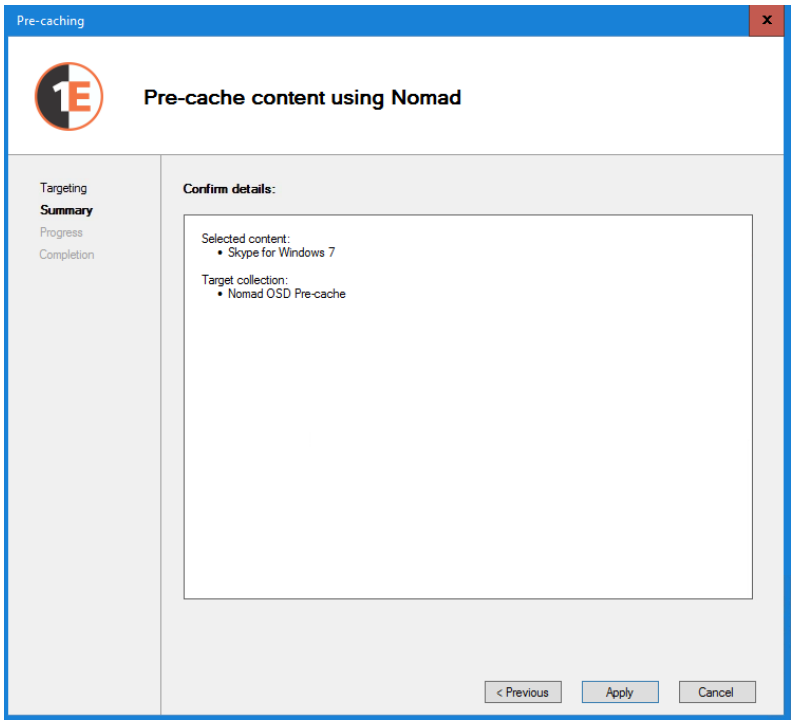
Enable Nomad for the Skype package and click **OK**.

Right-click on the **Skype for Windows 7** package, select **Pre-cache content using Nomad** to launch the Nomad Pre-caching wizard.

On the *Targeting* page, select the **Nomad OSD Pre-cache** collection and click **Next**.

Click **Apply** on the *Summary* page.

When the job completes, click **Finish** on the *Completion* page.



9.3.5.3 Using Peer Backup Assistant (PBA)

In an OS refresh or replace scenario, you will typically need to migrate user data and settings using the **User State Migration Tool (USMT).** In refresh scenarios, USMT will typically achieve this by saving the user state locally in the preserved **_SMSTaskSequence** folder and restoring it after the new OS has been installed, for more details refer to https://docs.microsoft.com/en-us/mem/configmgr/develop/reference/osd/sms_tasksequence-server-wmi-class.

> **Note**
>
> There are two common scenarios where a ConfigMgr State Migration Point would normally be required, such as:

Where the computer is being replaced, so the data needs to be stored off the old device

In a refresh scenario where the task sequence includes a step to format the disk before installing the new OS image, in which case the local **_SMSTaskSequence** folder is lost.

Nomad includes the PBA functionality, which allows a local peer to be used to temporarily store the user state from the computer being built. This removes the need for a User State Migration Point, keeping the user data local. In this example, we enable the Nomad clients as Peer Backup Assistant hosts, allowing them to store user state data that USMT has collected from their peers. We then configure the Task Sequence to include the necessary steps to capture and restore the user state using USMT and the selected Nomad peer as the store location.

Refer to Peer Backup Assistant - PBA for more background and further details, including:

Single-site PBA

High-availability PBA

Configuring PBA hosts

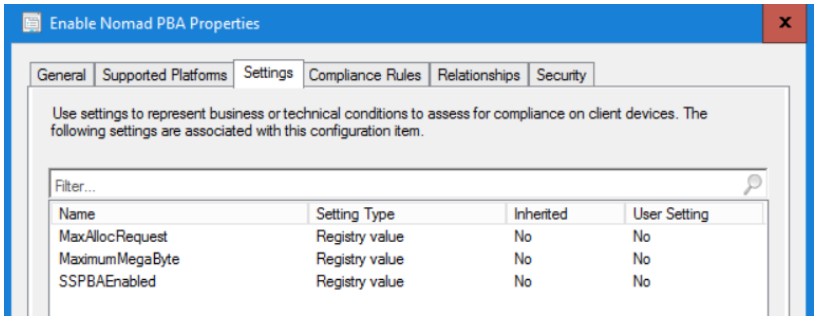
Using PBA with HTTP and HTTPS P2P

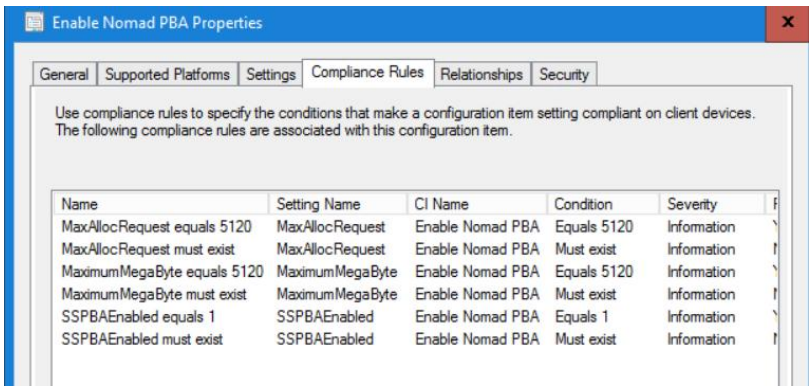
Using PBA with Configuration Manager task sequences.

9.3.5.3.1 Enable Peer Backup Assistant

Peer Backup Assistant (PBA) functionality needs to be enabled on Nomad clients to enable them to become potential hosts for storing user state information from other computers on the subnet. Enabling PBA involves setting the MaximumMegaByte and MaxAllocRequest registry values, the following example uses a ConfigMgr Configuration Item to apply them.

This example shows how you can enable PBA on existing Nomad clients and makes use of a preconfigured ConfigMgr Configuration Item called **Enable Nomad PBA** with the opposite **Settings** and **Compliance Rules**.





From the **Assets and Compliance** workspace we select the **Configuration Baselines** node, right-click our **1E Client Configuration** baseline and select **Properties**.

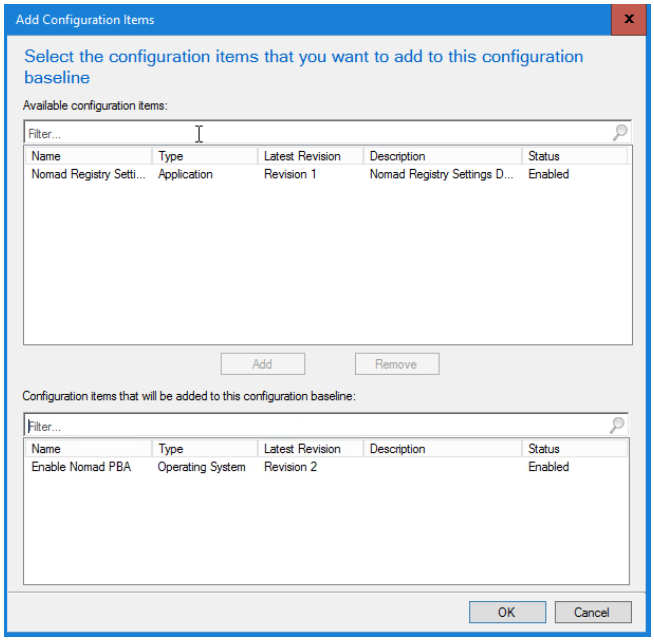
From the **1E Client Configuration Properties** dialog box, we select the **Evaluation Conditions** tab, then click **Add** and select **Configuration Items**

In the **Add Configuration Items** dialog box we select the **Enable Nomad PBA** Configuration Item and click **Add** to add this to the **1E Client Configuration** baseline. We click **OK** to return to the **1E Client Configuration Properties** dialog box, then click **OK** to save the changes.

From the **Assets and Compliance** workspace we select the **Device Collections** node.

Right-click our **Lab Workstations** Collection and then select **Client Notification→Download Computer Policy** to ensure all our clients get the updated configuration baseline.

> **Note**
>
> The Enable Nomad PBA Configuration Item configures the following registry values under the **HKLM\Software\1e\NomadBranch** key in the registry:
>
> **\NMDS\MaximumMegaByte=5120:** The MaximumMegaByte setting defines the maximum space which can be allocated by the peer machine for PBA. This is the amount of disk space you want to allow Nomad to use for PBA functionality.
>
> **\NMDS\MaxAllocRequest=5120:** The MaxAllocRequest is the maximum space that any single machine can use during a PBA task. In a production environment, multiple machines might be offloading user state data onto a single machine, so this setting needs to be defined based on the maximum data expected from any single machine. In our lab, we will only be executing a single task sequence using PBA, so we have configured the setting to the same value as MaximumMegaByte.
>
> **SSPBAEnabled=1:** The SSPBAEnabled setting enables PBA to work in conjunction with Single Site Download.



9.3.5.3.2 Configure the Task Sequence to Capture User State

In this example we add tasks to the **Nomad Windows 10 Ent** task sequence to redirect the store location to a local peer selected at runtime and then capture the user state:

In the ConfigMgr console, we right-click our **Nomad Windows 10 Ent** Task Sequence and select **Edit**.

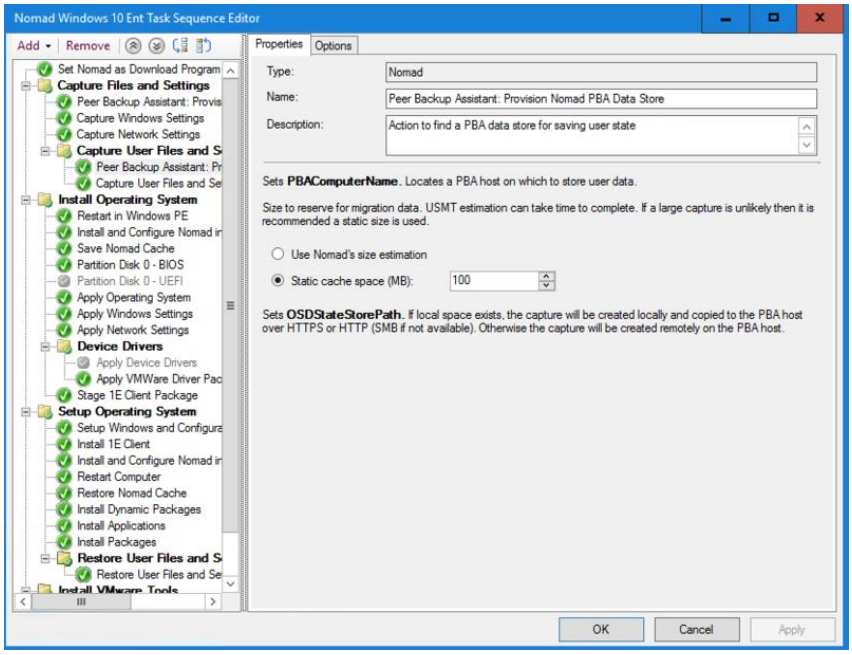
We delete the **Request User State Storage** and **Release User State Storage** tasks in the **Capture User Files and Settings** task group and click **Apply**, then repeat this for the **Restore User Files and Settings** task group.

We select the **Capture User Files and Settings** *task group*, click **Add** and select **1E Nomad PBA→Peer Backup Assistant: Provision Nomad PBA Data Store** .

In the Properties tab, we check the Cache space (MB) is set to **100** and then click **Apply**.

> **Note**
>
> Using the **Peer Backup Assistant: Provision Nomad PBA Data Store** step replaces the native ConfigMgr Request User State Storage step.
>
> Similarly the **Peer Backup Assistant: Finalize Nomad PBA Data Store** step replaces the native ConfigMgr Release User State Storage step in the **Capture User Files and Settings** task group.

> **Note**
>
> In this step, we are setting an arbitrary estimated capacity requirement (100MB) for storing user data. If the Microsoft Deployment Toolkit (MDT) has been integrated into the ConfigMgr environment, using **ZTIUserState.wsf** will estimate how much space is required to store the user state from the current computer and write this to the **USMTESTIMATE** Task Sequence variable, in which case you can enter **%USMTESTIMATE%** in this field.



With the **Capture User Files and Settings** *task* selected, we click **Add** and select **1E Nomad PBA→Peer Backup Assistant: Finalize Nomad PBA Data Store**.

We check the **Enable High Availability** box. By using **Enable High Availability**, we can automatically store additional backup copies of the PBA data store, after the primary data store has been created with **Peer Backup Assistant: Provision Nomad PBA Data Store** and after the USMT data has been saved and closed with **Peer Backup Assistant: Finalize Nomad PBA Data Store**.

In the **Properties** tab, we set the following properties and click **Apply**.

Minimum number of additional backups: **1**

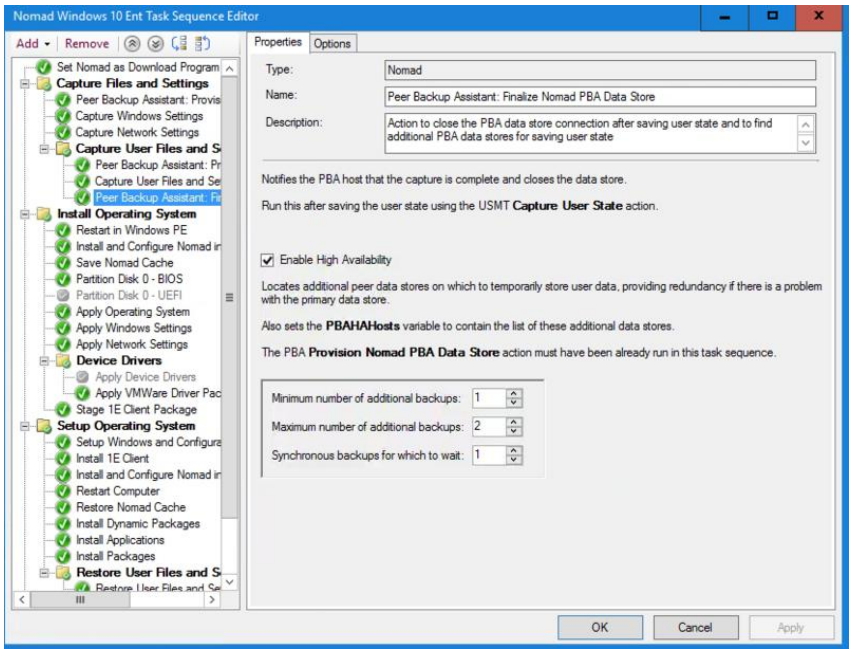
Maximum number of additional backups: **2**

Synchronous backups for which to wait: **1**

Note

The Peer Backup Assistant: Finalize Nomad PBA Data Store step releases the connection to the state store share on the remote computer and results in the saved user state content being preserved for 7 days (configurable using the PostCompleteTimeoutHours value in the **NomadBranch\NMDS** registry key on the store host).

Unless this task is executed, the content is only available for 3 hours (configurable using the PreCompleteTimeoutHours value in the NomadBranch\NMDS registry key on the store host).



9.3.5.3.3 Configure the Task Sequence to Restore User State

In this next step, we add the State Restore steps that complement the State Capture steps configured in the previous task to restore the user state from the local peer when the new OS has been installed.

We right-click the **Restore User Files and Settings** *task group,* select **Move down** so the group is no longer indented within the Setup Operating System group, then we click **Apply**.

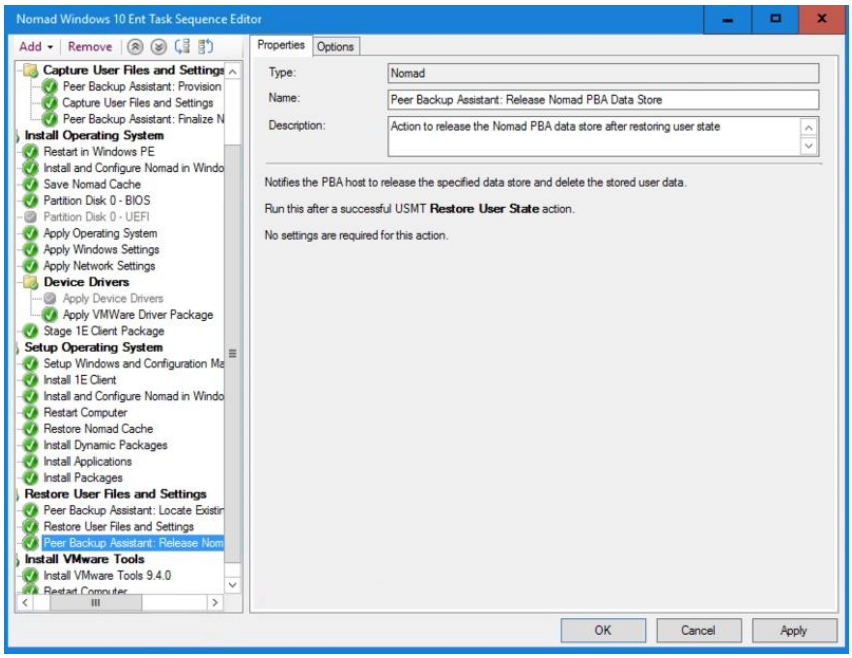
With the **Restore User Files and Settings** *task group* selected, we click **Add** and select **1E Nomad PBA→Peer Backup Assistant: Locate Existing Nomad PBA Data Store** .

> **Note**
>
> Using the **Peer Backup Assistant: Locate Existing Nomad PBA Data Store** step replaces the native ConfigMgr **Request User State Storage** step in the **Restore User Files and Settings** task group.
>
> Similarly the **Peer Backup Assistant: Release PBA Data Store** step replaces the native ConfigMgr **Release User State Storage** step in the **Capture User Files and Settings task group**.
>
> **Note**
>
> This task will get Nomad to locate the user state store location for the computer being built (defined by the COMPUTERNAME Task Sequence variable) and set the OSDStateStore variable to this path in the Task Sequence environment.

With the **Restore User Files and Settings** *task* selected, we click **Add** and select **1E Nomad PBA→Peer Backup Assistant: Release Nomad PBA Data Store**, then click **Apply**.

> **Note**
>
> This step will delete the user state from the peer client and release the disk space for other clients to use for storing state during a migration.

The **Restore User Files and Settings** group now looks like the picture opposite.



9.3.5.4 Performing an OSD refresh using Nomad

Now we have completed our preparation, our **Nomad Windows 10 Ent deployment** task sequence can be used to refresh a Windows 7 client, and migrate it to Windows 10 Enterprise.

9.3.5.4.1 Deploy the Nomad Windows 10 Ent task sequence

To deploy the task sequence and migrate our Windows 7 client to Windows 10:

In the ConfigMgr console, in the **Assets and Compliance** workspace we select the **Device Collections** node and create a Collection named **Nomad Windows 10 Refresh** with **Lab Workstations** as the Limiting Collection and add **1ETRNW72** to the Collection.

We then open the **Software Library** workspace, expand the **Operating Systems** node and select the **Task Sequences** node, then we right-click the **Nomad Windows 10 Ent** task sequence and select **Deploy** to start the *Deploy Software Wizard*.

On the *General* page, we select **Nomad Windows 10 Refresh** as the target Collection and click **OK**.

On the *Deployment Settings* page we ensure the Purpose is set to **Available** and click **Next**.

On the *Scheduling* page we select the **check box** next to **Schedule when this deployment will become available** and keep the default setting.

On the *User Experience* page and the *Alerts* page we click **Next**.

Finally on the *Distribution Points* page, we select:
Download content locally when needed by running task sequence (default).

> **Note**
>
> We chose **Download content locally when needed by running task sequence** to avoid a potential failure due to lack of disk space.

On our computer 1ETRNW72 we open **Software Center** from the desktop, and navigate to the **Operating Systems** node. Then we select **Nomad Windows 10 Ent** and click **Install**.

A dialog box will be displayed asking for confirmation of the of a new operating system. We then click **INSTALL** to run the task sequence.

> **Note**
>
> As an Administrator you will want to know where the content your Task Sequence requires has been cached. You can use the Nomad app to do this using the Task Sequences page to identify things like:

Download Status by Network Site

Device Count by Operating System

P2P Efficiency by Content Source.

In this example, we introduced how Nomad is used to obtain content while a task sequence is executing. The task sequence variable, **SMSTSDownloadProgram**, is set to **SMSTSNomad.exe**, which defines it as the default download program for the task sequence.

The Save Nomad Cache step not only saves the Nomad cache in WinPE to use the reserved folder location, but also gets the content of the offline Nomad cache (in the current OS) and sets that location as the new default cache path and renames and moves the logs into that location as well.

We have shown how the Nomad Peer Backup Assistant can be configured within a task sequence to enable user state to be stored temporarily on a local peer. The process involves:

Enabling the peers for Peer Backup Assistant by modifying values in the NMDS registry key

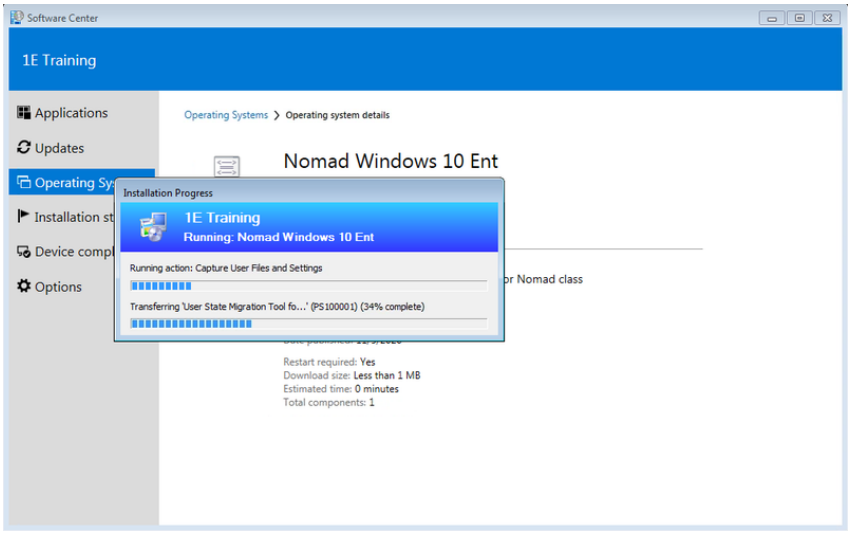
Using the Peer Backup Assistant custom Task Sequence steps to provision a data store on a local peer and setting the OSDStateStorePath variable to that store location

Running the Capture User State task, which copies the user state to the selected peer

Completing the capture to release the connection to the data store and retain the content for 7 days

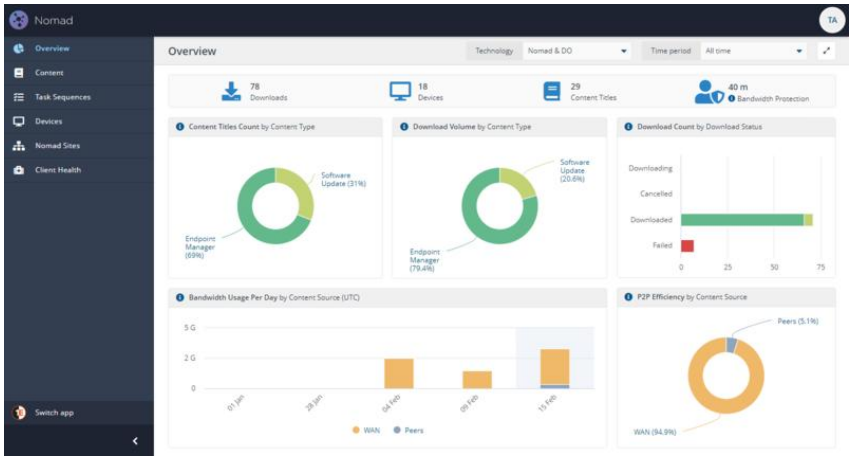
Using High Availability and SSD to offload the USMT data to multiple machines across a defined site

Once the new operating system has been installed, the user state is restored from the same location and finally, the content is deleted from the peer data store to free up space for other peers.



9.3.6 Monitoring Nomad

The Nomad app provides visibility of content distribution activity and cache status for content distributed by both Nomad and Delivery Optimization. This includes Configuration Manager content distributed with Nomad and Software Updates content distributed with either Nomad or Delivery Optimization.



9.3.6.1 Explaining content versions

In Configuration Manager (CM), the content associated with a Package or Application Deployment Type may be updated by an administrator. In the case of Packages, CM increases the Package Version property, and for Application Deployment Types, CM generates a new Content ID for the Deployment Type.

The Nomad Overview page displays summarized distribution data for a selected period. The displayed data shows all downloads and download activity for all versions of content for that period. For example, if a device downloaded Package A version 1 a month ago and later downloaded version 2 of the same Package, the Overview page would reflect both downloads.

In this version it has not been possible to reflect previous versions in the **Content Titles** summary in the top status bar, or in the **Content Titles Count by Content Type** and **Download Volume by Content Type** tiles. These will only represent download activity for the latest version of content. This may result in apparent 'loss' of data (e.g. a reduction in the number of content titles or download volume) when content for an existing Package or Application is updated in CM, as these metrics will only include download activity for the latest version. This will be addressed in a later version of Nomad.

> **Note**
>
> Other pages in the app, such as the Content page, only show the latest version of any given **Content Title**. Those pages concern the current state of things (e.g. where content is available) because only the latest version is usable by CM deployments. As a result, showing older versions would be misleading for users.

The **Overview** page gives a brief snapshot of download activity. The page has multiple tiles showing:

Content Titles by Content type

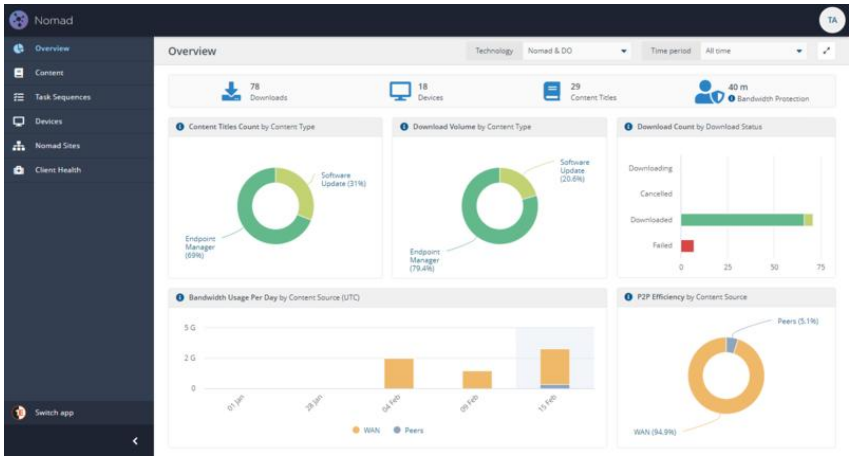
Download Volume by Content Type

Download Count by Download Status

Bandwidth Usage Per Day by Content Source (UTC)

P2P Efficiency by Content Source (Peer to Peer - P2P).

The results can further be narrowed down by using the **Technology** and **Time period** filters on the page.



9.3.6.2 Navigation and Filtering

By default, the view shows activity and status for all time and will show activity and status for both Nomad and Delivery Optimization. These defaults can be modified using the **Technology** filter and the **Time period** filter.

> **Note**
>
> Each content tile can be expanded using the **Expand** button on the top right-hand corner of each tile.

9.3.6.2.1 Time period filter

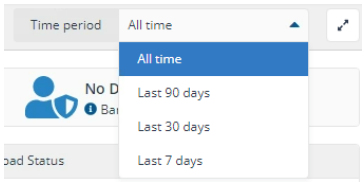
Using the **Time period**filter at the top of the page, you can narrow down the results by date. You can choose from the following options:

Last 90 days

Last 30 days (Default)

Last 7 days.

> **Note**
>
> If these filters are applied to any app page, it is reflected on all other pages in the Nomad App.



9.3.6.2.2 Technology filter

You can use the **Technology** filter to differentiate between downloads through Nomad or Delivery Optimization (DO).

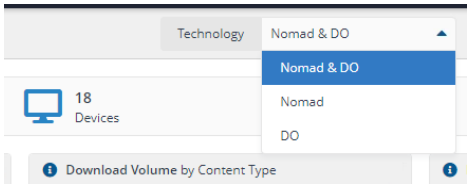
The following options are available:

Nomad & DO (Default)

Nomad

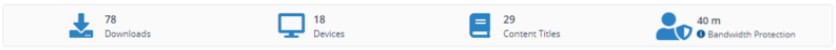
DO.

> **Note**
>
> If this filter is applied to any app page, it is reflected on all other pages in the Nomad App.



9.3.6.3 Top status bar

The status bar along the top of the page shows high-level statistics for the currently selected **Technology** (Nomad or DO) and **Time period**. The bar is shown on the Overview page and includes four icons, **Downloads**, **Devices**, **Content Titles** and **Bandwidth Protection**.



Item	Description	Icon
Downloads	Downloads reflect the total number of content downloads. This includes both Delivery Optimization (DO) and Nomad downloads. The results can be filtered on the **Time period** and **Technology** filters and display the total number of downloads of any version of content that occurred in the selected period. A download counts as any download activity for a given Content Title on a given device. For example, if there are 10 content titles downloaded by 50 devices, the total count of download instances would be 500. For CM Applications, each Application Deployment Type counts as a separate Content Title.	

Item	Description	Icon
	Clicking on this icon navigates to the **Content** page filtered to show **Content Titles** reporting download activity within the selected **Time period**.	
Devices	Displays the total number of devices that have reported download activity for any content version in the selected **Time period**, including: Packages Applications Updates from Configuration Manager. Clicking this icon navigates to the **Devices** view, filtered to show devices where download activity was reported within the selected **Time period**.	
Content Titles	Displays the total number of unique **Content Titles** where download activity of the latest version of the content titleis reportedin the selected**Time period.** For CM content, a**Content Title**is a single Application or Package. Clicking on this icon navigates to the Content view filtered to show the **Content Titles** that have reported download activity within the selected**Time period.** **Note** Applications in CM may have many Deployment Types. This summary counts an Application as a single Content Title.When viewing the Content view, Content Titles for CM Applications are further identified with the Deployment Type thatwas downloaded. So, the total number of Content Titles identified on the top status bar may be lower than the corresponding list of Content Titles on the Content page. This is because the Content page reports download activity for individual Deployment Types of CM Applications.	
Bandwidth Protection	Displays the total time that Nomad backed off when downloading content to protect end-user bandwidth.	

Item	Description	Icon
	Bandwidth Protection allows Nomad to adjust the speed of ongoing downloads to save bandwidth for other business use. Bandwidth Protection ensures Nomad doesn't consume excess bandwidth and hinder other business activity.It does that by tracking the download time of data packets. If the time increases, it slows itself down (backing off) by sleeping for a few moments before downloading another packet.	

9.3.6.4 Content tiles

Content tiles display statistics for content download activity in the following panes:

Content Titles Count by Content Type

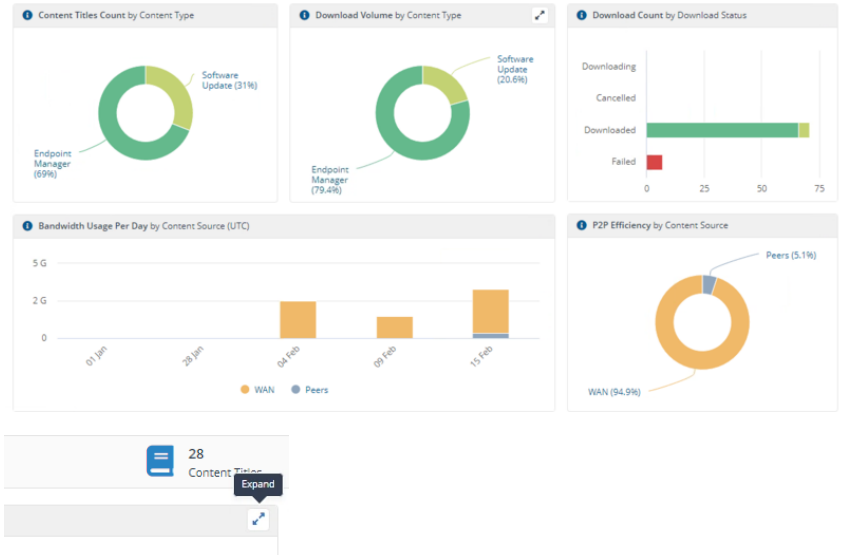
Download Volume by Content Type

Download Count by Download Status

P2P Efficiency by Content Source

Bandwidth Usage Per Day by Content Source UTC.

> **Note**
>
> Each content tile can be expanded using the **Expand** button on the top right-hand corner of each tile.



9.3.6.4.1 Content Titles Count by Content Type

The **Content Title Count by Content Type** tile shows the total number of unique **Content Titles** for where there is download activity reported for the latest version of the content within the selected **Time period**.

The data is grouped by **Content Type** and displayed as a donut chart. The app currently reports on two **Content Types**:

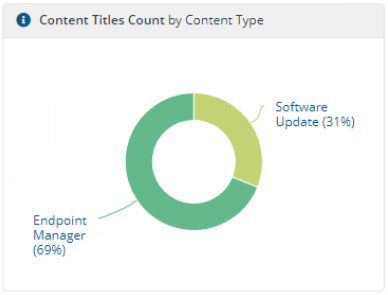
Endpoint Manager - CM applications and packages that are not delivered by DO

Software Update - includes any Microsoft Software Updates deployed through CM or Windows Update.

> **Note**
>
> Applications in CM may have multiple **Deployment Types**. This tile counts an Application as a single **Content Title**. When viewing the **Content view**, **Content Titles** for CM Applications are further identified with the **Deployment Type** that was downloaded.
>
> As a result, the total number of **Content Titles** identified on the top status bar may be lower than the corresponding list of Content Titles on the Content page (which reports download activity for individual **Deployment Types** of CM Applications).

Hovering over a **Content Type** segment of the chart displays the count of **Content Titles** of that type, also represented as a percentage of all **Content Titles**.

Clicking on a **Content Type** segment of the chart will navigate to the **Content** view, filtered to show related **Content Titles**.



9.3.6.4.2 Download Volume by Content Type

The **Download Volume by Content Type** tile shows the cumulative volume of content of the latest version of content downloaded by all devices within the selected **Time period**. The data is grouped by **Content Type** and displayed as a donut chart.

The chart enables you to see the effect that different types of content have on your network, in terms of the volume of data associated with them. It shows the percentage of packages and software updates by volume for:

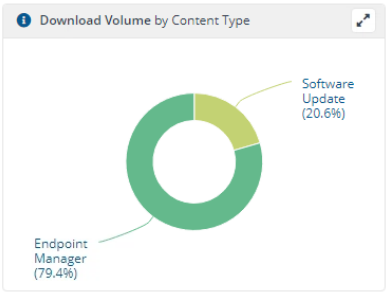
Endpoint Manager - CM applications and packages that are not delivered by DO

Software Update - content that can be delivered by Nomad, or DO if you're using Windows Update directly.

For example, if a single content title is 100MB and it is downloaded by 100 devices, the cumulative **Download Volume** reported for that particular **Content Title** would be 10,000MB. The chart shows the cumulative volume for all **Content Titles** on all devices, grouped by **Content Type**.

Hovering over a **Content Type** segment of the chart displays the total volume of downloaded content of that type. This is also shown as a percentage of total volume of downloaded content.

Clicking on a **Content Type** segment of the chart navigates to the **Content** view, filtered to show **Content Titles** of the selected segment.



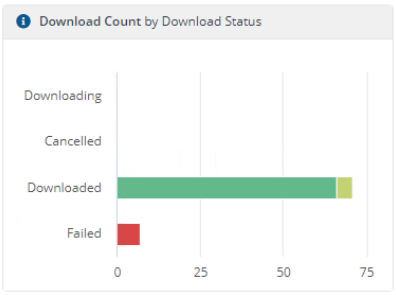
9.3.6.4.3 Download Count by Download Status

The **Download Count by Download Status** tile shows the status of download activity within the selected **Time period**, displayed as a bar chart by:

Status	Description
Downloading	Number of downloads currently in progress, where a download has been reported as started but has not yet reported complete, failed or cancelled.
Cancelled	Number of downloads whose last reported status was **Cancelled**, downloads may be cancelled by the user, or by the system, for example if the system is shut down or higher priority downloads are queued.
Downloaded	Number of successful downloads, if the downloaded content is still cached on a given device, it's represented by the dark green part of the Downloaded bar labelled **(Downloaded (Cached)** when you hover over it. If the downloaded content was subsequently deleted from the cache on a given device, it's represented in the light green part of the **Downloaded** bar labelled **(Downloaded (Deleted)** when you hover over it.
Failed	Number of downloads whose last reported status was **Failed**.

Hovering over any of the bars displays the number of downloads in the selected download state.

Clicking on any of the bars navigates to the **Content** view, filtered to include **Content Titles** where one or more devices is in the selected download state.



9.3.6.4.4 Bandwidth Usage Per Day by Content Source (UTC)

The **Bandwidth Usage Per Day by Content Source (UTC)** tile represents daily download activity throughout the entire network during the selected **Time period**.

A column is displayed for each day when there was download activity. Each column indicates the volume of content downloaded over the WAN (in orange) or from peers (in grey). Hovering over a segment of the column will display the volume of content downloaded on that day.

This view demonstrates the value that Nomad and Delivery Optimization are providing through reduced WAN traffic. If the majority of content is being downloaded over the WAN, it could indicate that peers are simply not available (e.g. users working from home) or it could be an indication that Nomad or Delivery Optimization are not correctly configured to optimize content from peers.

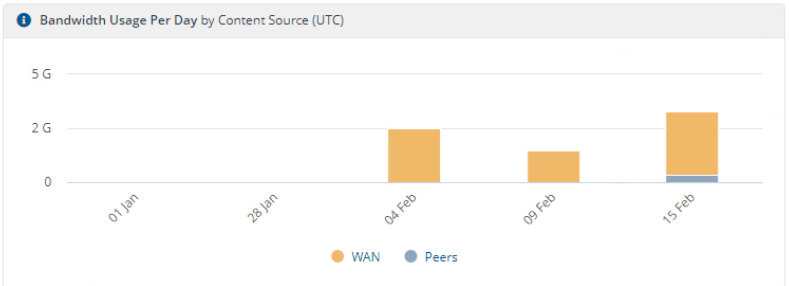
The columns on this chart are not clickable, they are for data visualization only and do not navigate to another view of the data.

> **Tip**
>
> On the Overview page, when you select the **All Time** filter, the **Bandwidth Usage Per Day by Content Source (UTC)** graph displays a maximum 365 days of data.

> **Note**
>
> This chart only displays content that was downloaded over the network either from a peer or from the source (e.g. a CM Distribution Point), if a device:

Requests content that is already in its cache, it will not be represented in this chart

Only has some content in its cache and downloads the remainder of the content from peers or the source, the content that was downloaded will be shown.



9.3.6.4.5 P2P Efficiency by Content Source

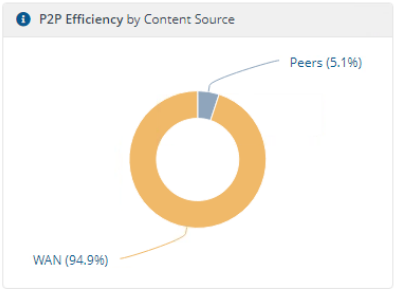
The **P2P Efficiency by Content Source** tile represents the overall peer-to-peer efficiency across the entire network during the selected **Time period**.

The data is grouped by source (Peers and WAN) and displayed as a donut chart showing the volume of content downloaded from peers (in grey) and from the source over the WAN (in orange). This gives an indication of the overall value of Nomad and Delivery Optimization across your organization.

Ideally, more content will be downloaded from peers than from the source over the WAN, which saves network bandwidth. Where this is not the case, it could be due to many users working remotely without any local peers, or it could be due to configuration settings on the client that are not optimized for peer-to-peer caching and availability.

This chart is not clickable, it is summary data visualization only and does not navigate to another view of the data.

> **Note**
>
> In this chart, the volume of content downloaded from peers includes any content requested by a device during the selected **Time period** and was already in the cache at the time (i.e. 'already cached' is represented as content obtained from a peer). If the content was downloaded from a peer or over the WAN during the selected **Time period**, it will be represented accordingly.



9.3.7 Ensuring Nomad is secure

An overview of Nomad security methods, and how to customize default Nomad security settings.

Nomad is a peer-to-peer technology that works by using HTTP/HTTPS or the native Windows OS File and Print Sharing services to share content among computers.

In this section we explain details of Nomad file sharing mechanisms and offer configuration advice related to your desired level of security. Additionally, we describe settings that will affect the sharing of deployment content, as well as settings related to storing user migration data when using Peer Backup Assistant - PBA.

9.3.7.1 Configuration Manager content security

Nomad does not replace existing Configuration Manager (CM) security, so any content distributed by CM, whether it involves Nomad or not, undergoes a hash checking process before it is actioned by the CM client. CM provides a hash of content using the SHA-256 algorithm. CM content on a Distribution Point (DP) has a hash value provided to the CM client through its deployment policy.

When the CM client has received all of its requested content, a hash value of all the content received is generated at the client. This value is compared to the one provided in the policy from the DP source. If a single byte of the content has changed during the transfer between the DP and the client these values will not match, and that content will be deemed to fail the hash check, this ensures that any content that fails the hash check is not executed.

9.3.7.2 Nomad security methods

This table summarizes security methods for Nomad operations, including both content deployment and user data migration.

Component	Detail
Election Process	AES 256 is used when you enable FIPS compliant communication encryption during the Nomad agent install FIPS compliance is disabled by default When FIPS compliance is disabled, RC2 block encryption is used.
Nomad Share and NTFS Permissions	SMSNomadP2P&-Local Account Nomad known pwd (SMB Share-Read) Authenticated Users-Domain Authenticated Account (SMB Share-Read) SYSTEM-NTFS Write-Option to limit to Machine Account (SMB Share – Read).
HTTPS Peer copy (Optional)	Encryption - Microsoft Cryptographic Provider – 256 Bit Symmetric Key Cipher Data Encryption – AES256 Algorithm with 256 key length
Nomad Hash Check Process	Content Hashing Algorithm – SHA 256
ConfigMgr Hash Check Process	Content Hashing Algorithm – SHA 256
Nomad Peer Backup Assistant - PBA Poll and ind	Microsoft Cryptographic Provider – 256 Bit Symmetric Key Cipher Data Encryption – AES256 Algorithm with 256 key length
HTTPS Nomad PBA user data copy to and from PBA host	Encryption - Microsoft Cryptographic Provider – 256 Bit Symmetric Key Cipher Data Encryption – AES256 Algorithm with 256 key length

Component	Detail
Nomad PBA USMT user data encryption	In Replace scenarios where a native Configuration Manager (CM) Computer Association (CA) is used, user data is encrypted using AES 256 with the randomly generated key securely stored in the CM database. This occurs before the data gets copied to the target PBA Host For Refresh or Replace scenarios not using the native CA, AES 256 is used to encrypt user data, with the key being generated by Nomad, the key gets generated when the task sequence runs and is never stored remotely.

9.3.7.3 How Nomad manages content and secures user data

In this section, we'll separate out the way Nomad manages content and the methods behind securing user data when using Nomad Peer Backup Assistant - PBA. These two approaches to securing data are the same in principle, but contain essential differences, that we'll highlight in the following sections.

9.3.7.3.1 Securing captured user data

In this section, we'll describe how Nomad incorporates encryption into the remote storage of captured user data. When using Nomad PBA, it can be important that captured user data is stored encrypted prior to it being restored on to a target device and deleted from the former storage hosts. The following sections explain how this is implemented.

9.3.7.3.1.1 Configuration Manager computer associations

Configuration Manager (CM) supports encryption of captured user data, with the encryption key stored in the CM database. The key is retrieved using the management point server during capture and restore operations within a task sequence. To acquire the key, the requesting host must be authenticated using the CM client certificate. Nomad PBA supports use of this key, and when the task sequence runs, the downloaded key is stored in the task sequence environment.

When running under a full OS, the task sequence environment is secured by applying the Windows file system, share and logon security typically applied using Group Policy. When running in WinPE, the security environment is different.

9.3.7.3.1.2 Task sequence environment and WinPE

During the WinPE phase of the running task sequence, the local host is not a member of the domain, and an interactive logon is not possible. The only way a user can interact with a host is through a Windows command shell. For this to be possible, command shell access must be explicitly enabled during boot image creation in the Configuration Manager console.

Typically, command shell access is only enabled during task sequence development to facilitate troubleshooting. In a production environment, command shell access is usually turned off. Windows share access is not possible in WinPE.

9.3.7.3.1.3 When encryption is not required

In User State Migration Tool (USMT), encryption of captured user data must be enabled on the command line of the USMT scanstate.exe application. In some circumstances you may prefer not to encrypt captured data, and instead maximize ready access to the stored data when performing the restore. In this case the unencrypted data is secured only through the NTFS and share permissions implemented in Nomad PBA.

For some instances of OS deployment, securing captured user data is not even required. In an OS Refresh, USMT makes use of Windows file-system hard-links. In this scenario, user data is never stored off the local disk and Nomad PBA or an SMP is not required.

9.3.7.3.2 Transferring content and user data between peers

This section discusses how you can implement to help content and user data transfer between peers.

9.3.7.3.2.1 Nomad election and PBA traffic

Nomad election and PBA traffic is communicated over port 1779 by default (You can configure this if needed). It is also encrypted with the Microsoft Base Cryptographic Provider using the AES 256 encryption algorithm with a 256-bit key length.

9.3.7.3.2.2 Transferring content using SMSNomadP2P&

You can transfer content between peers using either the local computer account or the local account, SMSNomadP2P&. The Nomad agent is responsible for managing the password when using the SMSNomadP2P& local account, with the password synchronized between peers. To ensure a secure password, a new password gets regenerated on every Nomad agent service startup, when your computer reboots, Nomad resets the password.

The SMSNomadP2P& account password is complex and set to 14 characters long, and the account denied “Log on locally” security rights. This behavior cannot be changed as it's hard coded into the product. This feature is more secure than using Active Directory accounts because no one can know the password used, this password is different for each local SMSNomadP2P& account.

The 14 character password for SMSNomadP2P& is calculated based on a public hash shared by the master during election and a private (secret) hash. At start-up, Nomad generates a new private hash and password. The private hash gets communicated using encrypted communications during an election, and peers work out the password by applying the same algorithm. If that password gets altered, no other device could connect to the NomadSHR or Cache folder without a way of communicating that password out to every system that would need to use it.

> **Note**
>
> Please refer to The Nomad share for more details about Nomad share security, for more details about:

Enhanced Nomad share security

Nomad Branch service and the Nomad share

Custom share permissions.

9.3.7.3.2.3 Transferring user data

For Nomad PBA, we have an additional, unique local account created by Nomad that's used to transfer user data between source and target devices; user data gets stored in the NMDS share on the participating Nomad PBA host. A unique account gets generated each time user data gets stored on a remote host and takes the format **NMDSUser<number>** for example, NMDSUser0001. The local computer account cannot be used when transferring user data.

The password for the local account gets synchronized in the same way as the SMSNomadP2P& account. The PBA local account gets assigned full permissions and rights to the NMDS share and NTFS folder on the PBA host. No other accounts get assigned permissions. Nomad also creates the NMDSUsers local group, to which it adds the NMDS account(s).

9.3.7.3.2.4 Active Directory considerations

Both HTTP/HTTPS and Windows File and Print sharing requires authentication to ensure secure access to cache content or user data that's shared or accessed. In an Active Directory Domain, Group Policy refers to this as network login rights. The Local Computer Security Policy must be modified, assigning the local account SMSNomadP2P& to the setting Computer Configuration→Policies→Windows Settings→Security Settings→Local Policies→User Rights Assignment→Access this computer from the network. For Nomad PBA, customers must assign the above rights to the **NMDS_Users** local group.

If Active Directory Group Policy enforcement is in place, ensure that the SMSNomadP2P& local computer account has access granted to the **Access this computer from the network** settings at the Active Directory Group Policy level.

The File and Print Server service is not available in WinPE and therefore the Nomad share will not exist. For this reason, the Nomad agent in WinPE will only be capable to copy content from a Nomad master running in the full OS and is not able to act as a master itself. The process of accessing and copying content from the remote cache is the same in WinPE as in the full OS and is done using a local SMSNomadP2P& account. Using the local computer account to connect to the remote share is not supported.

Note

Nomad PBA does not support off-line (WinPE) user data capture and restore.

9.3.7.4 Changing the default behaviors of the Nomad security model

So far, we have described the default behavior of Nomad. Organizations that have more strict security policies may wish to adjust the default behavior of Nomad. These options can be configured in the Windows Registry.

You can find these values in the following registry location:

For 32-bit systems - HKLM\Software\1E\NomadBranch

For 64-bit systems - HKLM\Software\Wow6432Node\1E\NomadBranch.

9.3.7.4.1 Using HTTP and HTTPS

Nomad 6.2 introduced Peer copy over HTTP or HTTPS. Configuring Nomad to use HTTP/HTTPS means that Nomad Peer BackUp Assistant (PBA) uses the transport to transfer USMT capture data between the capture/restore and PBA hosts.

By default, Nomad uses the SMB transport. Implementing HTTP/HTTPS requires additional Windows Installer properties need to be specified when installing or upgrading the NomadBranch agent. For existing installations of the agent, the registry will need to be updated, in order for Nomad to use HTTP or HTTPS.

The principal registry setting used to configure Nomad is P2PEnabled. By configuring this setting, the agent can be configured to use either SMB, HTTP or HTTPS and, if required, fall back to using a different transport. The values for selecting the transports are:

Registry setting	Explanation
P2PEnabled = 0x0001	P2P enabled. This option is set by default and enables Nomad P2P using SMB. When set, the Nomad agent will create the NomadSHR file share started, unless the CustomShare option has been enabled in SpecialNetShare. When P2PEnabled is set in addition to Bit 5 (use HTTP) or Bit 6 (use HTTPS), Nomad will attempt to use HTTPS/HTTP and will fall back to SMB if HTTPS/HTTP is unavailable on other peers. To disable SMB P2P, set this bit to 0.
P2PEnabled = 0x0020	Use the HTTP protocol to share its own cache and access other caches.
P2PEnabled = 0x0040	Use the HTTPS protocol to share its own cache and access other caches.

Other registry values are used to set the HTTP/HTTPS ports and configure the use of HTTPS and PKI, for example:

P2PHTTPPort

P2PHTTPSPort

CertIssuer

CertSubject

P2PSSLSettings.

> **Note**
>
> P2PSSLSettings indicates that Nomad should use a PKI or self-signed certificate. If using a PKI certificate, then you must specify Certissuer and CertSubject.

Using file and print sharing

You can use the SpecialNetShare registry value to configure security options. SpecialNetShare can be a combination of multiple options by combining the bit values. You can find a complete list of options for this registry key in SpecialNetShare. If you change the default settings, ensure you apply the same setting consistently on all Nomad Clients.

9.3.7.4.2 What if Windows file and print sharing and HTTP/HTTPS are disabled?

If the File and Print sharing is unavailable, we recommended you configure Nomad to use HTTP or HTTPS, which are also supported when you use Nomad in WinPE.

If Windows File and Print Sharing and HTTP/HTTPS is not allowed on the local host due to security restrictions, then the Nomad is still able to copy content using the SMB protocol from a peer who happens to have Windows File and Print Sharing enabled. However, the local host will not be able to act as a master and serve content to other peers. This is the case in WinPE, where Windows File and Print Sharing is unavailable. Nomad clients running in WinPE are still able to access remote peer cached running under the full OS using SMB.

In any set ConfigMgr task sequence, to use Nomad in Windows PE, in the**Install Nomad** task sequence step configure P2PEnabled=0x0007. This is the combined value of having P2P enabled and allowing the device to act as a P2P server and client if you wish the WinPE Nomad agent to act as a master.

> **Note**
>
> Normally, you would not want a WinPE Nomad client to act as a master as this state tends to be transitory with several reboots occurring.

9.3.7.5 Configuration table

The following table summarizes the configurations discussed on this page.

Device state	Default Configuration	HTTPS	Device account Security (Not applicable to Nomad PBA)	Connection-less (UDP) (Not applicable to Nomad PBA)
Full-OS	Account: <COMPUTERNAME>\SMSNomadP2P& Account: <COMPUTERNAME>\NMDSUser<nnnn> Group: <COMPUTERNAME>\NMDSUsers Password:	**Client (Peer) Authentication:** Account: <COMPUTERNAME>\SMSNomadP2P& Account: <COMPUTERNAME>\NMDSUser<nnnn> Group:	Account: <DOMAIN>\<COMPUTERNAME>$ Password: Unknown; auto-generated; managed by AD Nomad Share permissions: Uses defaults, for example	P2PEnabled = 0x0007 0x0001 (P2P enabled) 0x0002 (P2P server) 0x0004 (P2P client)

Device state	Default Configuration	HTTPS	Device account Security (Not applicable to Nomad PBA)	Connection-less (UDP) (Not applicable to Nomad PBA)
	Unknown; auto-generated by Nomad during service restart. For PBA automatically generated during PBA. Nomad Share permissions: Uses defaults, for example Authenticated Users, SMSNomadP2P& NMDS share and folder permissions NMDS_User<nnnn> Full access	<COMPUTERNAME>\NMDS_Users Password: Unknown; auto-generated by Nomad during service restart. For PBA automatically generated during PBA. **Server (Master) Authentication:** Certification based authentication, either PKI or Nomad Self-signed certificate used.	Authenticated Users Group Policy: Add Domain Computers	
Windows PE (Not applicable to Nomad PBA)	Account: <DOMAIN>\SMSNomadP2P& Password: Manually created and managed by ConfigMgr admins	Account: <COMPUTERNAME>\SMSNomadP2P&> Password: Manually created and managed by ConfigMgr admins	P2PEnabled = 0x0005 0x0001 (P2P enabled) 0x0004 (P2P client)	

9.4 Nomad features

Many Nomad (Nomad) features are available with minimal configuration of the Nomad client. However, some features require additional configuration of the client on Configuration Manager Distribution Points.

Nomad features maximize download efficiency in branch network deployment scenarios, and reduces the number of Configuration Manager Distribution Points. Nomad integrates closely with Configuration Manager, assists with WAN link usage efficiency during downloads, copes with different network protocols.

9.4.1 Nomad features and concepts

With Nomad, you get all the benefits you would expect from Nomad with the additional benefits of the Tachyon platform, included in the license fee:

Increased patch compliance by ensuring clients are functioning, and you are able to deploy updates to them at all times.

Total control over downloads in your environment with the ability to stop them in their tracks if needed.

Centrally managed content in the Nomad cache on clients, with the ability to remove content from any client in real time.

9.4.1.1 New features in Nomad

Many Nomad features are available with minimal configuration of the 1E Client. However, some features require additional configuration of the 1E Client on Configuration Manager Distribution Points.

9.4.1.1.1 Platform

Works with Tachyon 8.1

Insights on how Nomad enhances user experience - with the rapid shift to a Work From Anywhere (WFA) workforce and an increased focus on the Digital End-User eXperience, Nomad on Tachyon Platform now provides insights into how it helps to ensure a great user eXperience. With the introduction of Nomad's Bandwidth Protection Reporting, you can now see how Nomad is preventing end-user disruption due to software and update deployments. Bandwidth Protection Reporting will allow you to see the positive impact Nomad is having across the organization, to individual sites, subnets, all the way down to a single client.

Support for Cloud-based content in Task Sequences - cloud-based services to support Work From Anywhere (WFA) users are becoming more critical to the way enterprises work, there is an increased reliance on Cloud Distribution Points for distributing content.

Feature improvements - as Configuration Manager evolves and new features are released, Nomad on Tachyon Platform is being continuously maintained to ensure it works seamlessly with new releases.

9.4.1.1.2 Client

NomadBranch 8.1 client is the Nomad module in 1E Client 8.1

Support for Cloud-based content in Task Sequences - cloud-based services to support Work From Anywhere (WFA) users are becoming more critical to the way enterprises work, and there is an increased reliance on Cloud Distribution Points for distributing content.

Enhancements:

Improvements to the Certificate Selection criteria to authenticate with a DP (or any download source)

Download reporting now includes back-off data, for Bandwdith Protection Reporting.

9.4.1.1.3 Tools

Nomad AdminUI Console Extensions now require .NET Framework 4.8

Cloud infrastructure support

Enhancements:

Provide a way for SCCM Console users to use alternate credentials to authenticate with ContentDistribution/Platform, for details refer to Using Nomad pre-caching.

PlatformUrl validation is improved, by logging a warning during installation. In UI mode users have the option of continuing with the installation, for details refer to Installing Nomad Branch Tools.

9.4.1.2 Modern management

Nomad provides a way of managing legacy and modern applications in a unified way by providing enhanced oversight, security, and awareness to IT departments, with a particular focus on Delivery Optimization (DO). The following table describes the Nomad capabilities:

Nomad capability	Nomad feature	Uses Platform features
Content Distribution	**Bandwidth management and peer sharing** Protect the WAN when downloading from DP and share content with local peers. Refer to Nomad fundamentals: Full control over WAN link usage.	✓
Single Site Download Share content across subnets in the same location. Refer to Single Site Download.	✓	
Pre-caching Get content distributed ahead of important deployments. Refer to Nomad Pre-caching.	✓	
Cache management Periodically delete unused content from the cache. Refer to Cache management.	✓	

Nomad capability	Nomad feature	Uses Platform features
Cloud-attached CM support Download content from Cloud DP / Content enabled CMG. Refer to Cloud Support.	✓	
OS Deployment	**Peer Backup Assistant** Use available storage on peers instead of servers to temporarily store user state during OS deployment. Refer to Peer Backup Assistant - PBA.	✓
PXE Everywhere Dynamic peer-based PXE eliminates the need for PXE servers. Refer to Using Nomad with PXE Everywhere.		
Nomad OSD Tools Nomad support for Configuration Manager OS Deployment. Refer to Nomad OS Deployment task sequence actions.		
Nomad Management	**Nomad app** Real-time visibility of what content is downloading or available in each location, subnet, and client. See how much WAN traffic is being saved overall and each day. Refer to the Nomad app.	✓
Delivery Optimization (DO) Visibility		

Nomad capability	Nomad feature	Uses Platform features
Real-time visibility of Delivery Optimization downloads and content availability in each location, subnet, and device.		
Nomad Download Pause Immediately stop Nomad downloads across your network or on specific CM Collections. Refer to Nomad Download Pause.		
Client Health	**Nomad Client Health** Real-time monitoring to ensure Nomad is running, can communicate through the firewall, is correctly registered with the CM client, its cache share is accessible. Refer to Nomad Client Health Policy.	✓
MEMCM Client Health Real-time monitoring to ensure the CM client is installed, running and assigned to the correct site, it is communicating with the MP, supporting services are running and WMI is healthy, with real-time remediation for many client issues. Refer to MEMCM Client Health Policy.	✓	
Windows Client Health Check for application crashes, free disk space and WMI repository health. Refer to Windows Client Health Policy.	✓	

9.4.2 Content Distribution

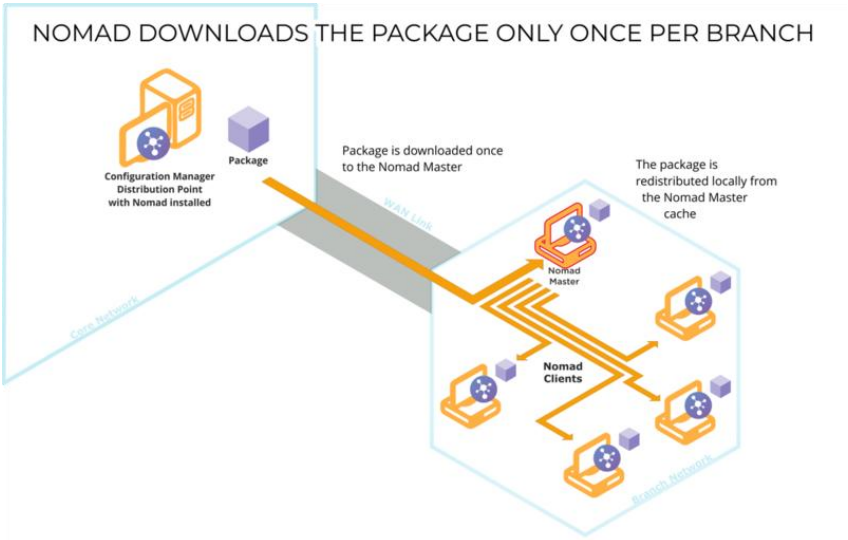
1E Content Distribution is a Tachyon Consumer providing control and visibility on content deployments and delivery in an organization.

9.4.2.1 Download once to branch

Nomad ensures that software packages are only ever copied once per branch over the WAN, utilizing local computers as temporary file caches to distribute the software locally. This reduces the bandwidth required for delivering software updates and means that small offices or sites connected by poor network links can receive software updates more reliably.

The Nomad clients with local copies of the package can themselves act as the master if the need arises. This significantly reduces the number of Configuration Manager servers required to manage a Configuration Manager hierarchy, thereby reducing initial and ongoing maintenance costs.

Refer to Deploying software with Configuration Manager for example scenarios about deploying Applications and Packages where Nomad is integrated with Configuration Manager and how you can monitor those deployments using the Nomad app.

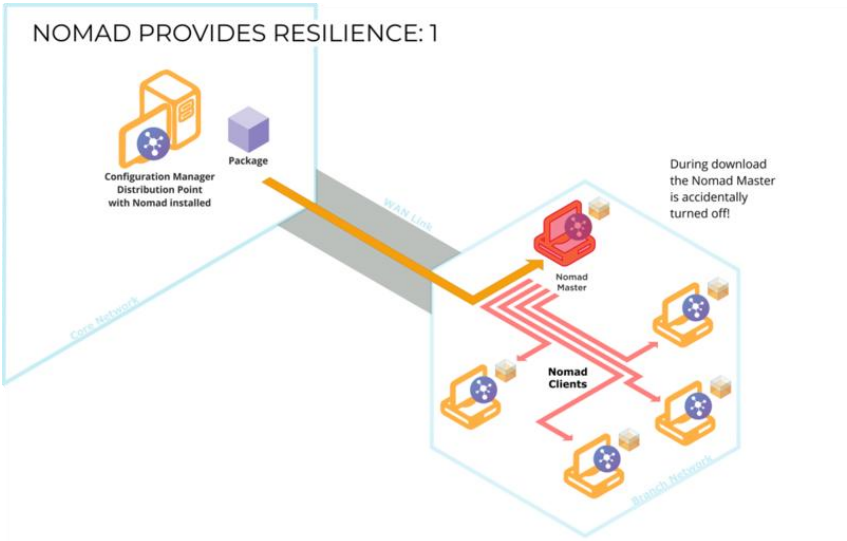


9.4.2.1.1 Nomad Master Elections

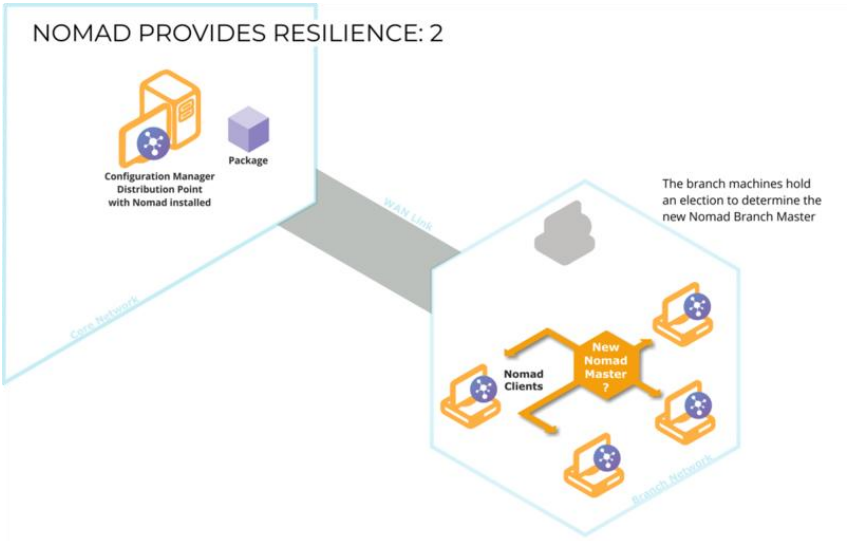
When a software package is deployed to the Nomad clients, an election is held per subnet in the branch to find an appropriate Nomad master, this Nomad master then downloads the software. The software is stored in the Nomad share which is then accessed by the other Nomad clients on the same subnet that require the software package.

Nomad is installed on each computer in the branch and on the distribution point. The computers on the branch network elect a local master. This acts as the single contact point for downloading packages from the distribution point and handles the local redistribution.

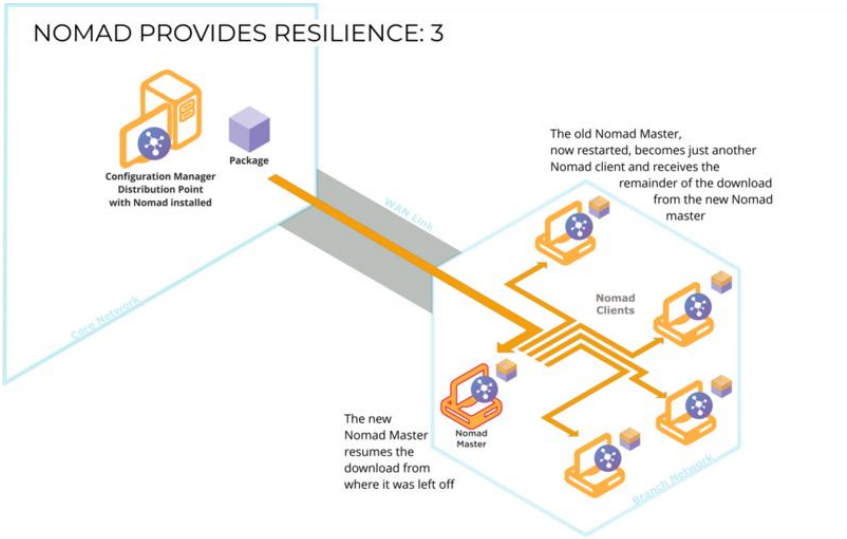
It is possible that a particular Nomad master may be affected in some way during the download. It could be turned off or disconnected from the network for example. If this is the case Nomad ensures that the download continues.



During download, elections continue to be held periodically to determine if the current Nomad master is still the most suitable candidate. If the local Nomad master is affected some way, for example if it is turned off during a download, the other Nomad clients on the branch network interact to elect a new master. The elections are weighted towards the most suitable candidate using a combination of rules.



Once a new master is elected, the download continues to this new master starting from the point at which the download is currently at in that client's cache. The other treat this new master in exactly the same way as the previous master. In fact, if the previous master is turned back on, it may receive the rest of its interrupted download from the new master instead.



See Election rules and master elections for more details about the election process.

9.4.2.1.2 Nomad cache

An overview of the Nomad cache including different methods used by Nomad peers to access the cache on the elected master. The Nomad cache is essential to Nomad's download once to branch feature. The cache enables Nomad to hold its downloaded content so that it can be distributed locally to other Nomad peers. The Nomad cache contains downloaded content (such as packages, applications, and software updates) which can vary in size from relative small patches to rather large OS image files.

As outlined above, Nomad combines the use of elections and cached storage to ensure that content is only downloaded once per subnet over the WAN. Further efficiencies can be made by implementing the Single Site Download advanced feature to ensure that downloads over the WAN only occur once per site.

Note

Refer to Nomad cache for more details, including peer access methods, switching between wireless and wired network connections and multi-forest environments.

9.4.2.1.3 Election rules and master elections

When you install Nomad on computers within a remote branch, part of the installation includes a service called *NomadBranch.exe*. This service runs continuously on the Nomad clients and manages the process of electing masters and transfers the download between peers.

As a package is deployed to computers within a remote branch, one branch Configuration Manager client is elected as the Nomad master. This client downloads the package to its local cache and the other clients on the remote branch IP subnet uses this local master as an alternative distribution point. The other clients can either connect to the local master over HTTP[S] or they connect to its cache folder over Microsoft Server Message Block (SMB) protocol and download the package to their own cache.

Note

Standard Configuration Manager behavior remains unchanged when using Nomad. Nomad clients will not start to download the package until they have received the Configuration Manager deployment, subject to the usual polling cycle.

However, if this elected master became unavailable, the Nomad clients hold an election to nominate another master. The election process starts when the master is discovered to be unavailable.

A master is elected based on election rules including percentage of the package already downloaded and election weighting. Any one of the remote Nomad clients can be elected as a master, even when they are halfway through downloading a package. In this way, software is downloaded once over the WAN and distributed locally.

Cached packages are kept on the local computer. If disk space becomes restricted, a separate automatic cache cleaning process is initiated which deletes packages cached by the peer-to-peer process.

9.4.2.1.3.1 Election rules

Elections for a master occur on a per package basis and are called for the following reasons:

Whenever any Configuration Manager deployment with Nomad enabled in the package properties starts

When a computer which is copying content from a master notices that the master is no longer available – this may happen if the master is switched off or disconnected from the network

Every 5 minutes while a master is actively downloading to ensure a more suitable master (one with more content than the currently elected master) has not been introduced to the network since the last election.

The outcome of an election is decided using the following criteria in order of precedence:

Percentage of content already cached (it is only ever deemed to be 100% once it has been verified)

Election weighting (the higher weighting value wins)

Current master

Time since cache was last verified by Nomad

System uptime (amount of time the computer has been up and running)

Computer initiating the election

Computer name (alphanumeric).

9.4.2.1.3.2 Election weighting

Nomad performs automatic weighting depending on its situation, according to the criteria listed below, and stores the value in memory (not registry). The higher the value, the greater the probability of winning the election.

61 – the agent is running on a server OS and it is not a domain controller (DC)

40 – the agent is running on a laptop

30 – the agent is running on a wireless network

10 – the agent is running on WinPE

50 – default

If necessary, you can use the P2PElectionWeight registry setting to increase or decrease a Nomad client's probability of being elected a master. The range for this registry value must be between 0 and 99 inclusive. If not set, Nomad uses the values listed above.

The registry key is located at: *HKLM\software\1e\NomadBranch\P2PElectionWeight*

To take effect after setting the registry value, the client sevice must be restarted.

This method is not recommended because Nomad is already quite efficient in the way it elects a master and needs very little intervention in this process. However, you may want to reduce the chance of computers with low processing power, or prevent critical servers, becoming a master.

You should also consider the following points before you influence the weighting:

Use this technique in exceptional circumstances and only after testing has shown that you need to make a particular computer more or less likely to be elected as a master for specific operational reasons.

Choose the simplest weighting strategy possible - for example, set servers at 90, laptops at 10 and workstations at 50.

The weighting does not guarantee that the more heavily weighted computers will win the election – they may be turned off or another local peer may have already cached more of the requested content.

The final weighting value used by the computer during an election may differ from the registry value as Nomad will automatically adjust it depending on the chassis and the network connection used.

In the event you no longer need the values to be set, you should remove it and restart the service to resume dynamic election weighting.

Setting to 0 is a special case called Sensitive server weighting designed for use on critical servers. The 0 value prevents Nomad from acting as master, and devices with this value will not respond to election requests.

9.4.2.1.3.3 Sensitive server weighting

You can exclude computers from the election process by updating the P2PElectionWeight registry value to 0 (zero) and restarting the service – if you do not restart the service, the update will not take effect and the computers are still available for election. Computers with this registry value will not respond to election requests and are never considered candidates for elections. We also recommend you set the *SSDEnabled* registry value to 1 if you are using the single site download feature as this will enable the device to consume content from an SSD peer but not be a provider.

When using the default Nomad configuration, Nomad will not respond to elections on a DC and cannot be elected as a master. This is because it is not possible to create the local SMSNomadP2P& account on a DC and allow it to become a Nomad master. To prevent Nomad from becoming a master, set its weighting to 0. The topic on Nomad scenarios illustrate how elections are carried out and how it ties in with downloading installation packages, refer to Basic Nomad behavior in a simple environment.

9.4.2.1.3.4 Inhibiting sites and subnets

You can also define subnets and AD sites where computers will download but not participate in Nomad election, refer to Design Considerations: Inhibiting subnets and sites. This feature is useful for sites that have a local DP or a VPN without isolation.

Typically, VPN solutions isolate each client using single-node subnets (i.e. each client is in its own subnet with a 32-bit subnet mask). This is to prevent broadcast traffic between VPN clients that are typically geographically dispersed and not on the same local network. If the VPN solution is not configured in this manner and clients get an IP address with a subnet mask less than 32 bits, broadcasts can be exchanged between the VPN clients allowing Nomad to elect a master that is not on the same local network.

9.4.2.1.4 Distributing software with Nomad and Configuration Manager

Nomad integrates with the Configuration Manager (CM) client content download process. When Nomad is installed, it registers with the Configuration Manager client as an Alternate Content Provider (ACP), which means the CM client will use Nomad as an alternative to BITS when it requires content if Nomad is enabled for the requested content object. Nomad can be enabled on individual packages (including Driver Packages, Operating System Images, Operating System Upgrade Packages and Boot Images) and Task Sequences.

For Applications and Software Updates, Nomad is enabled on each client for all Applications and Software Updates through Default Client Settings. When the CM client requires Nomad-enabled content, it passes a request to Nomad, which in turn downloads the content, places it in the CM client cache and passes back to the CM client for execution. The 1E Client (with Nomad client module enabled) must be installed on all CM client machines and on all Distribution Points (DP).As well as enabling Nomad on the CM content objects as described above, additional options can be configured in the same manner. For example, you can set the priority for package downloads, interrupting less urgent downloads and then carrying on from where they left off. You can also configure Nomad to send status messages to CM that show the progress for package download.

Refer to Deploying software with Configuration Manager for example scenarios about deploying Applications and Packages where Nomad is integrated with Configuration Manager and how you can monitor those deployments using the Nomad app.

9.4.2.1.4.1 Supported Configuration Manager content sources

Nomad is able to download content deployed through Configuration Manager (CM) from the following sources:

Distribution Points - using either HTTP (default) or HTTPS (requires Nomad client configuration)

Cloud Distribution Points - using HTTPS (requires client configuration)

Cloud Management Gateway (CMG) - configured to function as a Cloud DP

Microsoft Update - where the Software Update deployment has been configured to download from Microsoft Update when the content is not available on a DP.

When the CM client instructs Nomad to download content, it provides a list of sources from which the requested content is available. The list of sources is prioritized as follows:

On-premises DP - based on Boundary Group configuration.

Microsoft Update - exclusively for Software Updates when this option is enabled in the Software Update Deployment.

Internet-facing DP.

Cloud DP or **CMG** - configured to function as a Cloud DP.

The Nomad elected master attempts to connect to each content source in the prioritized list in turn and will download the content from the first available source in this list. The elected master then shares this content with other peers on the network as described in the Download once to branch feature.

9.4.2.1.4.2 Nomad and Configuration Manager

Nomad can be set as a content provider for individual instances of the following types of Configuration Manager (CM) content. In the Configuration Manager Console, navigate to **Software Library → Overview** and then to one of the following:

CM Console node	Sub-node	Action
Application Management	**Packages**	Select a package.
Operating Systems	**Driver Packages**	Select a driver package.
Operating System Images	Select an operating system image.	
Operating System Upgrade Packages	Select an operating system upgrade package.	
Boot Images	Select a boot image.	
Task Sequences	Select a task sequence.	

Right-click and select **Properties**or click on**Create** to start a **New Wizard**. Nomad properties is then accessible on the **Nomad** tab.

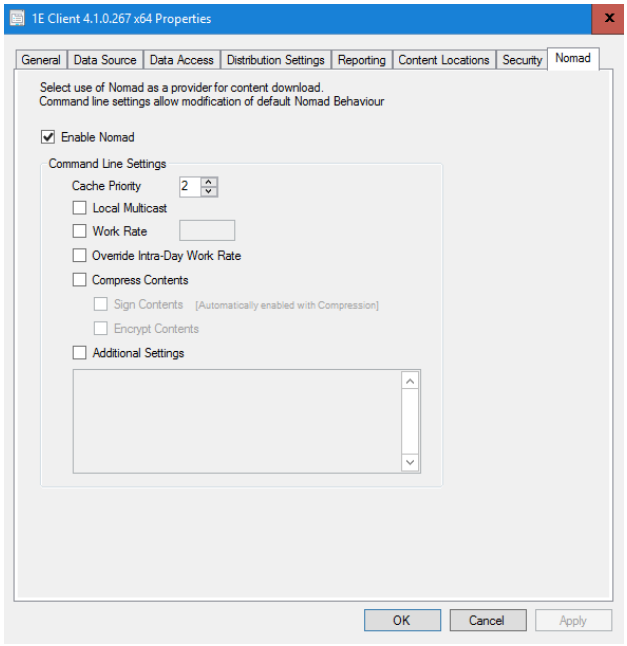
> **Note**
>
> Nomad can be set as a content provider for **Applications** and **Software Updates**. You must configure settings for *all* **Applications** and *all* **Software Updates** using **Client settings**, as described below Configuration Manager client settings, and not individual instances.

> **Note**
>
> Nomad includes a number of custom task sequence steps that can be used to integrate with OS deployments, refer to OS deployment task sequences: Custom task sequence actions for details.

9.4.2.1.4.2.1 Nomad tab

You can set the following options on the **Nomad** tab:

Option	Description
Enable Nomad	Enables Nomad to be used as a data transfer service for the selected package. The other controls on this page are only active if this is enabled. **Note** On the **Nomad** tab for a task sequence, this option is labelled **Enable Nomad – Modifies currently associated reference packages**. This is to emphasize the fact that, for task sequences, enabling Nomad at the task sequence level modifies the Nomad settings for all the packages referenced by that task sequence.
Cache Priority	defines the priority of this specific content in the Nomad cache to manage purging when new content requires cache space. Values are from 1-9; the lower the value, the more likely the content will be purged by other content that requires the space. Refer to Cache management for details.
Local Multicast	Enables local distribution multicast for the package after it is downloaded. **Warning** The Multicast feature is not supported in the Tachyon 5.2 release. This feature is under consideration for re-design and may be available in future versions of Nomad.
Work Rate	Work Rate (%) – determines the percentage of available bandwidth to use for the download. The default value is 80%. If you have set intra-work rates, (the lower of these two values is used unless you enable the Override Intra-Day Work Rate option. Please refer to MaxWorkRates for details about intra-day work rates.
Override Intra-Day Work Rate	Overrides the intra-day work rate for the duration of the download. If Intra-day work rates have been defined on the client and this option is selected, the value defined in the Work Rate property will take precedence over the Intra-day work rate for the current day and time.
Additional Settings	Enables you to define arguments for the download command-line. The arguments are listed in the Additional Settings table.



9.4.2.1.4.2.2 Additional Settings

Arguments	Default value	Range	Description
++pr	Configuration Manager defines the following default values: For Packages and Task Sequences the default is 3 For Applications the default is 0 For Software Updates the default is 1 Nomad will use the default values defined by CM unless the ++pr argument is specified. **Note** As these defaults are defined by Microsoft,	0 – Foreground (the highest priority) 1 – High 2 – Normal 3 – Low 4 – Background (the lowest priority)	Sets the priority for the package download. Packages with a higher priority will be downloaded before lower priority packages. **Note** Be careful not to confuse package priority *(++pr)* a setting related to Configuration Manager package downloads with cache priority, a setting on the Nomad properties page related to the Nomad cache. If a content download request with a higher priority comes along while content with a lower priority is downloading, the current download will be suspended and the higher priority content will be downloaded. When the higher priority content has finished downloading the

Arguments	Default value	Range	Description
	they may change in the future.		previously suspended download will be continued from where it left off. This caters to the situation where a large image package is being downloaded and a critical patch needs to be sent. Setting the critical patch to have a higher priority will enable it to download first and then allow the image package to continue downloading. **Note** If you modify the priority values for packages associated with a task sequence, you must set all the priorities for all the packages to the same value.
++sm		1 to 99	Sets the frequency of the Nomad download status message. These messages are useful for monitoring the status of large package downloads taking place over a long period of time. The messages appear in Configuration Manager under the downloading package's status. The messages are also logged locally in the Nomad log file on the client machine. The value for this argument sets the percentage of the download at which a status message is sent. So, *++sm=10* sets Nomad to send a message each time ten percent of the download has been transferred. The messages sent are subject to an overall default limit of one message per hour per client. This is to prevent

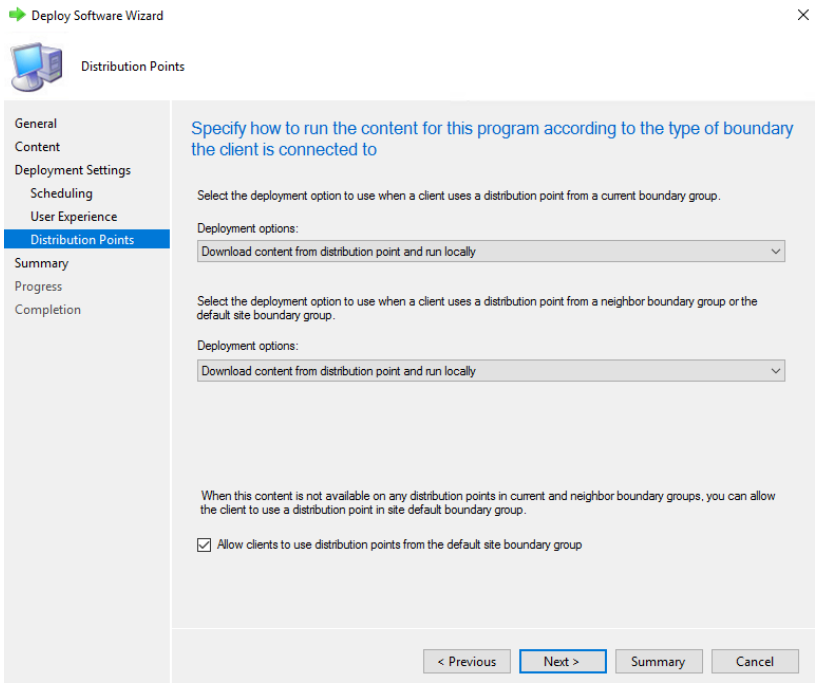
Arguments	Default value	Range	Description
			Configuration Manager from being overwhelmed by a status message coming from many thousands of clients.
--debug	9	1 – minimal logging 9 – default and recommended logging level 25 – detailed logging. If you use this, we recommend you increase the size of your log file to more than 1MB.	Sets the level for debug logging. Changing this value will result in a persistent change on the client.

9.4.2.1.4.2.3 Configuring deployments with Nomad

Packages and task sequences make use of deployments for distribution.

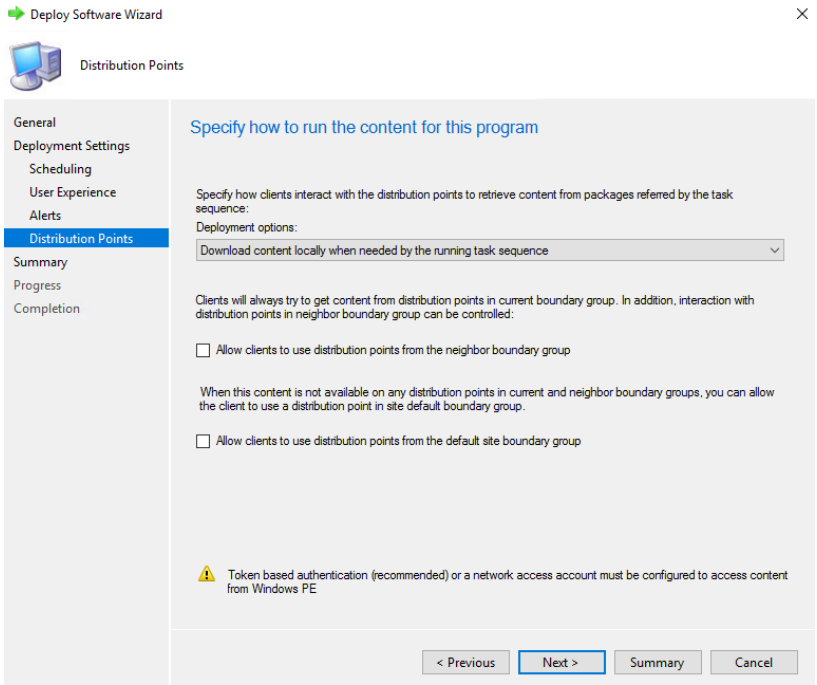
Package deployments intended for use with Nomad must be set to **Download content from distribution point and run locally** for clients using a distribution point from both a current boundary group and from a neighbor boundary group or the default site boundary group.

Using Nomad, you can also safely **allow clients to use distribution points from the default site boundary group**.



For task sequence deployments, select the **Download content locally when needed by the running task sequence** option on the **Distribution Points** screen in the **Deploy Software Wizard**.

Using Nomad You can safely **allow clients to use distribution points from the neighbor boundary group** and **allow clients to use distribution points from the default site boundary group** if this is appropriate based on your Boundary Group configuration.



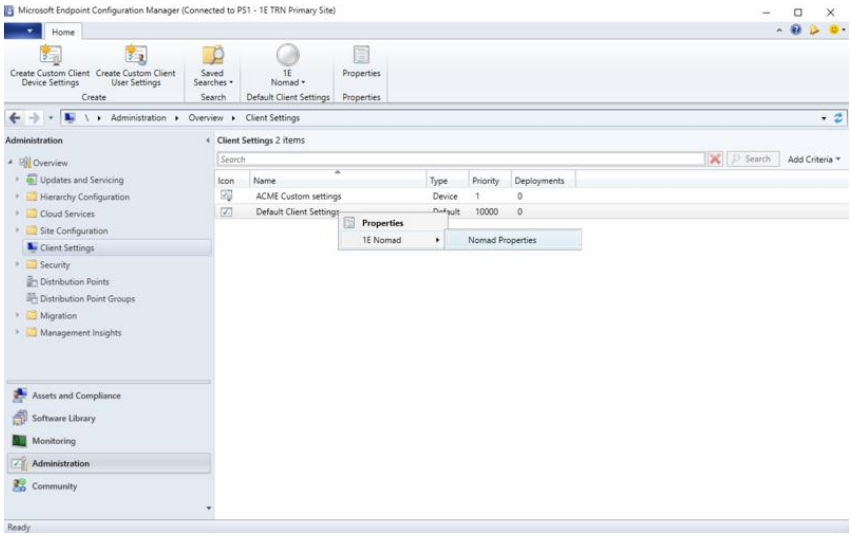
9.4.2.1.4.3 Enabling Nomad for Applications and Software Updates

Set Nomad as a download provider for applications and software updates in Configuration Manager **Client Settings**.

To do this:

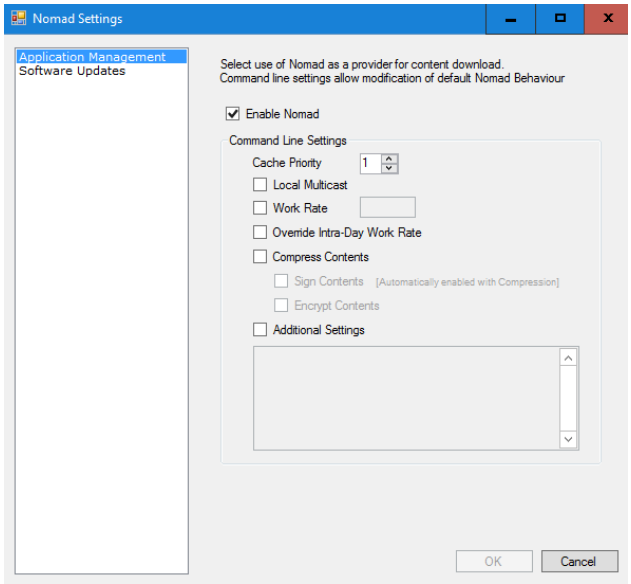
Open the Configuration Manager console.

Under **Administration**, choose **Client Settings**.



On **Default Client Settings**, choose **Nomad Properties** from the context menu.

In the **Nomad Settings** dialog, unique settings can be stored for both **Application Management** and **Software Updates**.



9.4.2.1.4.3.1 Custom device settings

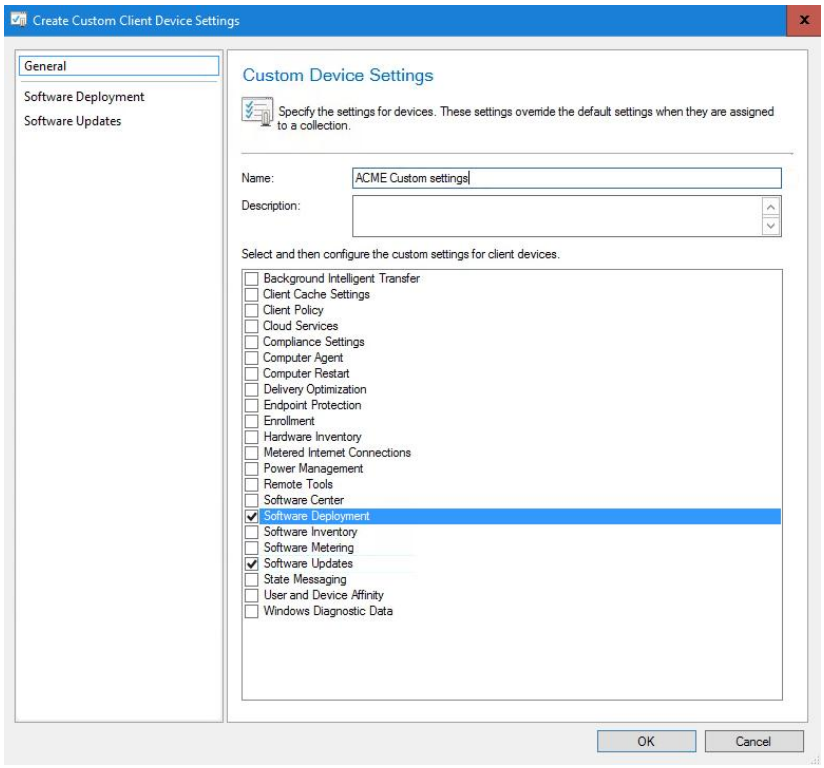
In addition to configuring the **Default Client Settings**, you can also enable Nomad for Applications and Software Updates in within a custom client settings group.

> **Note**
>
> You must configure **Default Client Settings** so that clients have default settings to fall back to if they move out of scope of the custom settings.

When creating new or modifying existing **Custom Device Settings** to enable Nomad, ensure the **Software Deployment** custom setting is selected (to enable Nomad for Applications) and **Software Updates** custom setting is selected to enable Nomad for Software Updates.

When the Custom Settings have been created or modified to include these options, right-click the custom client settings (by Name) in the **Client Settings** list in the console, select **1E Nomad** → **Nomad Properties** and enable and configure Nomad for Application Management and Software Updates as indicated in the screenshot above.

> **Note**
>
> When using Nomad in an OS Deployment Task Sequence that includes Applications or Software Updates, it is necessary for Nomad to be enabled (for Application Management and Software Updates respectively) in the Default Client Settings.
>
> When a Task Sequence is executing and the ConfigMgr client is initially installed, it uses only settings from the Default Client Settings and will not apply any custom settings.



9.4.2.1.5 Download resumption and consistency checking

To minimize repeated downloads of the same content from the Distribution Point, Nomad supports download resumption and consistency checking.

Refer to Deploying software with Configuration Manager for example scenarios about deploying Applications and Packages where Nomad is integrated with Configuration Manager and how you can monitor those deployments using the Nomad app.

9.4.2.1.5.1 Download resumption

Nomad downloads include checkpoint recovery, so if the connection to the distribution point is disrupted during a download, it is resumed when the connection is next available. Download resumption starts from the point it had reached when the connection was lost. This means that no previous time spent downloading the package is wasted.

9.4.2.1.5.1.1

9.4.2.1.5.2 Consistency checking

Nomad must be installed on all the Configuration Manager DPs. This not only lets central multicast work, but also enables package file checksums to be calculated centrally allowing efficient recovery from file transfer issues if one exists. The central creation of the checksums also minimizes the computational overhead.

Nomad uses manifest files to describe the download contents of Configuration Manager applications and packages. This enables it to provide file-level transfer and, when integrated with Configuration Manager remote differential compression (RDC), file delta downloads. The Nomad client automatically generates a manifest for each version of each package. The generation request occurs as the first Nomad client attempts to download the newest version of a package.

9.4.2.1.5.2.1

9.4.2.1.5.3 Manifest files

The manifest, a *LSZ* file, is stored in the root of the Nomad cache. This lists each file, its time stamp, a CRC checksum and the Configuration Manager hash value for the content. Nomad uses this manifest to ensure that the correct files have been downloaded for each package and to enable the rapid detection of changes between versions of packages.

9.4.2.1.5.3.1 Hash checks for Windows 10 service updates

Nomad now gets the hash from the *LSZ* file and validates the calculated hash with it. Since the *LSZ* file can contain SHA2 or SHA1 hashes, along with cyclic redundancy checks (CRC) for individual files, the precedence of the validation is:

Use HashV4 (which is SHA2) if it exists, for the validation.

Use Hash (which is SHA1) if it exists, for the validation.

Otherwise, only perform CRCs on all the files that have that value in the *LSZ* file.

This enables standalone downloads to get the hash check on the server side (from the *.ini* file) as well as on the client side (from the *LSZ* file).

9.4.2.1.5.4 Distribution point resilience

If a DP becomes unavailable during a download, Nomad will failover to the next DP on the list ensuring download resilience efficient content delivery.Configuration Manager provides a list of DPs from which the content for packages can be downloaded. Under certain circumstances, DPs may become unavailable. Using a list supports failover by selecting a new DP to continue the download.

Earlier versions of Nomad would only attempt to download once from each DP in the list. If a DP was not available, Nomad would abort the download. However since v4, Nomad now cycles through the list of DPs until a connection is established. If no DP is accessible, it will wait for a time before trying the list again until a timeout is reached.

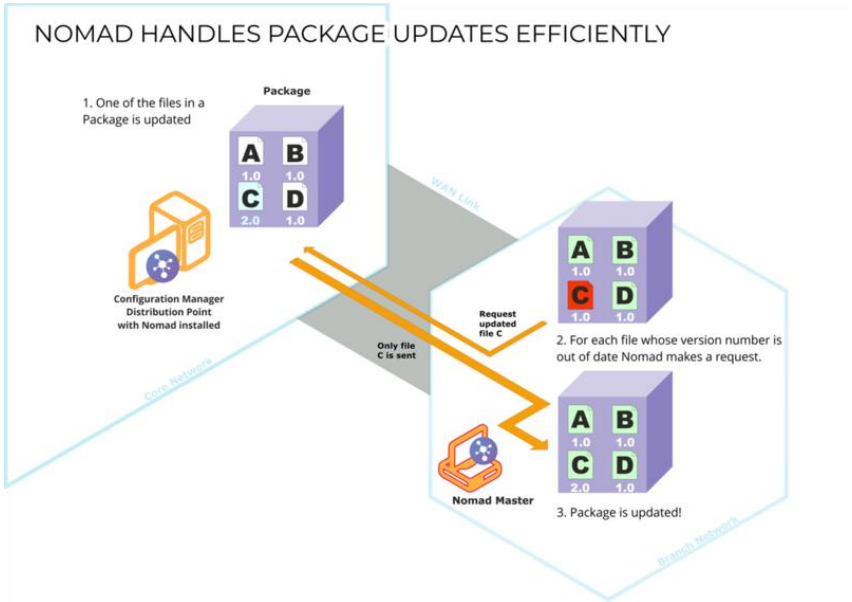
The delay before retrying the DP list is configured in the RecycleDPDelay registry value

The maximum download timeout is configured in the DownloadTimeout registry value.

9.4.2.1.5.5 File-level delta downloads

Nomad is able to perform package updates efficiently not only by downloading just the files whose versions have changed, but also by downloading just the portions of the changed files that are different. In a similar way to file consistency checking, Nomad can also efficiently deal with package updates.

In this example, if a package that has been previously downloaded has one of its files updated, Nomad compares each of the file versions for its cached package with the file versions for the incoming updated package. If a file has an older version, it is requested for download. if that is the only file that has been updated the transfer is complete and the package is updated.



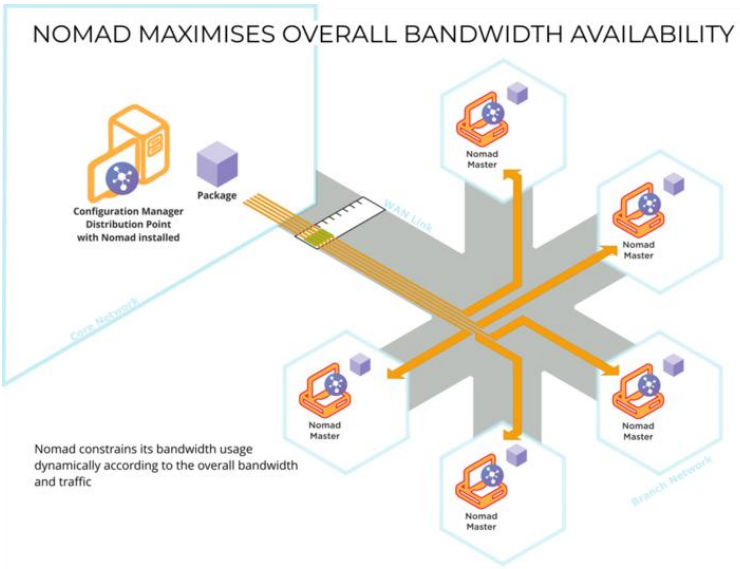
9.4.2.1.6 Bandwidth Protection

Nomad dynamically analyzes the overall WAN traffic to ensure that it only uses a percentage of the total. It is also aware of mobile devices and knows the difference between wireless and wired connections and is able to select the most efficient available connection to use.

9.4.2.1.6.1 Full control over WAN link usage

Nomad respects business data on the network – it detects the true end-to-end available bandwidth and monitors this throughout the duration of the download. This is calculated using a sophisticated algorithm that looks beyond the receiving capabilities of each device's network card. If bandwidth is available, the transfer speeds up; if it becomes restricted, the transfer slows down. As a result, overall WAN availability is maximized and the impact on the critical link between the branch networks and the central network is minimized.

To avoid placing a burden on office wireless bandwidth and to use the most efficient transfer system possible, Nomad can be configured to switch from a wireless to a wired network connection automatically when one becomes available. (Please refer to Design Considerations - Managing stable LAN connections).



9.4.2.1.6.2 Bandwidth Protection Reporting

With Bandwidth Protection Reporting, so you can now see how Nomad is preventing end-user disruption due to software and update deployments. Bandwidth Protection Reporting will allow you to see the positive impact Nomad is having across the organization, to individual sites, subnets, all the way down to a single client.

Using the Nomad app, you can view bandwidth protection metrics on the following pages:

Overview page

Devices page

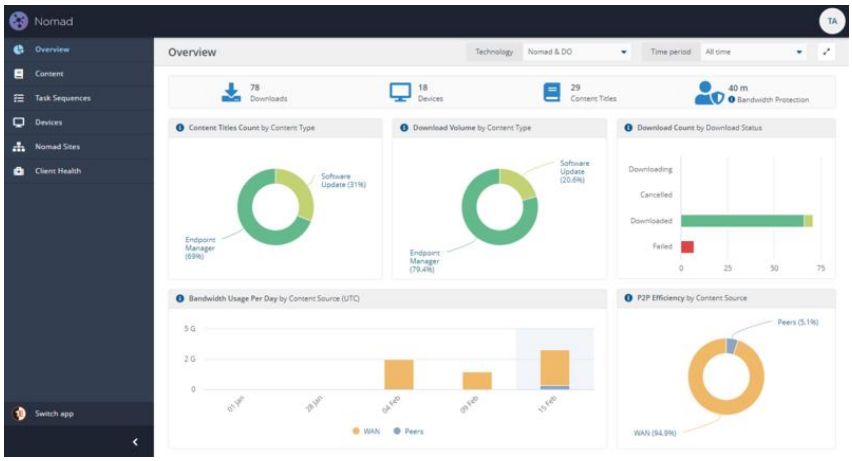
Nomad Sites page.

The following new metrics are available in the Nomad app to help demonstrate how Nomad benefits your organization:

Metric	Description
Bandwidth Protection	Displays the total time that Nomad backed off when downloading content to protect end-user bandwidth. This is the result of the **Bandwidth Protection Time** column dived by the **Active Download Duration** and multiplied by 100.
Bandwidth Protection %	Bandwidth Protection shown as a percentage of downloads.
Bandwidth Protection Time	Duration the client backed off from downloading to save download bandwidth.

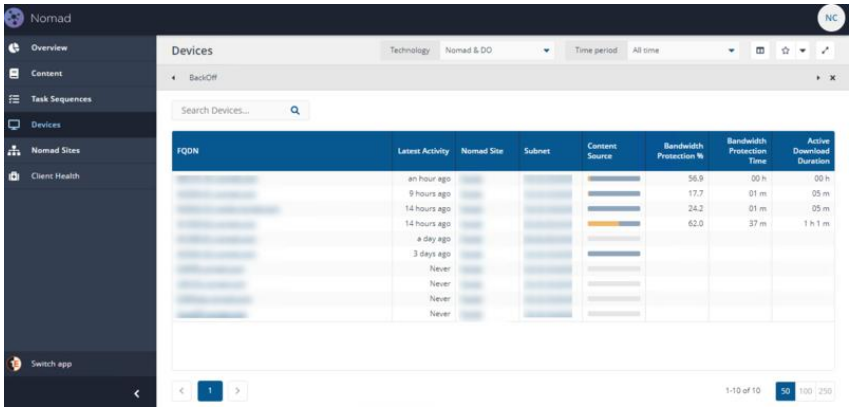
9.4.2.1.6.2.1 Overview page

The Overview page gives a high level view of the current status of content throughout the entire network, including **Bandwidth Protection**.



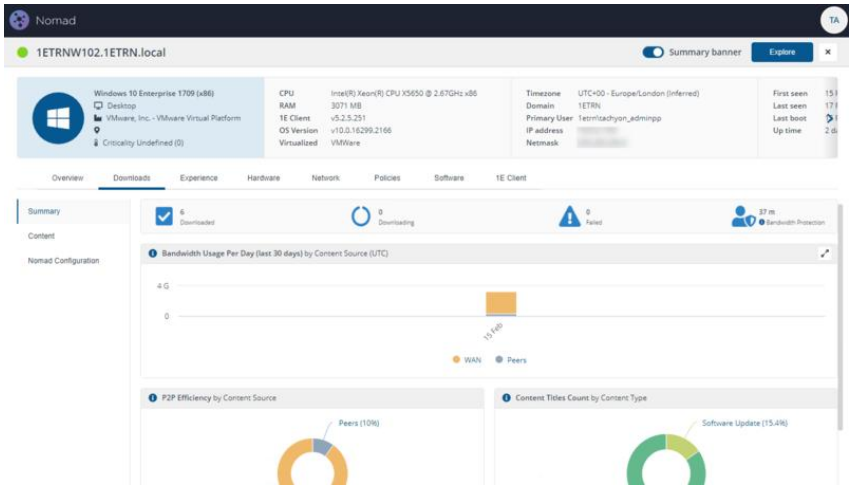
9.4.2.1.6.2.2 Devices page

The Devices page lists all Devices that have sent Nomad device registration events and have sent download events within a selected time period, and includes **Bandwidth Protection %** and **Bandwidth Protection Time**.



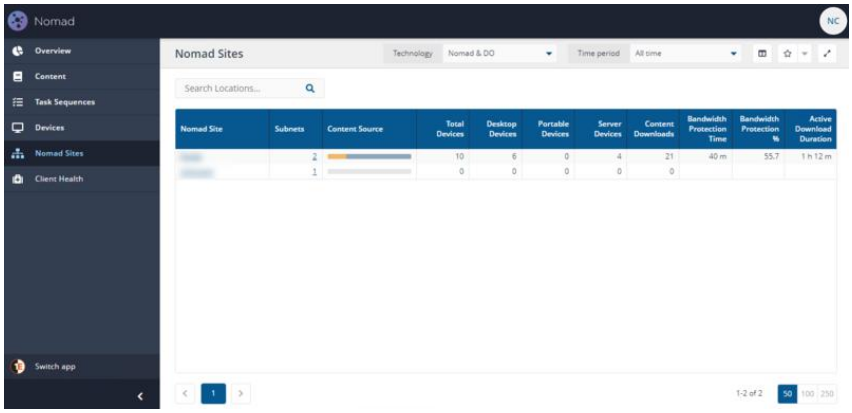
9.4.2.1.6.2.2.1 Devices page details view

The status bar along the top shows high-level download statistics for a particular device, including **Bandwidth Protection**.



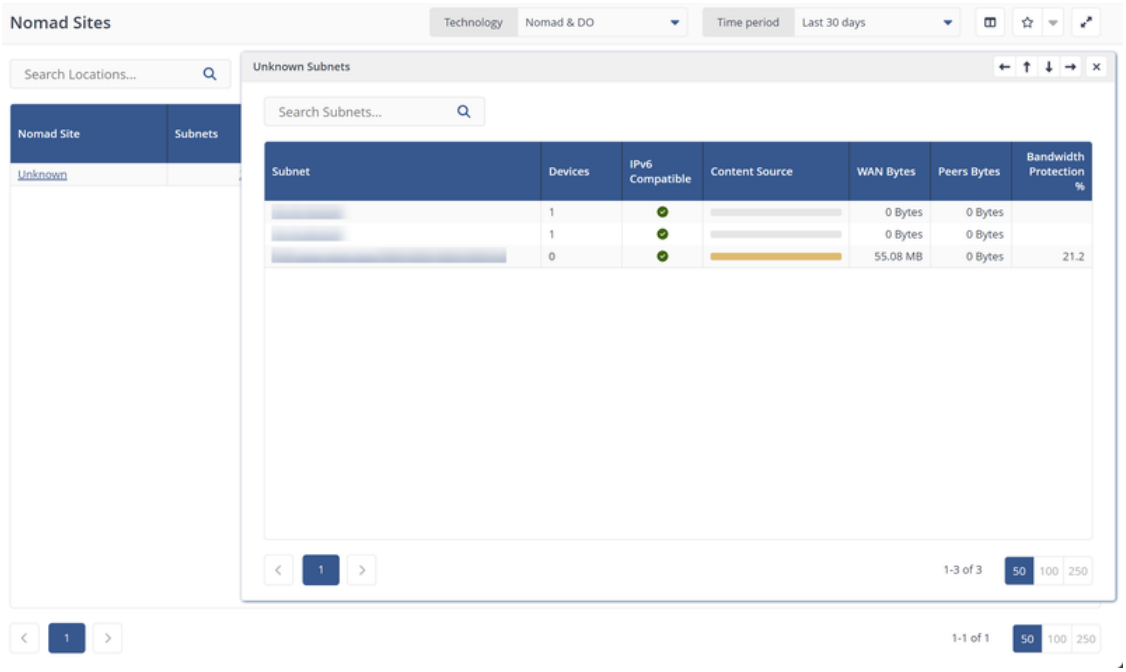
9.4.2.1.6.2.3 Nomad Sites

The Nomad Sites page shows how the network is being used for content distribution in different locations, including **Bandwidth Protection**.



9.4.2.1.6.2.3.1 Nomad sites subnet drawer

A drawer that opens up when you click on **Subnets**, **Content Source**, **WAN Bytes** etc. except **Network Location**. It shows a list of all Subnets falling under that location, including **Bandwidth Protection %**.



9.4.2.1.7 Nomad FanOut

Windows imposes a limit on the number of concurrent connections on the Nomad share. The FanOut feature compensates for this limitation by enabling any peer that has more content than the requester to respond to the FanOut request. It is not limited to peers that have an active connection to the master.

9.4.2.1.7.1 How FanOut works

To use FanOut, the Nomad *SpecialNetShare* registry value must be updated to include bit 6 (*0x40*or 64 decimal) on all devices hosting Nomad.

By default, the Nomad cache share *(NomadSHR)* is limited to six concurrent connections by Windows. This means that up to six Nomad peers (devices that request the download) can obtain content from the master at any given time (the device that wins the election on the subnet and becomes the central source for the download). Under normal circumstances, if a Nomad client tries to connect to the master and all six connections are in use, the Nomad client retries later.

The FanOut feature compensates for this limitation by enabling the Nomad client to ask for an alternative peer on the same subnet that has the content it needs, any other peer on the subnet can respond to this request but will only do so if it meets certain criteria, it must:

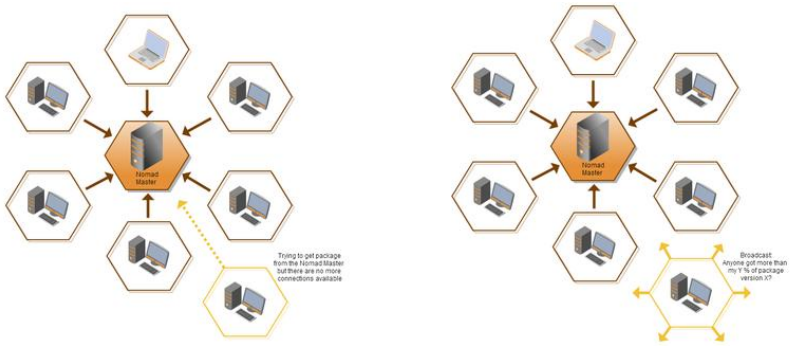
Have more content than the Nomad client requesting it

Have available connections on its own *NomanSHR*

Not already be connected to a FanOut peer (a device connected to the master share that responds to FanOut requests and allows other devices to connect to it).

Refer to Deploying software in large networks - Using FanOut for large subnets for an example scenario about deploying software in a large network and how you can monitor those deployments using the Nomad app.The following illustrations demonstrate how FanOut works.

If a Nomad peer gets a Maximum connections limit when trying to connect to a master, it broadcasts a request for who has more than a certain percentage of a package with a certain ID.



A device responds to a FanOut request if the following conditions apply:

If it is currently active and downloading, or it is idle and has downloaded part or all of the package from the master

It has a larger percentage of the package than the device broadcasting the request

If the broadcast request has not been received over a wireless link

Its version of the package is greater than or equal to the package version held by the device broadcasting the request

It has free connections to its Nomad share

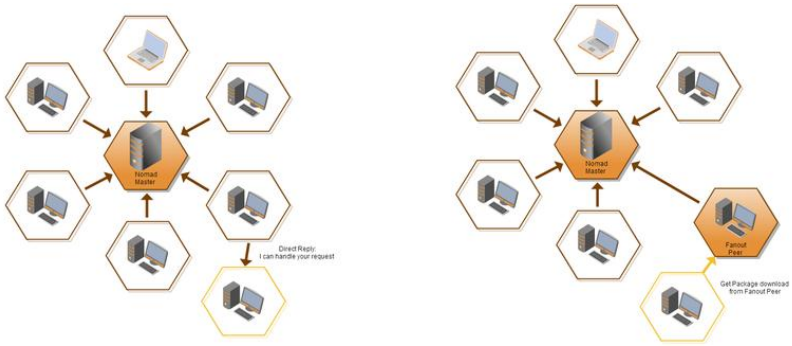
Its election weighting is greater than zero – i.e. it is not set as a sensitive server

It is not a domain controller

It is not part of any inhibited subnets and sites - please refer to Design Considerations: Inhibiting subnets and sites

Its NomadSHR exists and P2PEnabled is turned on, it is not set to 0.

The Nomad peer will attempt to connect to the first FanOut peer that responds to its request. In this way, rather than limiting the distribution to six Nomad peers, many more devices can be accessing the download from the master, exponentially speeding up content deployment on large subnets.



9.4.2.1.7.2 Checking to see if FanOut is working

To observe FanOut on Nomad client when the connection to NomadSHR is reached on the elected master:

Open *NomadBranch.Log* on a Nomad client. This client must not be the master.

Notice that the client has failed to connect to the master.

It then polls for a FanOut peer.

It receives a response and starts the download.

Date/Time	Log Text
12/8/2014 1:41:29 PM	AttemptConnection "1ETRNW81"
12/8/2014 1:41:29 PM	Standard P2P connecting to master \\1ETRNW81\NomadSHR as "1ETRNW81\SMSNomadP2P&"
12/8/2014 1:41:31 PM	Failed to connect to "\\1ETRNW81\NomadSHR" - No more connections can be made to this remote comp (0x00000047)
12/8/2014 1:41:31 PM	FanOutPeer Poll
12/8/2014 1:41:31 PM	FanOutPeer candidate 1ETRNW71 40.817%
12/8/2014 1:41:31 PM	RANDOM=832 users=0 delay=832 attempt=1
12/8/2014 1:41:32 PM	AttemptConnection "1ETRNW71"
12/8/2014 1:41:32 PM	Standard P2P connecting to fanout peer \\1ETRNW71\NomadSHR as "1ETRNW71\SMSNomadP2P&"
12/8/2014 1:41:34 PM	FanOutPeerSMB Connected OK
12/8/2014 1:41:34 PM	Nomad Branch event Evt_Infomational : FanOutPeer connected - \\1ETRNW71\NomadSHR (level=1) for PS100015
12/8/2014 1:41:34 PM	SMB Connected OK
12/8/2014 1:41:34 PM	CopyLstFromPeer:: - \\1ETRNW71\NomadSHR\PS100015_1.LsZ
12/8/2014 1:41:34 PM	P2P 0100007F 2000 "PS100015_1.LsZ" blk=0 (blk/s=0) 0(0)

9.4.2.1.7.3 Limitations

Nomad FanOut cannot currently be used with the following features:

Nomad is installed in WinPE is not capable of becoming a FanOut peer (i.e. a provider of package content) because file sharing is not supported. However, Nomad is capable of requesting content from and connecting to FanOut peers on the local subnet.

Nomad FanOut is not compatible with Nomad multicast, if multicast is enabled for a particular package, Nomad FanOut is not used, regardless of the value in *SpecialNetShare*

Nomad FanOut will not be used when Nomad is run in standalone mode

Nomad FanOut is disabled for computers using wireless connectivity.

9.4.2.1.8 Content Distribution overview

1E Content Distribution is a Tachyon Consumer, providing control and visibility on content deployments and delivery in an organization.

9.4.2.1.8.1 Content Distribution features

Content Distribution offers visibility for the following using the Nomad app:

The status of all deployments, including both delivery and execution of content

The effectiveness of Peer to Peer technologies like Delivery Optimization (DO), Nomad and BranchCache

Historical trends like Peer to Peer effectiveness

Where content is located or cached by a Peer to Peer technology.

In addition, to the reporting use-cases mentioned above, Content Distribution supports other content distribution uses-cases like:

Single Site Download (SSD)

Nomad Pre-caching

Nomad Download Pause.

> **Note**
>
> The above features were previously provided by ActiveEfficiency Server, which has been replaced by Content Distribution on Tachyon Platform 5.2.

9.4.2.1.8.2 Content Distribution components

Content Distribution consists of four main components, the Nomad app is the front end of Content Distribution and the other components form the back end.

Component	Description
Nomad app	Shows content distribution stats and provides a UI to manage content distribution.
Content Distribution Consumer	REST API collects content distribution data from endpoints and provides it to the Nomad app for rendering.
ContentDistribution database	A database that backs the REST API and stores its data.
1E Client	A component running locally on the endpoint captures content distribution data and posts it to the REST API.

9.4.2.1.8.3 Nomad app

Content Distribution features are exposed to the user in the Nomad app. Each page in the Nomad app offers different tiles displaying various Peer to Peer metrics.

The **Overview** page gives a high level view of the current status of content throughout the entire network. By default, the view will show activity and status for both Nomad and Delivery Optimization. These defaults can be modified using the **Technology** filter (to show Nomad or DO activity only) and the **Time period** filter.

The **Overview** page gives a brief snapshot of download activity. The page has multiple tiles showing:

Content Titles by Content type

Download Volume by Content Type

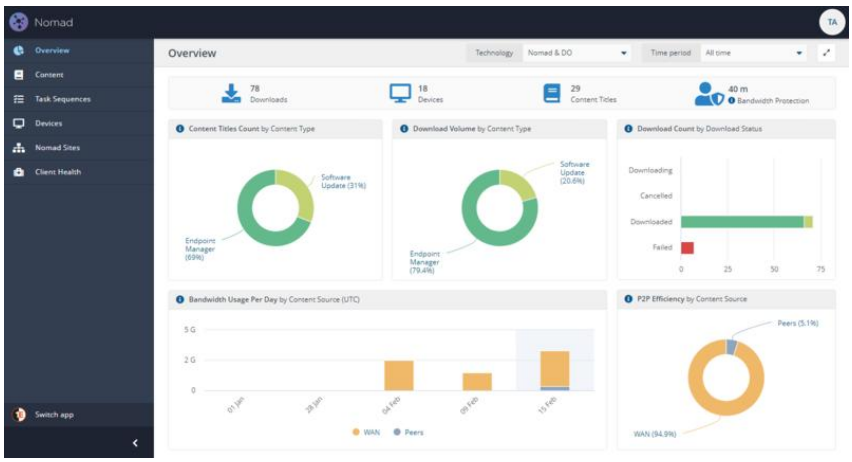
Download Count by Download Status

Bandwidth Usage Per Day by Content Source (UTC)

P2P Efficiency by Content Source (Peer to Peer - P2P).

The results can further be narrowed down by using the **Technology** and **Time period** filters on the page.

Please refer to the Nomad app reference for more details.



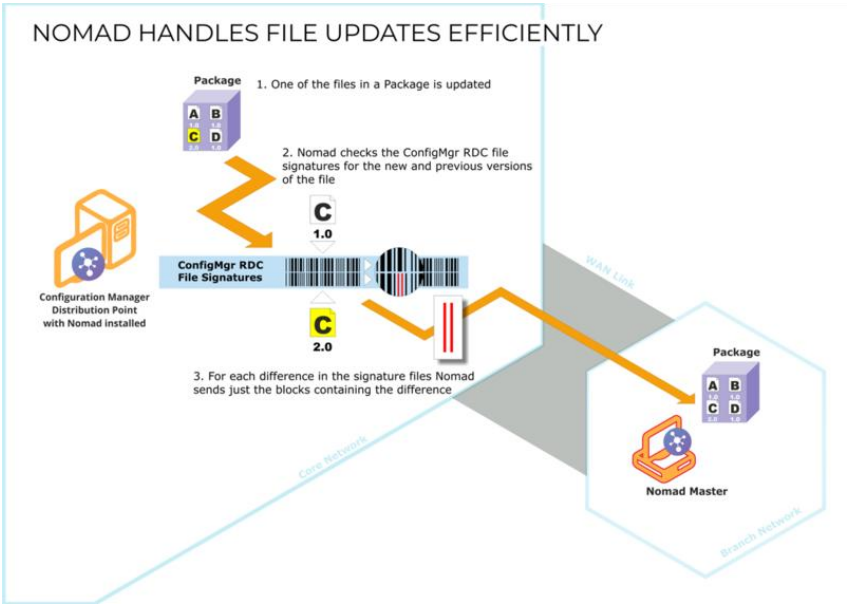
9.4.2.1.9 Remote differential compression (RDC) integration

Not only is Nomad aware of the file level differences between different versions of a package so that only changed files are downloaded, it is also aware of the differences within individual files.

This is sometimes known as binary differential replication or binary deltas but is more commonly known as remote differential compression (RDC) integration, for details refer to https://docs.microsoft.com/en-us/previous-versions/windows/desktop/rdc/about-remote-differential-compression.

Refer to Deploying software in large networks - Using FanOut for large subnets for an example scenario about deploying software in a large network and how you can monitor those deployments using the Nomad app.

In our example, a package that has been previously downloaded has one of its files updated. Nomad compares the Configuration Manager RDC signature file (where each block in the file is given a number that identifies it according to its contents) for the new version of the file and the one before it. By identifying the changes, Nomad is able to download just the file blocks containing the differences.



In combination with other Nomad features such as bandwidth protectionanddynamic elections, remote differential compression (RDC), when used with Configuration Manager (CM), results in an even more efficient and reliable mechanism for transferring content across the WAN. The Nomad client automatically generates a manifest file for each version of a package when the first client attempts to download the newest version of a package. If RDC is enabled, file delta downloads becomes a feature of the manifest file and the client will download just the differences from either the DP or the local peer.

RDC integration occurs on:

Configuration Manager distribution point (DP)

Nomad client master

Nomad client peers.

The only configuration required for RDC is:

Enable Configuration Manager RDC on the DP

Install Nomad using the SIGSFOLDER property on any DPs (or update the Nomad SigsFolder registry value).

> **Note**
>
> On Configuration Manager, RDC is not used for applications. This is because an application's content version always remains at 1, only the content revision gets updated with a new content ID, so RDC for applications will not occur. This is not a limitation of Nomad, but simply the way the application model is implemented.

9.4.2.1.9.1 RDC on distribution points

RDC signature files must be generated and copied to the default signature folder (*C:\SMSSIG$*) by Configuration Manager. If you use a different location for the signature files, you must update its location in the in SigsFolderregistry value. Signature files are generated for every package, including OSD images.

9.4.2.1.9.2 RDC on the elected client

The RDC file copy feature only works between the DP and the elected master. The package download process remains almost the same as in earlier versions of Nomad, except for files that have an RDC value specified for them in the manifest file.

The Nomad master checks for the package version *(n-1)* on the subnet. If the version *(n-1)* is cached locally or available on another client on the same subnet, it uses RDC to copy delta blocks from the DP. Once the elected master starts to download the newest version of a package, it first fetches the manifest file and RDC data generated by the *NomadBranch* service for that package on the DP. The RDC data contains the needs list (*.needs.bin*) for all the files in the package that have changed between versions *n-1* to *n*. These *.needs.bin* files are used to create the target files by copying blocks from the files cached locally and from the DP.

If the master becomes unavailable during this process, a re-election takes place and the new master re-downloads the needs list from the DP.

> **Note**
>
> The *NomadBranch* service skips RDC calculations while generating the *LSZ* of a package where the *LSZ* of version *n-1* has not been generated earlier or if the *LSZgen* request is for the first version of the package.

9.4.2.1.9.3 RDC on the peer

RDC file copy is done between the DP and the elected master only in a subnet. The remaining devices or peers in the subnet copies all the blocks of files modified in the package using normal P2P.

9.4.2.1.9.3.1 Alternate source copy

Alternate source copy, often referred to as alt-copy, takes place when the elected master does not have the previous version of the package, but another device on the subnet has it. The elected master can still do RDC file copy by copying the required blocks using RDC_alt copy from the other device on the subnet.

> **Note**
>
> If a version *n* of a package is not available from Nomad peers but version *n*-1 is, Nomad fetches *n*-1 on the assumption that at least some files are unchanged between versions, then it will download just the remaining, different, files in version *n* from the DP.
>
> This mechanism relies on the name of the content remaining the same between versions with just a change in the version number, and so it only works for packages. A new version of an application or software update has a completely new name, and version numbers are not meaningful. There is no configuration option for this, Nomad does it automatically.

On Windows Server DPs without a primary or secondary site server, RDC must be installed manually using Windows Server Manager.

> **Note**

Alternate source copy will only work when clients download from the same DP.

9.4.2.1.10 Downloading content for CM Software Updates from Microsoft Update

This feature enables Nomad to download content from Windows Update / Microsoft Update (WUMU). Starting in CB version 1806, software updates can be deployed to devices without first downloading and distributing content to Distribution Points, instead clients download updates directly from the cloud.

Refer to Deploying software updates using Configuration Manager for an example scenario about deploying software updates using CM and how you can monitor those deployments using the Nomad app.

9.4.2.1.10.1 Configuration

Downloading the following type of updates is enabled by default in the Nomad client (1E Client 4.1 and later). Downloading from Microsoft Update is also enabled by default.

The settings are defined in CompatibilityFlags and you will need to ensure the relevant bits remain set if you are using that registry value to configure other options, as follows:

Type	Enable Nomad to download	Enable Nomad to download from Microsoft Update
Software Updates (including Windows 10 feature updates)	Always enabled	Set bit 27 (0x08000000, 134217728 in decimal)
Office 365 updates	Always enabled	Set bit 28 (0x10000000, 268435456 in decimal)
Windows 10 Express Installation Files and Delta Content for Updates	Set bit 26 (0x04000000, 67108864 in decimal)	Set bit 28 (0x10000000, 268435456 in decimal)

To enable all the above, then AND bits 26, 27 and 28 with whatever you have already set in CompatibilityFlags.

Please refer toDistributing software with Nomad and Configuration Manager: Enabling Nomad for Applications and Software Updatesfor how to configure client settings to set Nomad as a download provider for applications and software updates.

Note

Please note, there is no configuration is required on Distribution Points.

9.4.2.1.10.2 How it works

9.4.2.1.10.2.1 Configuration Manager and Microsoft Updates

Configuration Manager supports Windows Update / Microsoft Update (WUMU) cloud service as a content location for Software Update deployments.

When creating a deployment of a software update, on the **Download Settings** page you can configure the setting

If software updates are not available on distribution point in current, neighbor or site boundary groups, download content from Microsoft Updates. Enabling this setting means *intranet-connected* clients will download software updates from Microsoft Update if updates aren't available on Distribution Points. *Internet-based* clients always go to Microsoft Update for software updates content. This setting is beneficial when dealing with extremely large update content and if you want clients to always get content from the Windows Update / Microsoft Update (WUMU) cloud service. This feature supports any update type supported by Configuration Manager software updates management, including Windows and Office updates.

9.4.2.1.10.2.2 Nomad and Microsoft Updates

Before the introduction of this feature in Nomad 7.0, if Configuration Manager client Content Transfer Manager (CTM) asked Nomad to get a download job from WUMU, it used to fail the job with error code ERROR_UNKNOWN_TRANSPORT 0x2059, which notifies E_FAIL to CTM. Nomad does this because it expects CTM to take over the download using BITS. With the introduction of this new feature in Nomad 7.0, Nomad client can now manage the content download from WUMU, and use Nomad's P2P feature to download content from peers that already have the necessary content.

At the time of writing CB 1902, and therefore Nomad, does not support Windows Update for Business.

9.4.2.1.10.2.3 Compatibility with Distribution Points

WUMU is treated as just another Distribution Point and features like DP resilience would work as expected. If Nomad was for example, downloading an update from a DP and encountered an issue in reaching the server, then it would continue the download from WUMU (if configured) from wherever it was interrupted.

9.4.2.1.10.2.4 Hash validation

When downloading from a Distribution Point, Nomad client retrieves the LSZ file and does a full hash validation of the update as well, because Nomad on a DP can retrieve it and keep it in LSZ file. Individual files are validated against HASH fetched from URL's, but the whole update is not validated together as the full Hash of the update isn't available anywhere in WMI.

9.4.2.1.11 Windows 10 Express Installation Files and Delta Content for Updates

As Windows 10 cumulative updates get very big, very quickly (often in excess of 1GB a few months after any given Feature Upgrade), Microsoft started publishing express installation files for these updates in addition to the traditional full update files. Configuration Manager introduced support for Windows 10 Express Installation File updates in Current Branch 1802 hotfix KB4163547.

Express installation files are a much larger payload on the Distribution Point compared to traditional software update files, but the feature enables clients to download delta byte-ranges from these files, so each month the amount of data a client has to download is typically much smaller. Configuration Manager Current Branch can be configured to support express installation files (refer to https://docs.microsoft.com/en-us/configmgr/sum/deploy-use/manage-express-installation-files-for-windows-10-updates for more details).

With the release of Windows 10 1809, Microsoft replaced express update files with a new way of managing deltas within software updates. In Configuration Manager 1902 the **Enable installation of Express installation files on clients** option in Software Update Client Settings was replaced with **Allow clients to download delta content when available**.

Note

Nomad supports the download of Express installation files and delta content for updates.

Refer to Deploying software updates using Configuration Manager for an example scenario about deploying software updates using CM and how you can monitor those deployments using the Nomad app.

9.4.2.1.11.1 Updates, Nomad and Delivery Optimization

The Microsoft implementation of byte-range downloads in Configuration Manager integrates with Delivery Optimization (DO) on Windows 10 clients. When the CM client has been configured to use express installation files or delta content for software updates, Delivery Optimization will attempt to get the content from other DO peers. In normal circumstances, if DO is unable to fulfil a request from DO peers it will revert to the HTTP source on the Internet. However, in this scenario, when the software update is managed by CM, DO reverts to the CM client to get the content from the DP and in turn Nomad will be used to download the content. It is therefore possible that when using express updates or delta content for updates, some byte ranges may be downloaded by Nomad and some by DO.

Any byte ranges downloaded by Nomad in this scenario will be available to Nomad and DO peers, whereas byte ranges downloaded by DO will only be available to DO peers. As DO is typically more aggressive than Nomad at clearing its cache, it is likely that Nomad will fulfil more byte-range requests than Delivery Optimization if the update deployment is phased over a number of days, whereas DO could be expected to fulfil more requests when the same update is deployed to all clients at the same time. It is therefore important when enabling express installation files or delta content for software updates in Configuration Manager to ensure you have Delivery Optimization configured appropriately for your environment, even though you are using Nomad.

9.4.2.1.11.1.1 Download mode

The download mode option is important as this determines which devices DO considers as peers it can share content with and may result in content being downloaded over the WAN, for details about download mode refer to https://docs.microsoft.com/en-gb/windows/deployment/update/waas-delivery-optimization-reference#download-mode.

Setting	Description
Download Mode is set to 1	On Windows 10 Enterprise and Education, Download Mode is set to 1 (LAN) by default. This will allow peers within the same network (including all clients sharing a public Internet address through NAT) to share content. The default value for other editions is 3 (Internet) allowing clients to get content from other peers on the Internet.
Download Mode is set to 2 (Group)	Setting Download Mode to 2 (Group) will by default enable peers within the same AD site (or if not in a defined AS Site, the same AD Domain) to share content. You can use other methods

Setting	Description
	to define the group, including DHCP Scope Option, DNS suffix or Azure AAD Tenant ID, refer to https://docs.microsoft.com/en-gb/windows/deployment/update/waas-delivery-optimization-reference#select-the-source-of-group-ids for details. If you enable the Configuration Manager Client setting **Use Configuration Manager Boundary Groups for Delivery Optimization Group ID**, Download Mode will be set to 2 (Group) and peers within the same CM Boundary Group can share content. In this scenario the CM client sets the Group ID on each client using a unique identifier for the CM Boundary Group that the client is in.
Download Mode to 0 (HTTP only)	You can turn off Delivery Optimization peer-to-peer content distribution by setting Download Mode to 0 (HTTP only). This will result in Nomad downloading all byte ranges, but will prevent DO from sharing other content. (e.g. Microsoft Store, Microsoft Updates outside of CM or Intune Win32 apps) with peers. We do not recommend turning off DO peer-to-peer if you are using or planning to use these Microsoft features.
Download Mode = 99 (bypass)	**Note** Do not use Download Mode = 99 (bypass). This option is only relevant on clients if you use WSUS (outside of CM) and prefer to use BranchCache rather than DO. If you are using CM and Nomad for software updates then this option is not needed and can prevent updates from successfully downloading.

9.4.2.1.11.1.2 Windows 10 express installation files

Nomad can download byte ranges from Windows 10 express installation files requested by the Configuration Manager client from either an on-premises DP, Microsoft Update or a Nomad peer.

> **Note**
>
> For details on how Configuration Manager Current Branch uses express updates, refer to https://docs.microsoft.com/en-us/sccm/sum/deploy-use/optimize-windows-10-update-delivery. This also details some native Configuration Manager caveats when using Express updates (notably the increased disk space required on Distribution points and source servers within Configuration Manager).

Using Express installation file or delta content for updates in Configuration Manager (with or without Nomad) has the following additional limitations:

Limitation	Description
Express installation file support.	Express installation files are supported on Configuration Manager Current Branch 1802 (with hotfix KB4163547) and CB 1806 or later, and Windows 10 versions 1703, 1709 and 1803 or later. Delta content for updates is supported in CM CB 1910 onward.
Nomad does not send status messages for downloads of express installation file or delta content for updates.	Nomad does not send status messages

Limitation	Description
	for downloads of express installation file or delta content for updates as there is no way for Nomad to determine if all the required byte ranges have been downloaded for a given update. Nomad is simply obtaining byte ranges as they are requested and notifies the CM Content Transfer Manager as it completes each

Limitation	Description
	download.
Deploying updates using express installation files typically takes longer to install.	Deploying updates using express installation files typically takes a lot longer to install compared to traditional full updates as a lot of processing is required on the client to calculate what byte ranges are required. As an example, a typical Windows 10 Express CU may take over 1 hour to download over even

Limitation	Description
	a fast 1GBs Network connection, where a copy of the same full update would typically take only a couple of minutes.
The Install Software Updates step in an OS Deployment Task Sequence may become unresponsive.	The Install Software Updates step in an OS Deployment Task Sequence may become unresponsive for several hours. As examples, a Windows 10 "Wipe and load" Task Sequence might fall back to

Limitation	Description
	using full versions of the software updates after several retries and an in-place upgrade, fail to initialize the Delta download startup task and hang at a "install Software Updates" step, meaning OS Deployment task sequences, may take some additional hours than normal to complete.

9.4.2.1.11.2 Enabling express installation file and delta content for updates in Nomad.

Once you have configured CM for express installation files or delta content for updates and are comfortable that your Delivery Optimization configuration is appropriate for your network, you

can enable the feature in Nomad through the CompatibilityFlags registry value on the client, setting bit 26 (0x4000000, or 67108864 in decimal).

Downloading the following type of updates is enabled by default in the Nomad client (1E Client 4.1 and later). Downloading from Microsoft Update is also enabled by default.

The settings are defined in CompatibilityFlags and you will need to ensure the relevant bits remain set if you are using that registry value to configure other options, as follows:

Type	Enable Nomad to download	Enable Nomad to download from Microsoft Update
Software Updates (including Windows 10 feature updates)	Always enabled	Set bit 27 (0x08000000, 134217728 in decimal)
Office 365 updates	Always enabled	Set bit 28 (0x10000000, 268435456 in decimal)
Windows 10 Express Installation Files and Delta Content for Updates	Set bit 26 (0x04000000, 67108864 in decimal)	Set bit 28 (0x10000000, 268435456 in decimal)

To enable all the above, then AND bits 26, 27 and 28 with whatever you have already set in CompatibilityFlags.

Please refer to Distributing software with Nomad and Configuration Manager: Enabling Nomad for Applications and Software Updates for how to configure client settings to set Nomad as a download provider for applications and software updates.

Note

Please note, there is no configuration is required on Distribution Points.

9.4.2.2 Single Site Download (SSD)

Nomad's Single Site Download (SSD) feature ensures a download across the WAN only happens once per site. It does this by maintaining information about which subnets are neighbors of each other (accessible on LAN rather than WAN), so that when an elected master considers a download from a DP rather than a peer in its subnet, it can discover which other local subnets already has the package. These subnets are typically at a single customer site, specifically a single geographical location.

Nomad SSD uses Content Distribution. When a Nomad client downloads a package, it registers this information with Content Distribution, enabling a profile to be created on which Nomad clients hold particular packages.

Refer to Deploying software in large networks for scenarios for deploying software in large networks, utilizing Single-Site Download (SSD), and how you can monitor those deployments using the Nomad app.

Without SSD, an elected master for each subnet always accesses a Distribution Point (DP), often over a slow or congested WAN, even if a neighboring subnet in the LAN had the requested package. In practice, this had no major impact on WAN traffic as Nomad only uses a proportion of the current *free* network capacity rather than the total rated capacity, but efficiency can be improved by enabling access to Nomad caches on other subnets.

When a Nomad client requires a particular package, it attempts to find a copy on the local subnet. If it is unable to find one, it queries Content Distribution to see if there are Nomad clients on adjacent subnets that hold a copy. If it finds one, it will download the package from it; if it doesn't, it will download the package from the DP over the WAN as a last resort.

> **Note**
>
> Nomad reacts dynamically to network adapter changes, and if its IP address changes it will automatically update its subnet information in Content Distribution. So, for example, closing the lid of a laptop and moving it to another subnet and resuming work there is handled by Nomad.

How SSD interacts with other CD features

SSD works seamlessly with FanOut – FanOut applies to peers and SSD applies to subnet masters

SSD will use IP addresses if P2PEnabled registry value is set to use net literal names

Work rates only apply to downloads from a DP not to P2P transfers, therefore they do not affect downloads from peers when using SSD

When packages are purged from the cache, the corresponding entries are deleted from Content Distribution. If you delete content directly from the cache, Nomad will not be aware that it has been removed and the corresponding Content Distribution record will not be deleted. If that host subsequently becomes a site master, it will inform requesting Nomad clients that it does not have the package, forcing them to request the package from the next master in the list.

Refer to Enabling SSD in WinPE to make use of Nomad SSD in OS Deployment.

Restrictions

The mechanism does not support alternate source copy downloads, such as downloading an older version of a package from a LAN neighbor then filling in the changes

Only the initial 0% downloaded of a package and the final percentage (which can be < 100% if the entire package cannot be downloaded) are registered with Content Distribution. There are no "10% so far" etc. intermediate records

Even if a computer has multiple NICs, only details of one NIC and its subnet are used for SSD. If that NIC is unavailable, SSD will not work properly (although Nomad itself may be working correctly, using the DP rather than another site)

Remote differential compression (RDC) integration is not supported over SSD, it will not be used when a subnet master is copying from a site master

IPv6 is not supported.

9.4.2.2.1 Site and Local SSD

The local SSD feature was introduced to supplement site SSD for clients on networks such as wireless where broadcasts are disabled, to prevent each client becoming its own master and downloading direct from the DP. In a SSD enabled environment, a master queries Content Distribution to get a list of devices on other subnets within the site that have content. With local SSD enabled, the master also queries for devices having content within local subnet. If any local

peers with content are available, then the master downloads from them, otherwise it attempts to download from Site peers (other subnets in the site), and if the master still cannot find any peers, it downloads the content direct from the DP.

In version 7.0 and later, a master skips using local SSD if it sees broadcast messages from peers. This means clients in mixed network environments can be configured with the same SSDEnabled setting (with Local SSD enabled) and clients can move seamlessly between networks. When on a wireless network (where broadcasts are typically disabled) local SSD can be used. On LAN networks (where broadcasts are typically allowed) local SSD would be skipped because a master is elected and sees broadcast activity from peers.

9.4.2.2.2 Configuration

Before enabling clients to use SSD, you need to ensure the following:

1E platform 5.2 or later is installed and running successfully.

The Content Distribution database is populated with information about sites and their associated subnets.

9.4.2.2.2.1 How to enable SSD

The following information applies to both new and existing installations of Nomad:

Make sure that 1E platform is installed in your environment and is used as a content location metadata repository, for more information refer to Introducing Tachyon

Within Content Distribution, populate the SSD sites and subnet information. A sample PowerShell script called **PostADSitesandSubnets.ps1** is included in the Nomad installation files, which reads sites and subnets from AD

Nomad captures a list of background channels from the 1E Client in the BackgroundChannelUrl and uses the first working URL as the PlatformURL by appending /Proxy/ContentDistribution/ if this PlatformURL is unreachable it attempts to connect to the next BackgroundChannelUrl, for details about BackgroundChannelUrl refer to Tachyon Architecture

Enable SSD on all Nomad agents, by modifying **HKLM\Software\1E\NomadBranch\SSDEnabled** to 3, this enables SSD for both "Provide" and "Consume" modes, specifically Nomad will provide content to other peers and consume content from other peers

If you already have Nomad installed and are only now enabling SSD, then ensure **HKLM\Software\1E\NomadBranch\Platform\ContentRegistration** is set to 1, in other words Nomad will register downloaded content with Content Distribution, this is automatically enabled for new installations of Nomad, and SSD.

> **Tip**
>
> If you have clients on networks where broadcasts are disabled (for example wireless) then enable local SSD by setting SSDEnabled=7. Also set ContentProviderOnWifi=1.

9.4.2.2.2.2 Building a subnet profile in Content Distribution

For Content Distribution to build a subnet profile for SSD and the peer backup assistant feature, Nomad must communicate with its web service. When the Nomad service starts, it connects and registers the hosting device by name with Content Distribution, which returns a device ID in the form of a GUID that enables it to uniquely identify the Nomad client and its default subnet. If it is

unable to communicate with Content Distribution, it retries every 5 minutes until it succeeds (as long as SSD is enabled). An attempt to communicate with Content Distribution is also made prior to a package download to register its status.

Please refer to Enabling SSD in WinPE to make use of Nomad SSD in OS Deployment.

The following points should be noted:

On a multi-NIC host, only one NIC gets registered, and a wired interface takes precedence over a wireless interface during registration

If Nomad fails initially to register an adapter, it retries every 5 minutes (for as long as SSD is enabled) until it succeeds

Wireless adapters can be configured to act as SSD content providers and consumers. Use the ContentProviderOnWiFi registry setting to do this

If the initial device registration was successful when the Nomad service started, but Content Distribution later becomes unavailable, when Nomad subsequently downloads and caches a package it will not be able to register the package with Content Distribution (see below for details). Nomad does not re-attempt package registration, so Content Distribution will not know that this particular Nomad host has the package.

9.4.2.2.2.3 Example PowerShell scripts

You can get information about sites and subnets from AD, or by other means. Example PowerShell scripts can be used for retrieving information about sites and their associated subnets from the AD and updating the Content Distribution database.

Refer to Nomad Branch Tools for details.

9.4.2.2.2.4 Viewing Nomad sites and subnets in the Nomad app

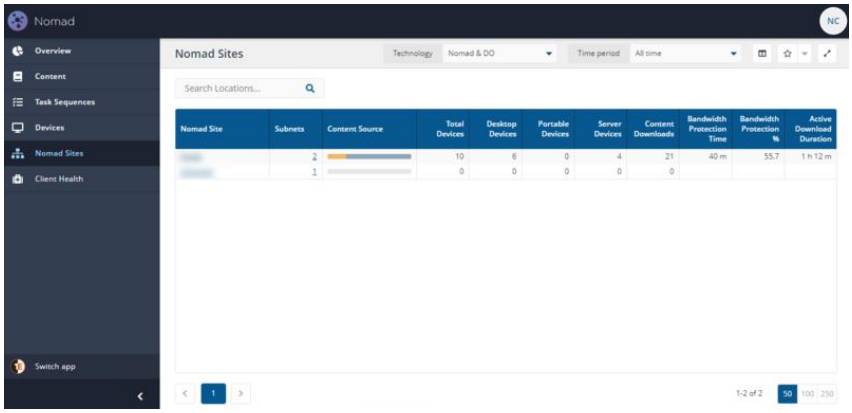
The sites and subnets stored in Content Distribution are visible in the Nomad Sites page of the Nomad app.

The Nomad Sites page is primarily designed to show how the network is being used for content distribution in different locations. It focuses on the volume of content downloaded from peers vs over the WAN, rather than the status of specific Content Titles in a given site. You can see what content is available in a given site by looking at the Content tab for that site.

> **Note**
>
> A Nomad Site corresponds to Nomad Single Site Download (SSD) site. Customers that have implemented SSD and upgrade ActiveEfficiency to the Nomad app and Content Distribution will see their defined SSD locations displayed as **Nomad Sites** in the app.
>
> Any subnets that are not included in a Nomad SSD Site definition will be represented in a site named **Unknown**. If no SSD sites have been defined, all subnets will be included in the 'Unknown' site.

> **Note**
>
> The Nomad app provides visibility of content distribution activity and cache status for content distributed by both Nomad and Delivery Optimization. This includes

Configuration Manager content distributed with Nomad and Software Updates content distributed with either Nomad or Delivery Optimization.



9.4.2.2.2.5 *Uninstallation, reinstallation and reactivation*

When you uninstall a Nomad client, all its registry values are deleted. However, if you subsequently reinstall it, the device ID returned when Nomad next registers with Content Distribution is one that is recycled from the database – this is because that is the device registered for the named computer, so it recognizes that the same computer is involved and restores the previous values to the registry.

> **Note**
>
> If you change the host name or domain, Nomad and Content Distribution will regard this as a new computer and generate a new device ID for it.

If a cached package is reactivated, such as after an OSD upgrade or cloning, Nomad will register the package with Content Distribution. (If this is a re-registration, the Content Distribution record is effectively unchanged).

9.4.2.2.2.6 *Improved resilience of content registration*

The **Content Registration Sync Cycle** is available in Nomad 7.0 or later (1E Client 4.1 or later) which registers pending and failed content registrations with Content Distribution.

Registrations can fail when Content Distribution or the SQL Server hosting the ContentDistribution database is busy, overloaded or down for maintenance, resulting in content registration mismatch between the clients and Content Distribution.

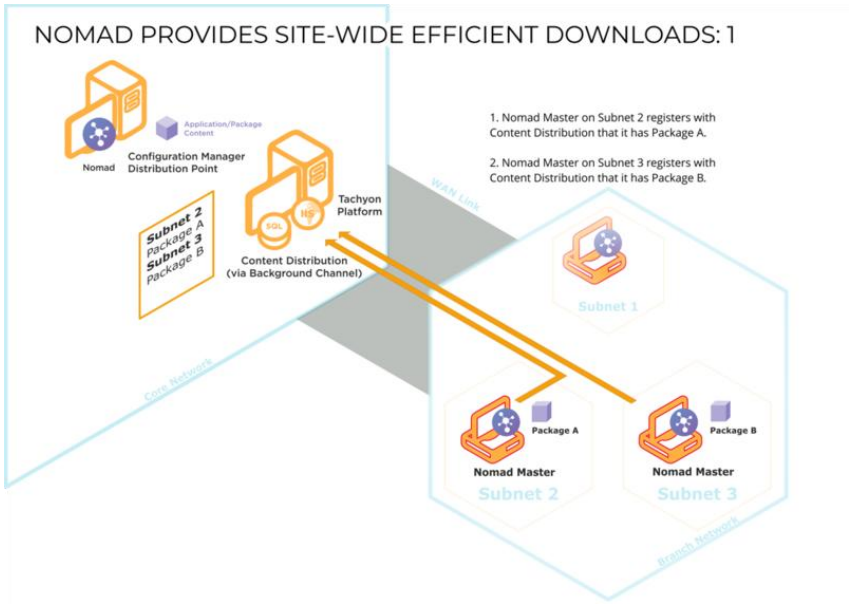
The following registry setting is used by the **Content Registration Sync Cycle** feature.

Registry value	Type	Default	Notes	Installer property
CacheStateSyncIntervalMinutes	REG_DWORD	1440 (1day)	Range: from 60 to	MODULE.NOMAD.CACHESTATESYNCINTERVALMINUTES

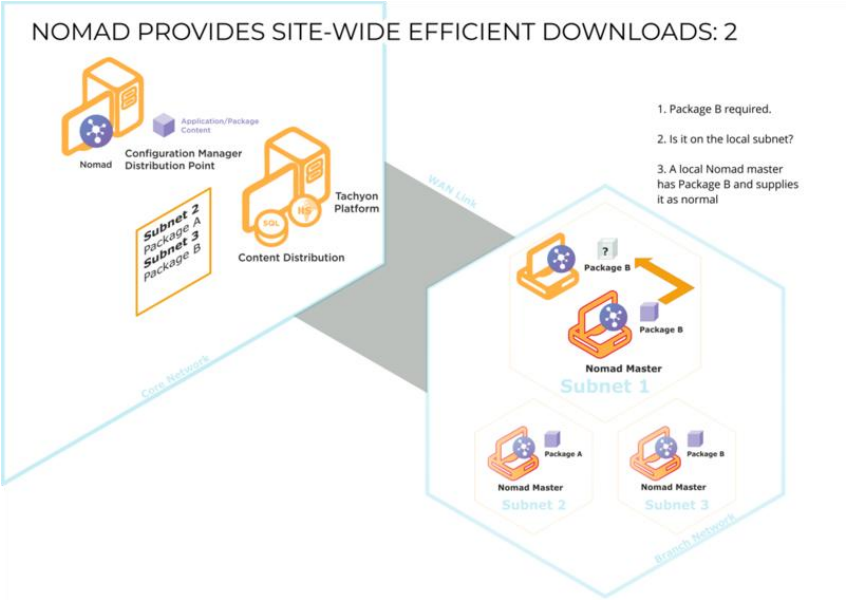
Registry value	Type	Default	Notes	Installer property
			525600 (1Year).	

9.4.2.2.3 How it works

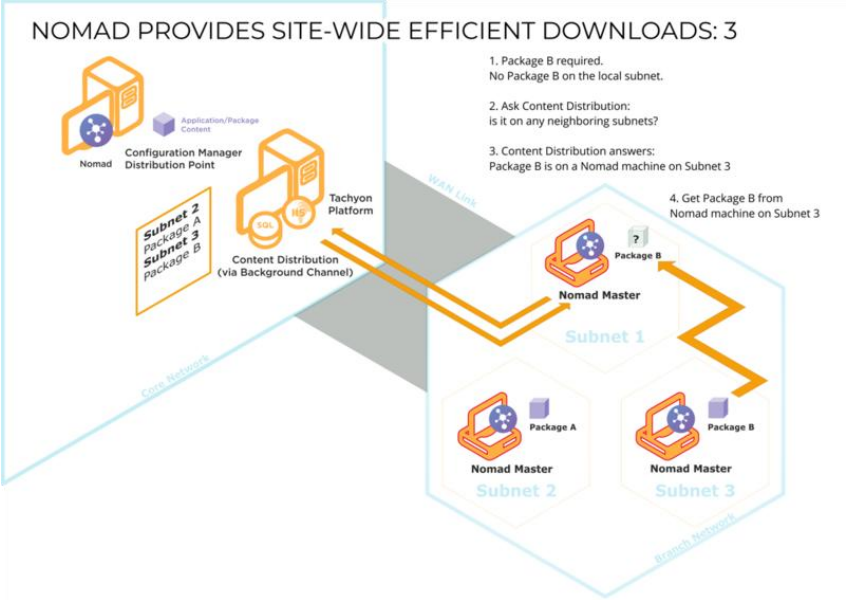
The information about sites and their associated subnets are stored and maintained in Content Distribution. When a Nomad client downloads a package, it registers this information with Content Distribution, enabling it to build a profile of which Nomad client holds particular packages and on which subnet.



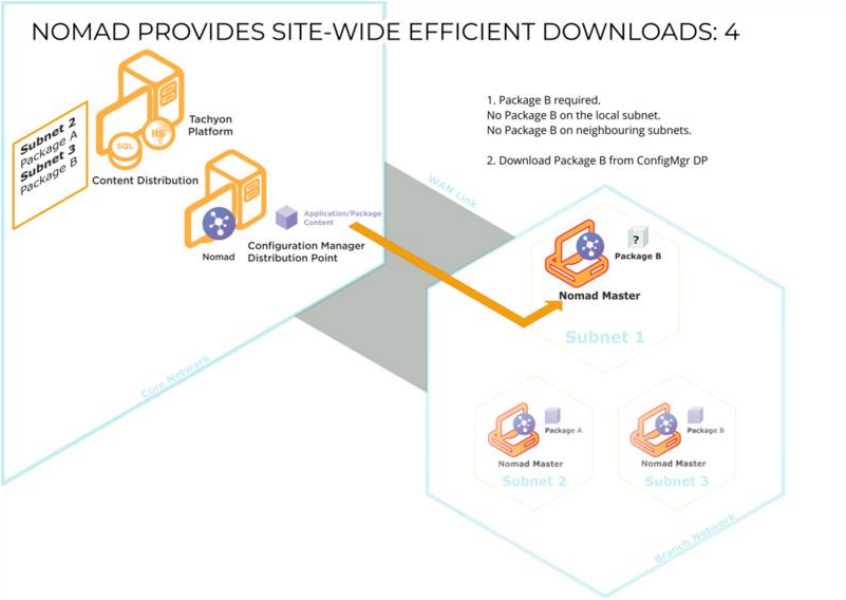
When a Nomad client on a subnet requires a particular package, it first tries to find a copy on the local subnet using the standard method for retrieving cached Nomad files.



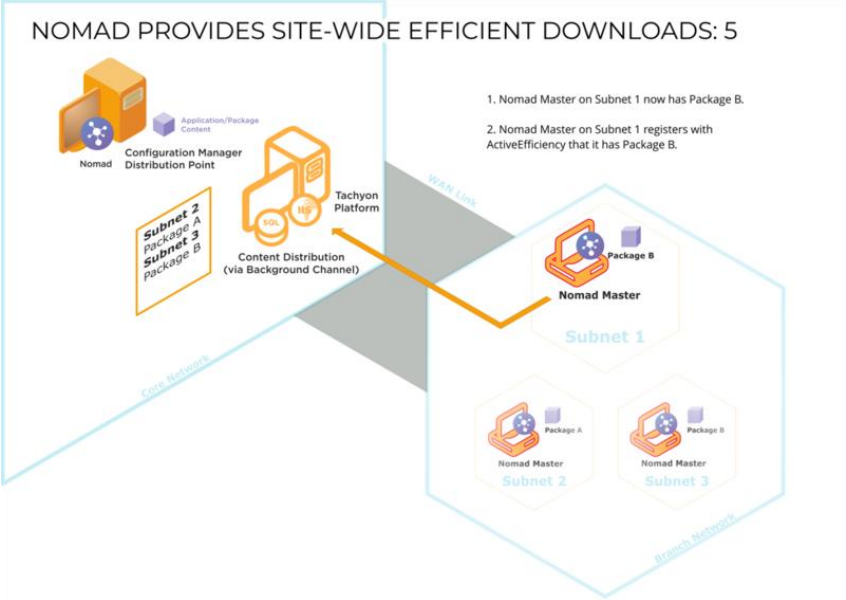
If no local copy of the package is found it then tries Content Distribution database to see if any Nomad clients on other subnets at the same site hold a copy.



Only when all other avenues have failed will Nomad resort to downloading the package from the DP over the WAN.



When the master has a portion of the package it, registers itself with Content Distribution to say that it can provide this package to other subnets if required.



9.4.2.2.3.1 Fetching content

When Nomad receives a request to download content, an election takes place for a master. The master queries Content Distribution about neighboring subnets (accessible on LAN rather than WAN) so that it can download content from a peer in an adjacent subnet (within the same location) if that content is not available on a peer in its own local subnet. For each subnet, the top 10 Nomad clients (in terms of percentage cached by the Nomad client) are listed – the subnet containing the master is excluded from the list if no peer has the content. During this process, the percentage specified by the requesting client is ignored. Although neighboring Nomad clients may have a lower percentage than the requesting Nomad client, they may in fact have gained more

since they last communicated with Content Distribution, so they are potentially useful sources for the package, hence the top 10 rule.

The master (now a subnet master) iterates through the list (which is sorted by percentage) and sends a package status request to each Nomad client. If it receives a response, the master attempts an SMB peer-to-peer download from that Nomad client (the current site master). If the attempt fails (it is not contactable or the limit on the number of concurrent connections is exceeded), it tries the next one in the list. If it fails to get the package from any of them, it downloads from the DP. If the list is empty, the master downloads from the DP. Nomad clients with a lower percentage of the package than the Nomad client requesting it will not respond.

> **Note**
>
> Nomad peers never deal with SSD; they only copy packages from their subnet's master. The subnet master may have the package completely cached or it may be actively downloading from another site or from a DP – the source makes no difference to the peer

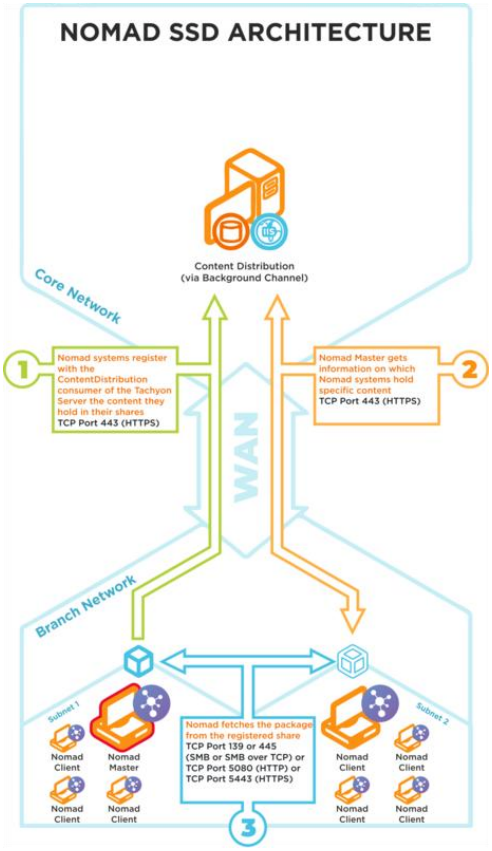
If a download is interrupted part way through (i.e. the source becomes unavailable), Nomad iterates through the remainder of the list and if it fails to get the package from any of them, it downloads from the DP.

When a download starts, Nomad registers the progress with Content Distribution (0% of the content has been downloaded) and when it finishes, the final percentage is also recorded. As long as the content downloaded is greater than 0%, the host becomes a candidate for another client until the package is deleted from its cache. Records with status of 0% downloaded are purged from Content Distribution.

> **Note**
>
> All Nomad clients that have SSD enabled will register content download with Content Distribution, not just the subnet master.

> **Note**
>
> If the Nomad client is running as a guest on VMware, it registers itself as *DeviceType=0* in the Content Distribution Consumer. Content Distribution excludes these devices from SSD query results as they are deemed ineligible to provide content.

9.4.2.2.4 Architecture and ports



Nomad SSD uses the following ports in its communications:

Ports	Notes
TCP 80 (HTTP)	**Step 1**
TCP 443 (HTTPS)	Nomad systems on the branch site register in Content Distribution the content they hold in their shares
TCP 80 (HTTP)	**Step 2**
TCP 443 (HTTPS)	Nomad Masters get information on which Nomad systems hold specific content
TCP 80 (HTTP)	**Step 3**
TCP 443 (HTTPS) TCP 139 (SMB)	Nomad Master fetches a package from the registered Nomad share on a neighboring subnet

Ports	Notes
TCP 445 (SMB over TCP)	

We recommend that the latest version of Tachyon Platform is installed to support this feature, please refer to Requirements for more details.

9.4.2.2.5 Enabling SSD in WinPE

To enable SSD in WinPE:

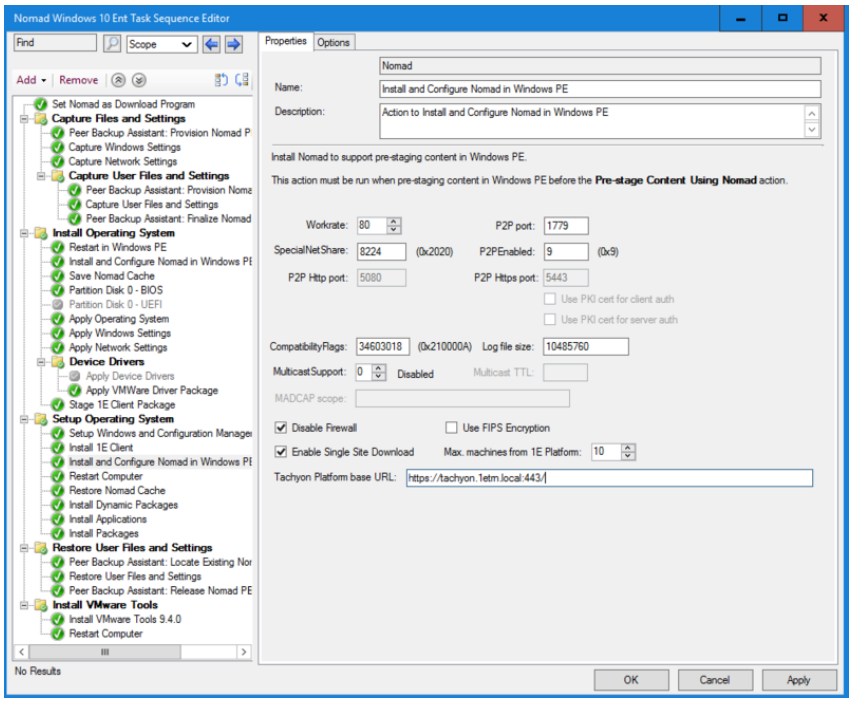
Edit the task sequence for which you want to use SSD.

Enable **Single Site Download**.

In **Tachyon Platform base URL:** enter for example, *https://<server_FQDN:port/* or *http://<server_FQDN:port/* depending on the protocol you are using, where **<server_FQDN>** is the FQDN of the Tachyon server or its DNS alias.

Click **OK**.

> **Note**
>
> After you upgrade to Nomad 8.1 you will need to update any pre-existing task sequences using this step to reflect the move from ActiveEfficiency to the Tachyon Platform.



9.4.2.2.6 Example Active Directory Single Site script

Sample script that scans the Active Directory (AD) environment for all sites and subnets and stores the information in the Content Distribution locations table. This information can then be retrieved

by Nomad at a later stage when implementing the Single Site Download (SSD) or Single Site PBA features.You can view Nomad Sites in the Nomad Sites page.

The Nomad Sites page is primarily designed to show how the network is being used for content distribution in different locations. It focuses on the volume of content downloaded from peers vs over the WAN, rather than the status of specific Content Titles in a given site. You can see what content is available in a given site by looking at the Content tab for that site.

Note

A Nomad Site corresponds to Nomad Single Site Download (SSD) site. Customers that have implemented SSD and upgrade ActiveEfficiency to the Nomad app and Content Distribution will see their defined SSD locations displayed as **Nomad Sites** in the app.

Any subnets that are not included in a Nomad SSD Site definition will be represented in a site named **Unknown**. If no SSD sites have been defined, all subnets will be included in the 'Unknown' site.

9.4.2.2.6.1 Prerequisites

Note

You can download the 1E Content Distribution Tools from the **Releases** page for your platform version at https://support.1e.com/.

The script requires:

Content Distribution version 8.0 or above.

Use PowerShell version 5.0 or above.

Run the script on a device joined to the AD domain where the required information resides and have permissions to read device attributes from AD.

9.4.2.2.6.2 Using the example PostADSitesandSubnets script

The sample script:

Clears all current sites and subnet information stored in the ContentDistribution database.

Connects to LDAP://RootDSE and enumerates the subnets for each Site and adds them to the ContentDistribution database.

Note

The example script does not support supernets.

You can modify the script to include filters and logic to ignore or add specific Sites or subnets.

Note

If you prefer to maintain your own list of Sites and subnets then you should consider using Example Single Site script, or Example Location Discovery script, instead.

9.4.2.2.6.2.1 Parameters

The script uses the following parameters:

PlatformUrl as a mandatory parameter - you must provide the platform base URL

Tls12 as an optional switch parameter - include this switch if TLS 1.2 is required to connect to your platform server.

For example, to run the script on a PowerShell command-line:

Example

```
.\PostADSitesandSubnets.ps1 -PlatformUrl https://tachyon.1etrn.local:443 -Tls12
```

9.4.2.2.6.2.2 How it works

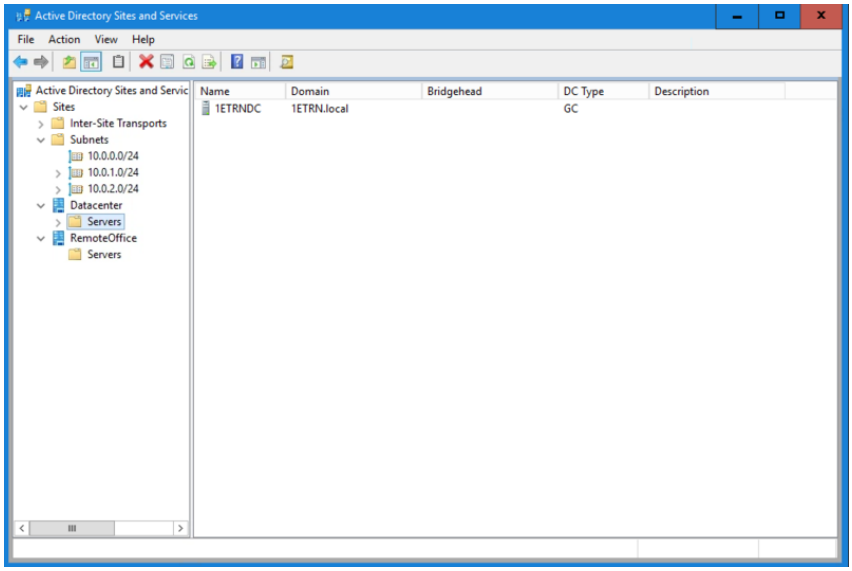
The script clears all current sites and subnet information stored in the ContentDistribution database, it then scans the Active Directory for stored sites and subnets and stores these in ContentDistribution. The AD environment scanned, is for the domain containing the device where you run the script.

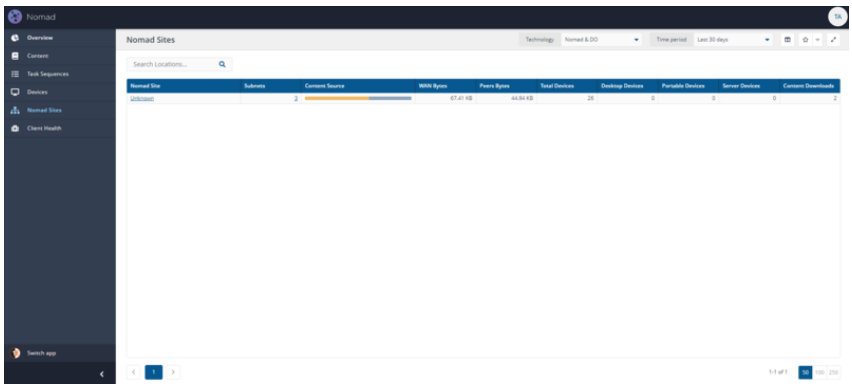
In our example, we have two distinct locations (a datacenter and a remote office), with the servers all located in the datacenter and the workstations all located in the remote office. It just so happens that the remote office has two subnets. Active Directory Sites have already been defined to reflect this configuration.

Before running **PostADSitesandSubnets.ps1** we only have an unknown Nomad site as you can see in the accompanying picture showing the Nomad Sites page.

The Nomad Sites page is primarily designed to show how the network is being used for content distribution in different locations. It focuses on the volume of content downloaded from peers vs over the WAN, rather than the status of specific Content Titles in a given site. You can see what content is available in a given site by looking at the Content tab for that site.

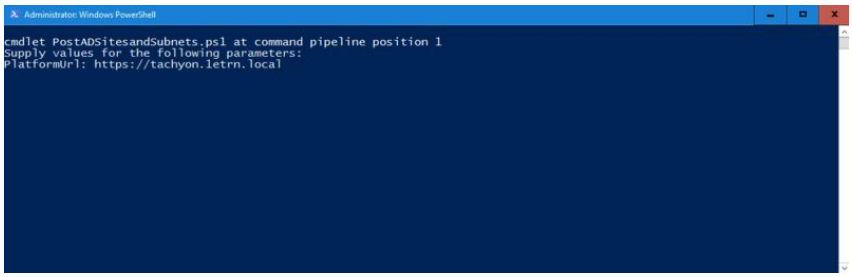
> **Note**
>
> A Nomad Site corresponds to Nomad Single Site Download (SSD) site. Customers that have implemented SSD and upgrade ActiveEfficiency to the Nomad app and Content Distribution will see their defined SSD locations displayed as **Nomad Sites** in the app.
>
> Any subnets that are not included in a Nomad SSD Site definition will be represented in a site named **Unknown**. If no SSD sites have been defined, all subnets will be included in the 'Unknown' site.



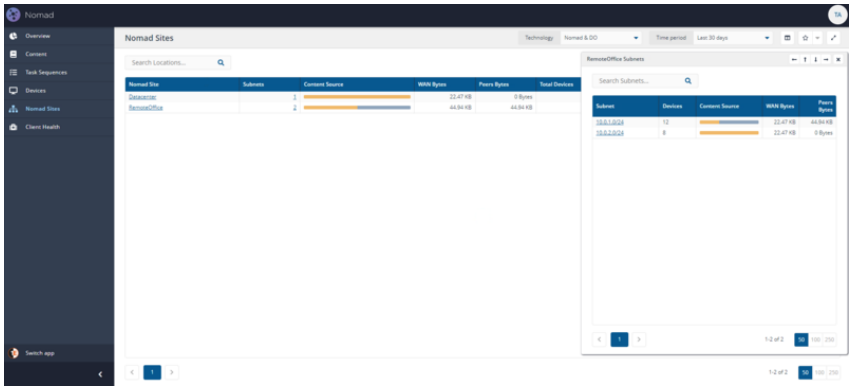


In our example we downloaded the script to **C:\Temp\nomadbranch.v8.0.4.265\scripts** folder, we right-click on **PostADSitesandSubnets.ps1** and select **Edit** to open the file in Windows PowerShell ISE.

We enter *https://tachyon.1etrn.local/* as the platform url for our environment and hit return.



Once the script completes we can return to the Nomad app and refresh the page, now we can see our environment's sites and subnets defined on the Nomad sites page.



9.4.2.2.7 Example Single Site script

Sample script that provides two functions to update sites and subnets in the Content Distribution locations table: DeleteAllLocations and AddLocation(). This information can then be retrieved by Nomad at a later stage when implementing the Single Site Download and Single Site PBA features. You can view Nomad Sites in the Nomad Sites page.

The Nomad Sites page is primarily designed to show how the network is being used for content distribution in different locations. It focuses on the volume of content downloaded from peers vs over the WAN, rather than the status of specific Content Titles in a given site. You can see what content is available in a given site by looking at the Content tab for that site.

> **Note**
>
> A Nomad Site corresponds to Nomad Single Site Download (SSD) site. Customers that have implemented SSD and upgrade ActiveEfficiency to the Nomad app and Content Distribution will see their defined SSD locations displayed as **Nomad Sites** in the app.
>
> Any subnets that are not included in a Nomad SSD Site definition will be represented in a site named **Unknown**. If no SSD sites have been defined, all subnets will be included in the 'Unknown' site.

9.4.2.2.7.1 Prerequisites

The **ExampleSitesAndSubnets.ps1** script is available from the **Scripts** folder in the 1E Content Distribution Tools download zip.

> **Note**
>
> You can download the 1E Content Distribution Tools from the **Releases** page for your platform version at https://support.1e.com/.

Content Distribution 8.0 or above.

PowerShell version 5.0 or above.

9.4.2.2.7.2 Using the example Single Site script

The sample script includes an example of how the script can be used:

Clears all current sites and subnet information stored in the ContentDistribution database.

Adds the following 3 sites and subnets in the ContentDistribution database.

"HOMER.SIMPSON.Springfield" "192.148.226.0/24"

"HOMER.SIMPSON.Springfield" "192.148.228.0/24"

"MARGE.SIMPSON.Springfield" "192.168.227.0/24"

Before using it in your environment, you must edit the script to replace the example "HOMER" site and subnets with your own list. Over time, you will manually modify the script to reflect your environment.

Note

The example script does not support supernets.

Note

If you prefer to automatically add Sites and subnets by querying AD, then you should consider using Example Active Directory Single Site script instead.

Parameters

The script uses the following parameters:

PlatformUrl as a mandatory parameter - you must provide the Tachyon Platform base URL.

Tls12 as an optional switch parameter - include this switch if TLS 1.2 is required to connect to the Tachyon Platform server.

For example, to run the script on a PowerShell command-line:

```
.\ExampleSitesandSubnets.ps1 -PlatformUrl https://tachyon.acme.local:443 -Tls12
```

9.4.2.2.7.2.1 How it works

The sample script provides the following two functions:

Script functions

```
function DeleteAllLocations()
Description: Deletes all rows from the ContentDistribution locations table
Params: none
Return: $result(empty)

function AddLocation()
Description: Adds a new entry into the ContentDistribution locations table
Params: site  - [string] containing the site name
             subnet - [string] containing the ipv4subnet in CIDR notation
Return: $result - newly created location object of the form #     {"Id":"efa192
26-266f-4bd0-8a9d-94fa5ac1b773","Site":"HOMER.SIMPSON.Springfield","Subnet":"19
2.148.226.0/24"}
```

You must edit this section with your own list of sites and subnets:

```
# optional will delete all existing entries
DeleteAllLocations

# sample adding 3 locations using the AddLocation function
# duplicate entires will report an error: (409) conflict
AddLocation "HOMER.SIMPSON.Springfield" "192.148.226.0/24"
AddLocation "HOMER.SIMPSON.Springfield" "192.148.228.0/24"
AddLocation "MARGE.SIMPSON.Springfield" "192.168.227.0/24"
```

9.4.2.2.8 Example Location Discovery script

Sample script to enable and disable the location discovery feature, along with the option to run it and load site, subnet and information in Content Distribution. This information can then be retrieved by Nomad at a later stage when implementing the Single Site Download (SSD) or Single Site PBA features.You can view Nomad Sites in the Nomad Sites page.

The Nomad Sites page is primarily designed to show how the network is being used for content distribution in different locations. It focuses on the volume of content downloaded from peers vs over the WAN, rather than the status of specific Content Titles in a given site. You can see what content is available in a given site by looking at the Content tab for that site.

> **Note**
>
> A Nomad Site corresponds to Nomad Single Site Download (SSD) site. Customers that have implemented SSD and upgrade ActiveEfficiency to the Nomad app and Content Distribution will see their defined SSD locations displayed as **Nomad Sites** in the app.
>
> Any subnets that are not included in a Nomad SSD Site definition will be represented in a site named **Unknown**. If no SSD sites have been defined, all subnets will be included in the 'Unknown' site.
>
> **Note**
>
> You can download the 1E Content Distribution Tools from the **Releases** page for your platform version at https://support.1e.com/.

The **1E Nomad** product pack is included in the platform zip. The platform zip file can be downloaded from https://support.1e.com/. Additional Product Packs are available from 1E Exchange.

The sample script requires:

ContentDistribution version 8.0 or above is installed.

1E platform with the Nomad consumer provisioned.

The**1E-Nomad-LocationDiscovery**instruction is uploaded and permissioned appropriately. The typical configuration is:

The **1E Nomad** product pack is uploaded into an Instruction set called **1E Nomad**.

The **Nomad Administrator** role is configured with **Actioner** permissions on the **1E Nomad** instruction set, and the **All Devices** management group.

The account used to run the script must be a platform user with the **Nomad Administrator** role assigned.

CSV file – described below.

9.4.2.2.8.1 CSV file

The **LocationDiscovery.ps1** script uses a CSV file as input, and accepts several parameters.

The input file should be made up of four columns, without column headers:

Site name

CIDR notation subnet associated with that site

Latitude of the site

Longitude of the site

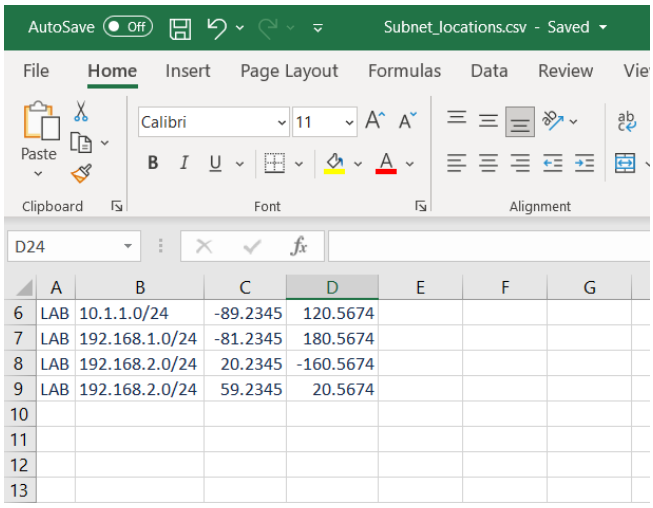
An example of the file contents for a site named LAB with four subnets would be:

LAB,10.1.1.0/24,-89.2345,120.5674

LAB,192.168.1.0/24,-81.2345,180.5674

LAB,192.168.2.0/24,20.2345,-160.5674

LAB,192.168.2.0/24,59.2345,20.5674



	A	B	C	D	E	F	G
6	LAB	10.1.1.0/24	-89.2345	120.5674			
7	LAB	192.168.1.0/24	-81.2345	180.5674			
8	LAB	192.168.2.0/24	20.2345	-160.5674			
9	LAB	192.168.2.0/24	59.2345	20.5674			
10							
11							
12							
13							

9.4.2.2.8.2 Using the example Location Discovery script

9.4.2.2.8.2.1 Parameters

The **LocationDiscovery.ps1** has the following configurable parameters:

Parameter	Description
TLS12	TLS12 is an optional switch type parameter. Include this switch if TLS 1.2 is required to connect to the CD server.

Parameter	Description
GetSettings	GetSettings is used to fetch the existing configured settings of the location discovery feature.
Enable	Enable is a switch to turn-on the location discovery feature. If this feature is enabled, a user needs to use the "execute" switch to download the automatic grouping of sites and subnets.
Disable	Disable is a switch to turn off the location discovery feature. If this feature is disabled, grouping of locations and subnets has to be provisioned by scripting in the ContentDistribution LocationsV2 table.
Execute	Execute is a switch to trigger automatic location discovery instruction and automates download of the Excel file containing sites and subnet grouping. This step takes at least 45 minutes, and depends on your devices and network topology.
OutPath	OutPath is a mandatory parameter in case of Execute switch is present. It indicates where the result file should be downloaded. The path should already exist.
InterSiteDistance	InterSiteDistance is a mandatory parameter to be configured if the location discovery feature is enabled. By default, its value is 500 meters.
Upload	Upload is a parameter used for uploading the Excel file containing site, subnet, latitude, longitude fields in the ContentDistribution LocationsV2 table. This step will take a backup of the existing LocationsV2 table, truncates it and loads new data from an input Excel file. If Excel is not loaded successfully, then the previous LocationsV2 table entries will be loaded again.
CDServer	CDServer is a mandatory parameter. You must provide the name of the ContentDistribution web server using this parameter.
Protocol	Protocol is a mandatory parameter. You must indicate if the ContentDistribution web server is configured for HTTP or HTTPS connections.

9.4.2.2.8.2.2 Example PowerShell command lines

The example **LocationDiscovery .ps1** script can be run on a PowerShell command line as shown in the following examples, where 1Etrnap.1etrn.local is the ContentDistribution server in our sample environment:

Get location discovery feature settings:

```
.\LocationDiscovery.ps1 -Disable -CDServer 1Etrnap.1etrn.local -Protocol http
```

Configure inter-site distance for location discovery feature:

```
.\LocationDiscovery.ps1 -InterSiteDistance 50 -CDServer 1Etrnap.1etrn.local -Pr
otocol http
```

Execute location discovery feature:

```
.\LocationDiscovery.ps1 -Execute -CDServer 1Etrnap.1etrn.local -Protocol http -
OutPath C:\Temp\
```

Import Site and Subnet information from C:\Temp\network.csv using HTTP after clearing the Locations table:

```
.\LocationDiscovery.ps1 -Upload C:\Temp\network.csv -CDServer 1Etrnap.1etrn.loc
al -Protocol http
```

9.4.2.2.9 Content Distribution purge configuration script

Sample script to view or update Purge Configuration in the Content Distribution Service defined in the ContentDistribution PurgeSettings table if it is configured.

9.4.2.2.9.1 Prerequisites

> **Note**
>
> You can download the 1E Content Distribution Tools from the **Releases** page for your platform version at https://support.1e.com/.

To script requires:

ContentDistribution version 8.0 or above is installed.

Use PowerShell version 5.0 or above.

1E platform has the Nomad consumer provisioned.

The account used to run the script must be a platform user with the **Nomad Administrator** role assigned.

9.4.2.2.9.2 Using the example Content Distribution purge configuration script

Parameters

The script uses the following parameters:

Parameter	Required	Description
CDServer	Mandatory	The hostname or FQDN of the CD server, as needed in your environment.

Parameter	Required	Description
Get	Optional	Include this switch to view the existing purge configuration. One of the switch from "-Get" and "-Update" should be specified.
Update	Optional	Include this switch to update the existing purge configuration. If this switch is enabled, the other 2 switches should also be enabled - **PurgeSchedule_HoursIn24HrFormat** and - **PurgeSchedule_Minutes**.
PurgeSchedule_HoursIn24HrFormat	Mandatory in case of -Update switch else optional.	It can take the value between 0-23 (inclusive).
PurgeSchedule_Minutes	Mandatory in case of -Update switch else optional.	It can take the value between 0-59 (inclusive).
Tls12	Optional	Include this switch if TLS 1.2 is enabled.
Protocol	Optional	The protocol for connecting to the server, either HTTP or HTTPS. By default, it is HTTPs.

9.4.2.2.9.2.1 Example PowerShell command lines

The **CDPurgeSettings.ps1** script can be run on a PowerShell command line as shown in the following examples, where *tachyon.1etrn.local* is the PlatformURL for our sample environment:

View the existing Purge configuration with HTTPS protocol and **Get** switch:

```
.\CDPurgeSettings.ps1 -Get -Protocol https -CDServer tachyon.1etrn.local:443
```

Update the existing purge configuration with HTTP protocol with confirmation:

```
.\CDPurgeSettings.ps1 -Update -PurgeSchedule_HoursIn24HrFormat 20 -PurgeSchedul
e_Minutes 10 -Protocol http -CDServer tachyon.1etrn.local:80
```

Update the existing purge configuration with HTTPS protocol with confirmation:

```
.\CDPurgeSettings.ps1 -Update -PurgeSchedule_HoursIn24HrFormat 20 -PurgeSchedul
e_Minutes 10 -Protocol https -CDServer tachyon.1etrn.local:443
```

Update the existing purge configuration with HTTP protocol and **tls12** support:

```
.\CDPurgeSettings.ps1 -Update -PurgeSchedule_HoursIn24HrFormat 20 -PurgeSchedul
e_Minutes 10 -Protocol http -Tls12 -CDServer tachyon.1etrn.local:80
```

9.4.2.3 Nomad Pre-caching

Pre-caching lets you preload the Nomad caches of particular machines directly from the Configuration Manager console. This enables downloads to be available on the branch prior to a deployment taking place, which can be very useful in large-scale deployment scenarios.

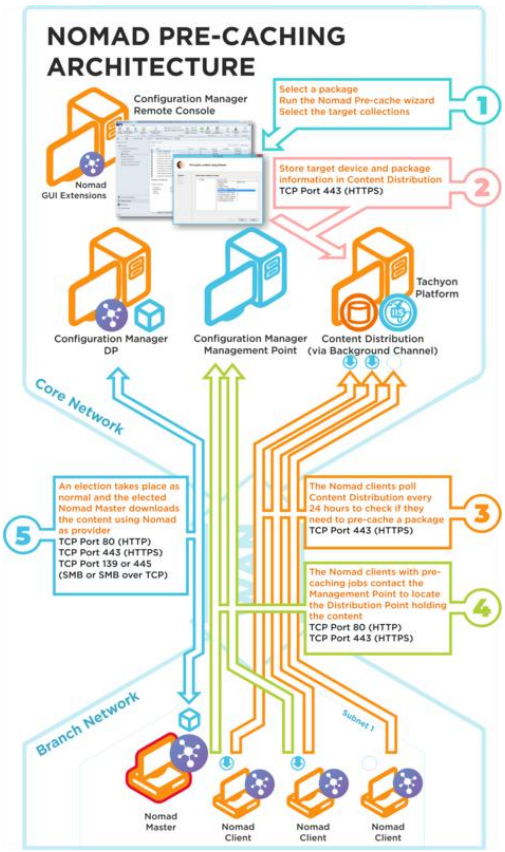
Before you start, ensure the following prerequisites are met:

Tachyon Platform 5.2 or later is accessible, with Nomad features enabled

Nomad Configuration Manager console extensions must be installed.

Refer to Using Nomad with Operating System Deployment OSD for example scenarios about how to use Nomad to maximize the efficiency of distributing large OS content across the network and how you can monitor those deployments using the Nomad app.

9.4.2.3.1 Architecture and ports



The Nomad pre-caching uses the following ports in its communications. If a site server is configured to use custom ports, pre-caching will use those ports to communicate with a management or distribution points. To ensure high-availability, pre-caching falls back to next available site server if it fails to communicate with a management or distribution point.

Ports	Description
N/A	**Step 1** Choose a package and run the Nomad pre-caching wizard, selecting the target device collection. This step does not require any port configuration but the Nomad Configuration Manager console extensions must be installed in the Configuration Manager Console.
TCP 80 (HTTP) TCP 443 (HTTPS)	**Step 2** The Nomad pre-caching wizard stores the target device and package information in Tachyon.
TCP 80 (HTTP) TCP 443 (HTTPS)	**Step 3** The Nomad clients, where the pre-cache feature has been enabled, poll Tachyon every 24 hours to see if they need to pre-cache some content. This takes the form of pre-caching notifications that tell the Nomad clients they need to process a download job to fetch the specified content.
TCP 80 (HTTP) TCP 443 (HTTPS)	**Step 4** The Nomad clients, with pre-caching notifications, contact the Management Point to locate the Distribution Point that holds the content. This may use HTTP or HTTPS depending on how the Management Point is configured.
TCP 80 (HTTP) TCP 443 (HTTPS) TCP 139 (SMB) TCP 445 (SMB over TCP)	**Step 5** A Nomad Master election takes place and the elected master processes the job by downloading the pre-cache content using Nomad as provider. This is then distributed locally to the Nomad peers that also require the pre-cached content. This communication depends on how the DP is configured. It may be one of the following: HTTP HTTPS SMB

Ports	Description
	SMB over TCP For Configuration Manager the default setting is either HTTP or HTTPS.

9.4.2.3.2 Enabling Nomad pre-caching

When you consider how to install the Nomad Branch Tools (refer to Installing Nomad Branch Tools), you can also install them in unattended mode by using the MODULE.NOMAD.PLATFORMURL installer property or by setting the PlatformURL registry value on the machine where the extensions are installed post-installation.

> **Note**
>
> If you have an existing Nomad 7.0.200 installation, and you upgrade to Tachyon Platform 8.1 you should also upgrade your Nomad Configuration Manager console extensions to the current version, doing this ensures you can view your pre-existing Nomad pre-cache jobs. When you upgrade from earlier versions of Nomad to Tachyon Platform, ActiveEfficiency is upgraded to Content Distribution. As a result, if you have an earlier version of the Nomad Configuration Manager console extensions, you may not be able to view your existing Nomad pre-cache jobs until you upgrade.

Nomad clients must also be configured to support pre-caching. This is done during installation in the Nomad screen of the 1E Client installer, for more details refer to Installing the 1E Client for Nomad.

Setting	Description
Enable Nomad	Check this box to enable Nomad. Nomad is used to support efficient content download for Configuration Manager and Tachyon. For Tachyon, its Nomad content download feature is enabled by default but only used if Nomad is enabled. **Note** If Nomad is enabled, when the 1E Client starts it will upgrade any previous installation of the NomadBranch client.
Enable 1E Platform features	Check this box to let you configure the Single-Site Download (SSD) options and WakeUp integration.

Setting	Description	
	Options	Enabled
	Content Registration only	This configures Nomad to use **Single Site Download** to *provide* content to peers by registering the content it has in its cache in Content Distribution on the Tachyon Platform. In the registry SSDEnabled is set to 2 and ContentRegistration is set to 1. This also allows content to be reported in Nomad app dashboards and Device View. Typically, content registration should be enabled, unless there is a specific reason for a computer not to be a master. Content Registration is automatically disabled in WinPE.
	Single-Site Download (SSD) only	This configures Nomad to use **Single Site Download** and *consume* content which has been registered in Content Distribution on the Tachyon Platform. SSD is used as a fallback if the client is unable to find content on the local subnet. In the registry SSDEnabled is set to 1 and ContentRegistration is set to 1. Nomad queries Content Distribution on the Tachyon Platform asking for peers that have registered content.
	Both enabled	This configures Nomad to use **Single Site Download** so that it can both *consume and provide* content, as well as reporting in the

Setting	Description
	Nomad app and Device View. In the registry SSDEnabled is set to 3 and ContentRegistration is set to 1. This is the recommended configuration unless there is a specific reason for a computer not to be a master. Content Registration is automatically disabled in WinPE.
Neither enabled	The client does not participate in **Single Site Download** activities, and does not report content details to Content Distribution. In the registry SSDEnabled is set to 0 and ContentRegistration is set to 0. **Enable 1E Platform features** has no effect, and is ignored.

If you need to enable reporting but prevent the Nomad client acting as an SSD provider, then use installer properties or mst transform files to configure MODULE.NOMAD.SSDENABLED and MODULE.NOMAD.CONTENTREGISTRATION.

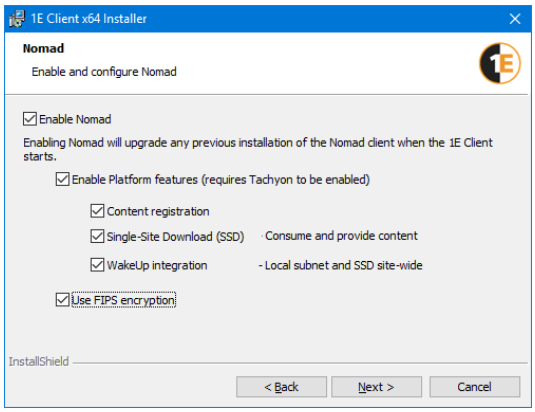
For more information about SSD, please refer to Single Site Download.

Options	Enabled
WakeUp integration	If you check **WakeUp integration** but not **Single Site Download (SSD)**, any attempt to wake-up peers with particular content will only be on the local subnet. If **Single Site Download (SSD)** is also checked, Nomad will try to wake peers with particular content in neighboring subnets on the site if peers on the local subnet do not wake.

Setting	Description
	Note The Platform settings are only available if you have enabled Tachyon. **Note** These settings do not affect other Platform features such as Pre-caching.
Use FIPS encryption	Checking **Use FIPS Encryption** configures the Nomad module to use FIPS encrypted communications. You must ensure that Nomad is configured with the same **FIPS encryption** setting on all your 1E Clients.

Note

Although the **Single-Site Download** option must be enabled in the installer, you can use the Nomad pre-caching feature without using SSD by not configuring the Single Site Download feature. If you are already using the SSD feature in your environment, no further Nomad client configuration will be required to enable Nomad pre-caching.



9.4.2.3.3 Using Nomad pre-caching

Nomad pre-caching is directly integrated with the Configuration Manager Console, is fully compliant and works with Role Based Access in Configuration Manager, refer to Nomad pre-caching RBAC support for details.

To start the pre-cache wizard, right-click any of the following types of content in the Configuration Manger console and from the context menu, choose Pre-cache content using Nomad.

Applications

Packages

Driver packages

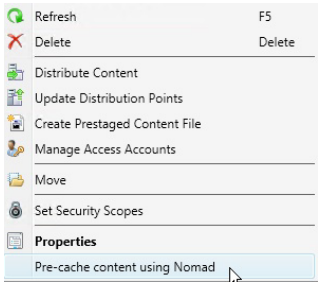
Operating system images

Operating system upgrade packages

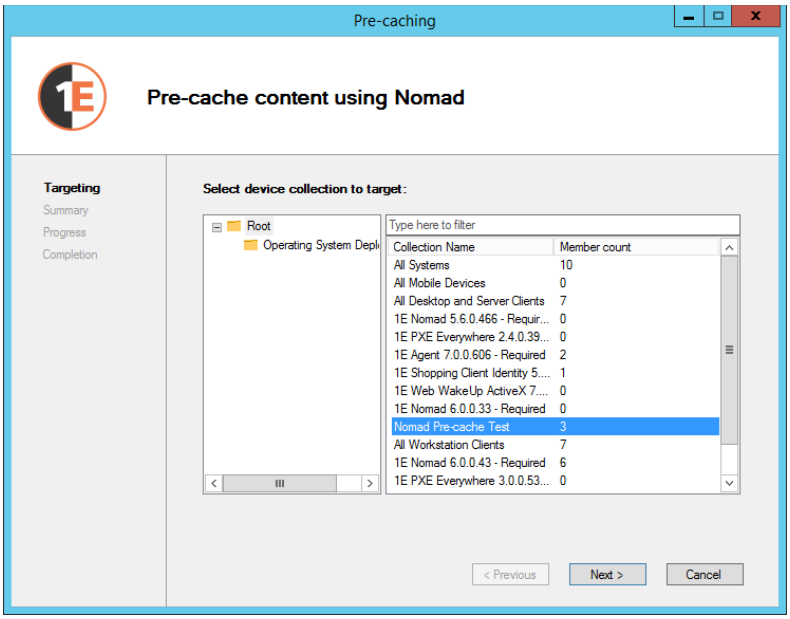
Boot images

Task sequences.

For task sequences, please refer to the note in the table under Dynamic pre-caching below:



On the **Targeting** screen, choose the device collection you want to pre-cache.



On the **Summary** screen, verify your selection.

Click **Apply** if it is correct

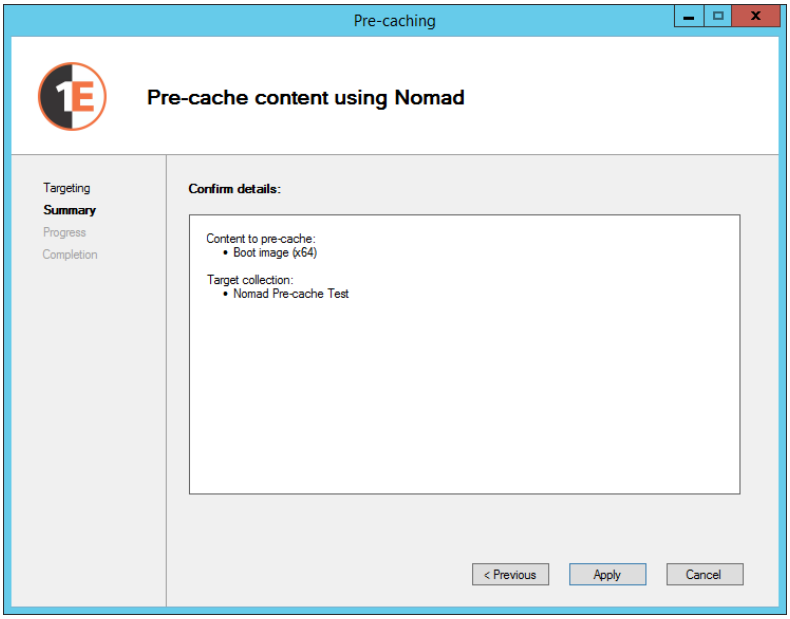
If it is incorrect, click **Previous** to start again.

The **Progress** screen displays the status while the wizard sets up the pre-cache notification in ContentDistribution.

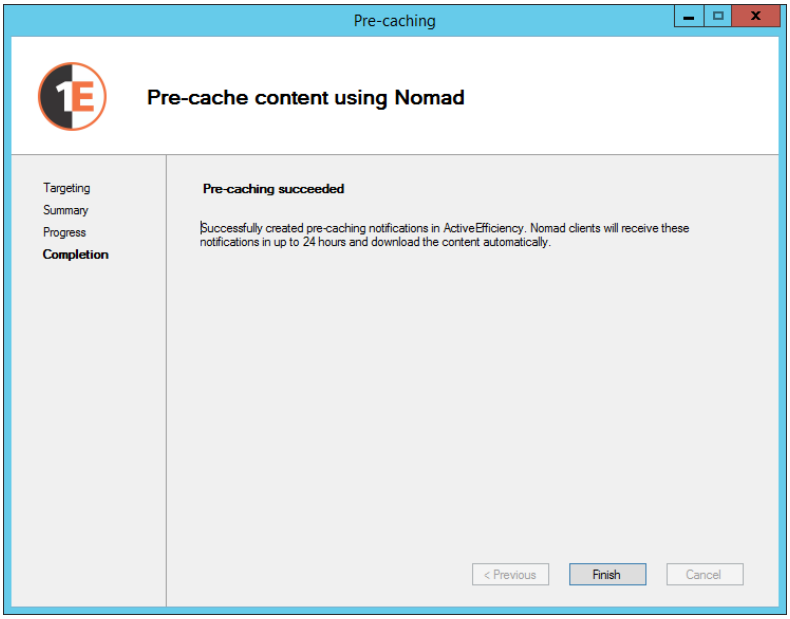
Note

From Nomad 8.1 there is support for providing alternate credentials to authenticate with the Tachyon Platform. If your Tachyon Platform instance resides in another

domain or the cloud, you will be prompted to enter alternate credentials for that location, which get stored in the credential store for any future requests.



On the **Completion** screen, click **Finish** to close the wizard.



9.4.2.3.3.1 Viewing pre-cached jobs

If you are not a full administrator, you can only view pre-cached jobs provided you have Read permissions on the collection as well as the content.

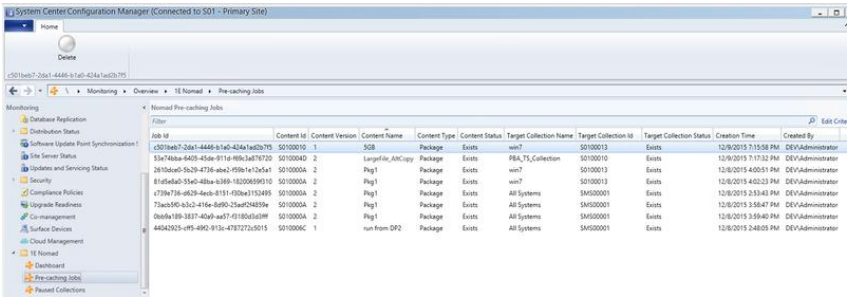
To view pre-cached jobs:

In Configuration Manager, choose **Monitoring**.

Expand the **1E Nomad** node and select **Pre-caching Jobs**.

The attributes for the job are displayed in the right-hand pane as follows:

Column title	Attribute definition
Job Id	The ContentDistribution identifier of the job.
Content Id	Configuration Manager identifier for the content referenced by the job.
Content Name	Name of the content referenced by the job.
Content Version	Version of the content referenced by the job.
Content Type	Type of the content referenced by the job (i.e. application, task sequence).
Target Collection Id	Device collection identifier targeted by the job.
Target Collection Name	Device collection name targeted by the jobs.
Creation Time	The time the job was created.
Created By	The person who created the job.
Content Status	(Visible only to those with full administrator rights) – displays the status of the content, i.e whether it exists or is deleted.
Target Collection Status	(Visible only to those with full administrator rights) – status of the device collection, i.e. whether it exists or is deleted.



9.4.2.3.3.2 Deleting pre-cached jobs

You can only delete pre-cached jobs if you have permissions for a particular content type. If you are not a full administrator, you will need:

Read permissions on collections (through a security role)

Access to the pre-cached job (i.e. content and the device collection)

To delete a pre-cached job:

In Configuration Manager, choose Monitoring.

Expand the Overview tree and choose Nomad Pre-cache jobs.

In the Nomad Pre-caching jobs list, right-click the pre-cached you want and from the context menu, choose Delete.

9.4.2.3.3.3 Managing pre-cached jobs with Powershell cmdlets

You can also manage pre-cached jobs by using PowerShell cmdlets.

To get all pre-cached jobs from ContentDistribution, run:

Get-PreCachingJobs [-PlatformURL <String>] [<CommonParameters>]

To remove pre-cached jobs from ContentDistribution run:

Remove-PreCachingJobs [-Id] <String> [-PlatformURL <String>] [-Confirm [<SwitchParameter>]] [<CommonParameters>]

Remove-PreCachingJobs -Before <String> [-PlatformURL <String>] [-Confirm [<SwitchParameter>]] [<CommonParameters>]

Remove-PreCachingJobs -AgeInDays <UInt32> [-PlatformURL <String>] [-Confirm [<SwitchParameter>]] [<CommonParameters>]

Remove-PreCachingJobs -All [<SwitchParameter>] [-PlatformURL <String>] [-Confirm [<SwitchParameter>]] [<CommonParameters>]

The parameters are:

Parameter	Optionality	Notes
-Id	Mandatory	ID for the job to delete.
-PlatformURL <string>	Optional	Location of ContentDistribution. If not provided, it is retrieved from the *NomadAdminUI* registry value.
-Confirm	Optional	Suppresses the confirmation prompt for the deletion.
-Before	Mandatory	Delete jobs before a particular date and time where the notation is *yyyyMMddHHmmss*.
-AgeInDays	Mandatory	Delete jobs older than a particular number of days.
-All	Mandatory	Delete all jobs. Exercise caution if you use this.

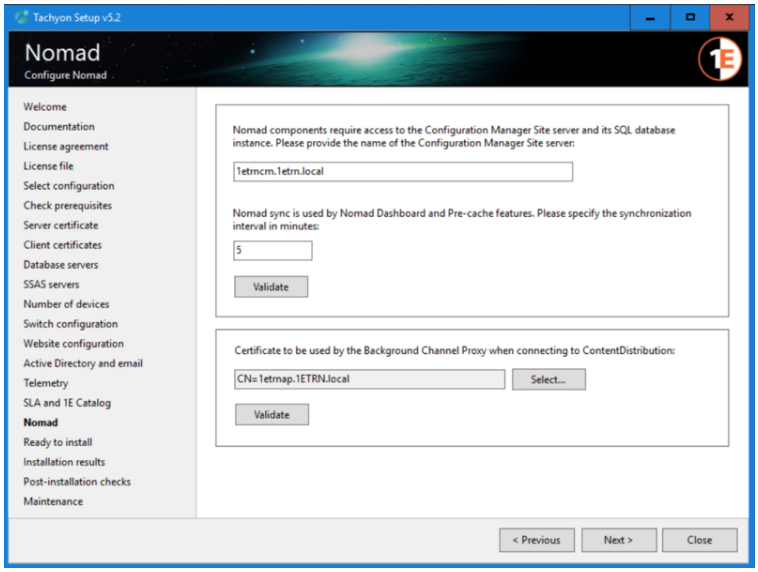
Parameter	Optionality	Notes
<CommonParameters>		Values are: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer, PipelineVariable and OutVariable

There is more information about *CommonParameters* at http://go.microsoft.com/fwlink/?LinkID=113216

9.4.2.3.3.4 Dynamic pre-caching

If the content or membership of a targeted collection changes after a pre-cached job is created, Nomad is updated to keep in sync with Configuration Manager. It does this by polling the Configuration Manager database at regular intervals to fetch updated content.

These intervals (you would have defined the intervals when you installed Tachyon Platform) have the following characteristics:



The range for the interval is between 5 minutes and 1440 minutes (1 day). By default, Nomad synchronizes with the Configuration Database every 30 minutes. If the values are outside the range, for example if the interval is less than 5, it will default to the minimum which is 5 minutes. Similarly, if the interval is greater than 1440, it defaults to the maximum which is 1440 minutes.

If a synchronization fails, it is rescheduled to run again in 15 minutes

Each synchronization task fetches the following:

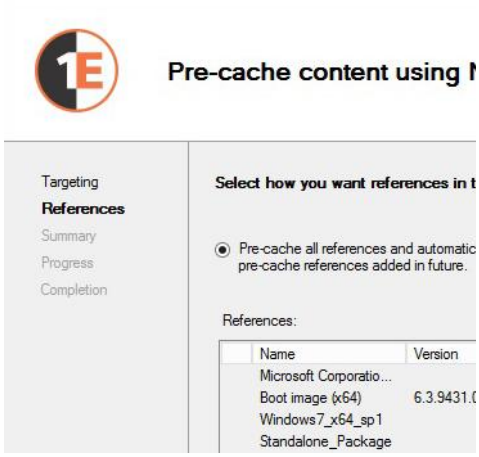
Pre-caching data (device collections and contents)

Dashboard data (status messages).

Pre-cached jobs are affected when these events take place in Configuration Manager, and on the next synchronization with Nomad:

Configuration Manager events	Next Nomad synchronization cycle	
Device collections	Where there is a change in membership for a device collection Where a device collection is deleted.	Nomad collection is updated to reflect the change in membership for that device Nomad pre-cached jobs for that device collection is deleted.
Packages	Where a package is updated Where a package is deleted.	Nomad is updated with the packages Nomad pre-cached jobs for that package as well as any pre-cached jobs referenced in a task sequence is deleted.
Applications	where deployment types are added or removed where an application is deleted.	Nomad deployment types for that application is updated Nomad pre-cached jobs for that package as well as any pre-cached job referenced in a task sequence is deleted.
Task sequences	If you chose to automatically pre-cache references (as well as those added later)	Nomad is updated: when references are added or removed when referenced content is updated or deleted when a reference is deleted

Configuration Manager events	Next Nomad synchronization cycle	

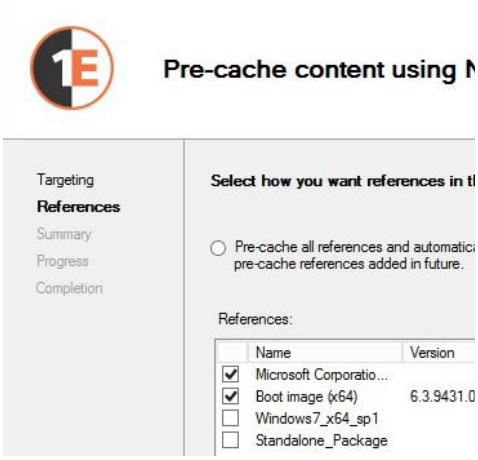


Note

Applications and packages that will be installed using a **dynamic variable list** will not be automatically pre-cached.

Also be aware that any other dynamic content will not be pre-cached, for example drivers deployed using Modern Driver Management (http://www.scconfigmgr.com/modern-driver-management/).

Dynamic content needs to be pre-cached independently as

Configuration Manager events	Next Nomad synchronization cycle
	separate jobs.
If you chose to selectively pre-cache references:	Nomad is not updated when references are added or removed
	Nomad is updated when referenced content is updated or deleted Nomad is not updated when a reference is deleted.

9.4.2.3.3.5 Manually forcing a synchronization between Content Distribution and Configuration Manager

You can force a synchronization to occur outside its normal cycle to assist in troubleshooting or just to speed up the sync process.

Navigate to https://<Platform_URL>/contentdistribution/v1.0/commands/cmsync

You should then see the response: *Initiated Cm Sync*

Check C:\ProgramData\1E\ContentDistribution\ContentDistribution.log for details.

> **Note**
>
> By default, all synchronization activities are logged in the ContentDistribution service log C:\ProgramData\1E\ContentDistribution\ContentDistribution.log.

9.4.2.3.3.6 Disabling synchronization

There may be instances, such as carrying out maintenance on the Configuration Manager server or the SQL Server instance, where you have to disable synchronization. To do this:

Open appsettings.json located in the service installation folder, typically in C:\Program Files\1E\ContentDistribution\Web\WebService

Set *Enabled* to *false* under the *CmSync* element, for example:

```
"CmSync": {
     "Enabled": false,
     "IntervalMinutes": "30",
```

```
        "TimeoutMinutes": 10,
        "CmServer": "1etrncm.1etrn.local"
    }
```

9.4.2.3.4 Hash validation

Hash validation is used when content is downloaded for pre-cached jobs and for LSZgen requests for these jobs. When a pre-cached job is created:

For task sequences, hashes for all referenced packages and applications are posted to Content Distribution

For applications, hashes for all its child deployment types are posted to Content Distribution.

On the client side:

Where a job is queued, the client queries the management point for content locations. The management point returns a hash for application content types only. If it does not return a hash, the client retrieves it from Content Distribution. Hashes from management points take priority over Content Distribution.

For the Tachyon server hosting Content Distribution, the client fetches the hash during the pre-cache cycle for that particular content.

9.4.2.3.5 Nomad clients polling the ContentDistribution database

9.4.2.3.6

After running the wizard, Nomad clients that are registered with the ContentDistribution database, and that were included in the selected device collection, will get a pre-cache notification within 24 hours. This notification tells Nomad that it has to process a download job on the content to be cached. The default number of notifications a client processes in one pre-cache poll cycle is 20, but you can modify this by updating the PrecachePollBatchSize registry value.

9.4.2.3.6.1 When is polling disabled?

Nomad clients normally start their polling cycle when the service starts, with a random delay to minimize the possibility of multiple simultaneous polls from different clients. However, polling will not start if any of the following is true:

The Tachyon Platform URL is not set in the Nomad registry.

Nomad is running on a machine using the Win PE operating system.

The Configuration Manager client is not installed on the machine – in order to download pre-cached content, the Nomad service needs to contact the management point and this is only possible if the client is installed locally.

To explicitly turn polling off for a Nomad client set the PrecachePollMinutes registry value to 0.

9.4.2.3.7 Nomad pre-caching RBAC support

Nomad pre-caching is tightly integrated into Configuration Manager and honors the permissions and restrictions enforced by role-based access control (RBAC). The following rules are used to

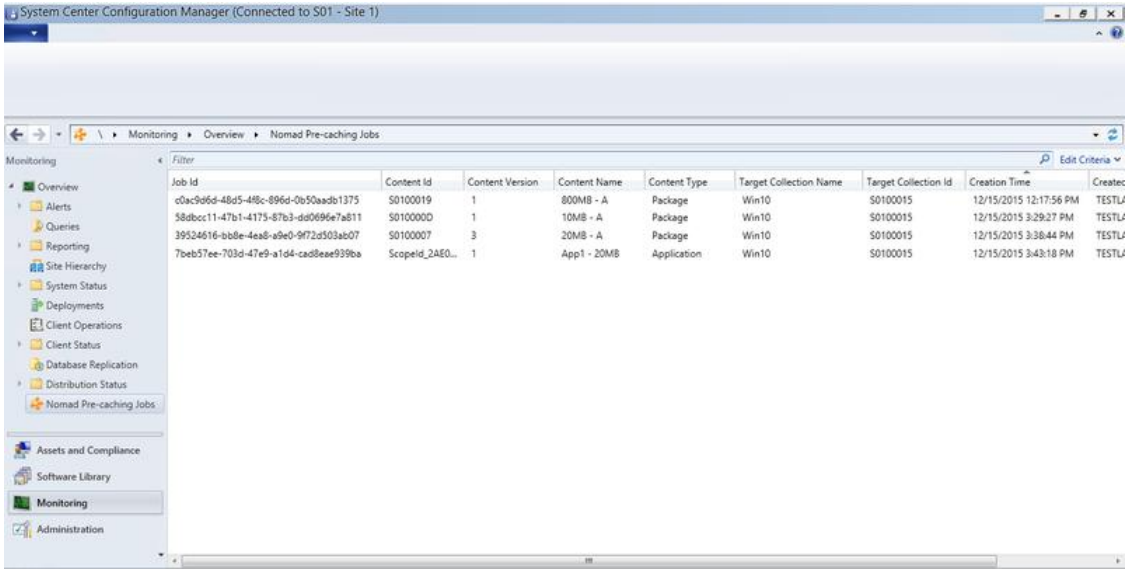
determine whether a particular user is allowed to pre-cache a particular content on a particular collection or not:

A user is only allowed to pre-cache a content item if they have the RBAC permissions to deploy it via Configuration Manager.

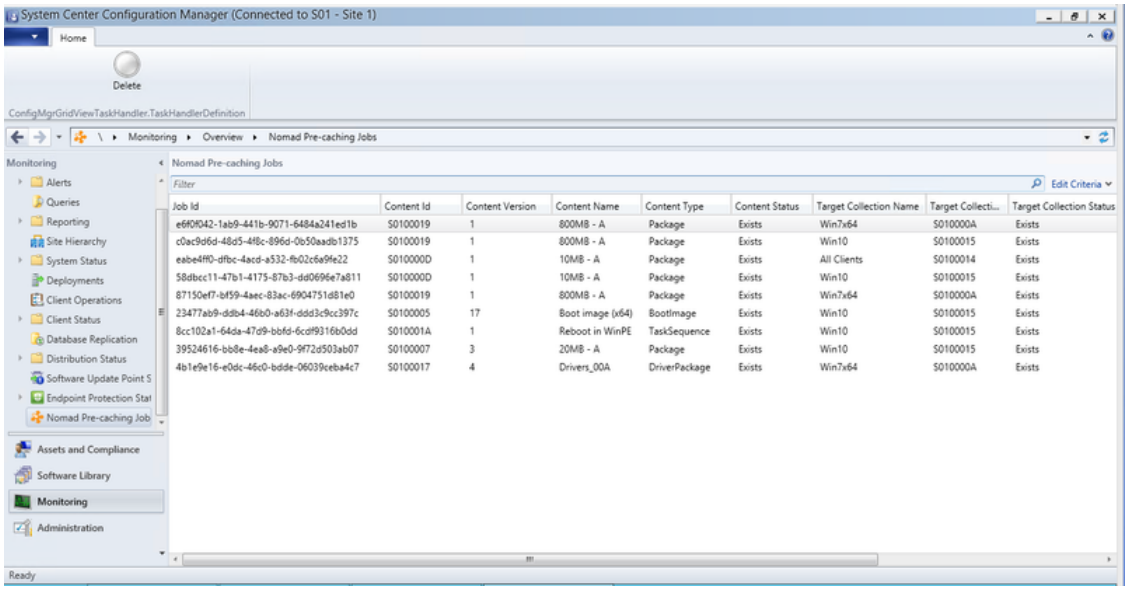
A user is only allowed to pre-cache to a device collection if they have the RBAC permissions to access that collection.

> **Note**
>
> Configuration Manager (CM) administrators will need to be a member of the Nomad Administrators group, so they can manage Configuration Manager collections, for example create, view and delete pre-cache and paused collections. Refer to Installing the Nomad app and 1E Content Distribution - Nomad roles and permissions for details.

If an administrator does not have the necessary RBAC permissions, they will not be able to see or access any of the Nomad pre-cache features in the Configuration Manager Admin console. Similarly, if they do not have the right permissions to a device collection, that collection will not be available to them in the Targeting screen of the pre-cache wizard.



However, full administrators will see:



The following table provides an overview of the availability of Nomad pre-caching for the built-in Configuration Manager security roles:

Nomad pre-caching support based on the Configuration Manager security role					
Built-in Configuration Manager Security Roles	**SOFTWARE LIBRARY**				
APPLICATION MANAGEMENT	**Operating System**				
Applications	**Packages**	**Driver Packages**	**Operating System Images**	**Boot Images**	**Task Sequences**
Nomad pre-caching Wizard					
Application Administrator	Pre-caching available (Access to Collection required)	Not available			

Application Author	Pre-caching Not available (Access to Application Management only)	Not available
Application Deployment Manager	Pre-caching available (Access to Collection required)	Not available
Asset Manager	No access to Software Library	
Company Resource Access Manager		
Compliance Settings Manager	Pre-caching Not Applicable for Software Updates (No Access to Application Management & Operating System, Only	

	Software Updates under Software Library available)	
Endpoint Protection Manager	No Access to Software Library	
Full Administrator	Pre-caching available (Access to Collection required)	
Infrastructure Administrator	Pre-caching not available (Access only to Windows Sideloading Keys in Application Management under Software Library)	
Operating System Deployment Manager	Pre-caching not available	Pre-caching available (access to Collection required)

Note

		If Package/ Application is part of a task sequence, pre-caching does not happen
Operations Administrator	Pre-caching available (Access to Collection required)	
Read-only Analyst	Pre-caching not available (Configuration Manager console is in Read-Only mode)	
Remote Tools Operator	No access to	

	Software Library
Security Administrator	
Software Update Manager	Pre-caching not applicable for Software Updates (No access to Application Management & Operating System, Only Software Updates under Software Library available)

9.4.2.3.7.1 Limitations

The following limitations are part of the current implementation of the Nomad pre-caching feature:

Software Updates are not supported by Nomad Pre-caching. Instead, make use of the available and mandatory advertisement dates.

Disabling Nomad Content Registration with the ContentDistribution database prevents Nomad clients from fetching further pre-caching notifications after the first batch of 20.

The Nomad Pre-caching Wizard allows packages that do not have content to be selected for pre-caching.

Delays may be seen when processing Pre-caching notifications for devices with many notifications. By default, Nomad clients will poll the ContentDistribution database once a day. Each time a client polls it will fetch a batch of 20 notifications to process, so for a client with 100 outstanding pre-caching notifications, it will take 5 days for all the notifications to be processed. The time between polls depends on the PrecachePollMinutes setting which can be reduced if there are many pre-caching jobs, though the 24-hour default is recommended.

Pre-caching jobs do not support Nomad *additional settings* (such as those configurable in the Nomad tab in the Package or Task Sequence properties).

Nomad won't re-download a pre-caching job with updated data format (that is compressed/encrypted), if the content has previously downloaded to the cache. The conversion will happen when ACP triggers the same content.

Nomad synchronization may cause issues if there is any replication issues between the central administration site and primary site.

Workgroup member clients may not be able to use the Nomad Pre-Caching feature, as it requires ContentDistribution registration using their FQDN.

9.4.2.3.8 Using network access accounts

Prior to this release, when a download is initiated, Nomad only used the credentials from the first Configuration Manager network access account it found to authenticate, and if that failed, the download stopped. From this release, Nomad cycles through all native Configuration Manager network access accounts to authenticate, thereby reducing the risk of failure.

> **Note**
>
> Nomad won't use network access accounts for SMB downloads from Distribution share. It uses the **SYSTEM$**account to connect to the package share location.

9.4.2.4 Nomad cache

An overview of the Nomad cache including different methods used by Nomad peers to access the cache on the elected master. The Nomad cache is essential to Nomad's download once to branch feature. The cache enables Nomad to hold its downloaded content so that it can be distributed locally to other Nomad peers. The Nomad cache contains downloaded content (such as packages, applications, and software updates) which can vary in size from relative small patches to rather large OS image files.

Nomad cache is used in a number of deployment scenarios, for example scenarios and how you can monitor those deployments using the Nomad app refer to:

Deploying software with Configuration Manager

Deploying software in large networks

Deploying updates for Office 365

Using Nomad with Operating System Deployment OSD.

9.4.2.4.1 Hard links

Nomad uses file system hard links between the Nomad and Configuration Manager client caches, ensuring that only a single copy of the content is retained. The use of hard links can be disabled using the NoHardlink setting.

Hard links are used for all content types except

Office 365 Updates, as this type of content is retained in the **Office 365 Click To Run** agent installation folder rather than the CCM cache folder

Content downloaded from Cloud Distribution Points

A hard link is the file system representation of a file by which more than one path references a single file in the same volume. Nomad uses this technique when making files in its cache available to the Configuration Manager cache if both of them are on the same volume and hard linking is not disabled. Both caches will hold the files but only uses one footprint on the physical volume. The Nomad cache is defined in the LocalCachePath registry value which is set during installation using the CACHEPATH installer property. If these caches are on different volumes, or hard linking is disabled, then Nomad copies content to the Configuration Manager cache.

Irrespective of whether hard linking is used or not, the following applies:

The Configuration Manager client and Nomad Branch each independently manages the content in their respective cache folders

When Nomad removes content from its cache as part of cache management, it also removes the same content from the Configuration Manager cache

When Configuration Manager removes content from its cache, content in the Nomad cache is not purged

Content downloaded directly by the Configuration Manager client (outside of Nomad) is not hard linked or copied to the Nomad cache

If the Configuration Manager client does not have sufficient space in its cache, it will not request a Nomad download.

9.4.2.4.2 Peer access methods

Nomad uses peer-to-peer connections to enable Nomad peers to access the Nomad master's cache. Nomad can share content with peers either through a file share (using Windows File and Printer Sharing Services) over SMB, or through an HTTP web service implemented in the Nomad client. Nomad also supports a 'connectionless' option for sharing content over UDP, but this should only be used as a last resort if SMB or HTTP/S are not viable in your environment.

Due to the complexity of network environments, Nomad provides some low-level control over the way the P2P communications are handled to help overcome certain scenarios that may arise. Specifically Nomad has a number of peer-to-peer connection related enhancements that enable it to work where:

File and Print Sharing Services are disabled

The connections may switch between wired and wireless communications

A multi-forest environment where peer computers from different forests may co-exist in the same subnet and are unable to access the Nomad master share using its hostname alone

Large files are being transferred.

9.4.2.4.2.1 HTTP/S

Nomad can be configured to use HTTP or HTTPS for all P2P sharing – thereby eliminating Nomad's dependency on SMB and **File and Printer Sharing Services**. Nomad also supports certificate-based client authentication, which eliminates the local SMSNomadP2P& account previously required for clients to authenticate with the elected master.

This is the recommended method of peer sharing content.

Note

For more detail please refer to Peer copy over HTTP or HTTPS.

9.4.2.4.2.2 SMB and File and Printer Sharing Services

This is the original and default method for Nomad peer sharing, which uses SMB and requires **File and Printer Sharing Services**.

Note

For more detail please refer to The Nomad share.

9.4.2.4.2.3 Connectionless P2P

Nomad can be configured to bypass these services and use the connectionless transfer protocol over the **User Datagram Protocol (UDP)** instead. Connectionless P2P does not use authentication and is approximately five times slower than SMB. This transfer method is only recommended for environments where other methods are not available.

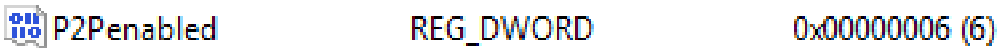
To enable Connectionless P2P update the Nomad P2Penabled registry value on all Nomad clients to:

0x0000 – P2P disabled

0x0002 – Enable connectionless P2P server

0x0004 – Enable connectionless P2P client.

In most cases both **P2P server** and **P2P client** should be enabled, by setting 0x0006 (decimal 6), as shown below:



9.4.2.4.3 Switching between wireless and wired network connections

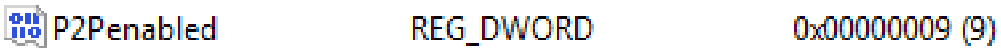
When network connections are switched between wireless and wired, Nomad may encounter problems accessing the share. Problems are likely to occur if DHCP uses a short lease time and the DNS does not reflect these changes quick enough. To mitigate these issues, Nomad has support for net literal names (IP addresses) for identifying its shares. Nomad clients normally use the elected master's hostname to connect to the NomadSHR in order to download the LSZ, LST and package files.

To configure Nomad to use net literal names (IP addresses) when connecting to peer shares, update the P2Penabled registry value to include:

0x0001 – P2P enabled

0x0008 – Enable use of net literal names (IP addresses).

For example, P2P enabled (0x1) plus enable use of net literal names (0x8), by setting 0x0009 (decimal 9), as shown below:



9.4.2.4.4 Multi-forest environments

By default, Nomad clients use the master's hostname to connect to the master in order to retrieve the package and signature files.

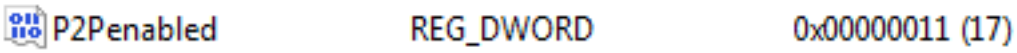
In a multi-forest environment computers from different forests may be present in the same subnet as the peers and are not able to connect to the master using just the hostname. In this scenario, Nomad should be configured to use FQDN for peer-to-peer connections. For this to work, it is necessary that the reverse lookup for IP addresses is correctly configured and running. If this is not available, Nomad reverts to using the IP address for its connection to P2P shares.

To configure Nomad to use FQDN when connecting to peer shares, update the P2PEnabled registry value to include:

0x0001 – P2P enabled

0x0010 – Enable use of FQDN name.

For example P2P enabled (0x1) plus enable use of FQDN (0x10), by setting 0x0011 (decimal 17), as shown below:



9.4.2.4.5 Cache management

The downloaded content in the Nomad cache consume disk space, therefore management of the cache is critical. Because files may be re-used and distributed to other devices on the same subnet or site, the simple solution of deleting the files as soon as they have finished downloading and executing is not sufficient. Instead, Nomad has a cache cleaner utility that automatically but intelligently maintains control over the cache's disk usage.

Nomad cache is used in a number of deployment scenarios, for example scenarios and how you can monitor those deployments using the Nomad app refer to:

Deploying software with Configuration Manager

Deploying software in large networks

Deploying updates for Office 365

Using Nomad with Operating System Deployment OSD.

9.4.2.4.5.1 Cache clean cycle versus CacheCleaner

There are two ways to clean the cache:

The cache clean cycle - which runs automatically on a cycle and clears the unused content from the cache as a preference (default off).

The CacheCleaner and its cache cleaner rules - which is either run by Nomad during an active download or manually from the command-line.

CacheCleaner can be run when required in addition to the automated cache clean cycle, for example when reserving space for new contents to be downloaded by manually running it from the command-line. CacheCleaner deletes content based on its priority and doesn't check its last usage date. So it is possible that content which is lower in priority but has been recently used, or is used regularly (like WIM files), may also get deleted when CacheCleaner runs. This mechanism therefore acts more as an emergency option to free up disk space but may result in the deletion of content that is likely to be used (which must then be downloaded again when needed). The cache clean cycle helps to maintain the low profile of the Nomad cache by removing content that is less likely to be used.

Both cache clean cycle and CacheCleaner methods are described in detail in:

Cleaning the cache using the cache clean cycle

Cleaning the cache using CacheCleaner.

9.4.2.4.5.2 Cleaning the cache using the cache clean cycle

The automated cache clean cycle runs automatically on a regular configurable interval. Nomad was designed to cache content that Configuration Manager has requested or that has been pre-cached using Content Distribution. Because of this the content accumulated in the Nomad Cache can become quite extensive, with a large degree of it no longer relevant or useful. For example, a Windows software update which has been superseded by a newer update is no longer relevant or useful and can be safely removed. The cache clean cycle helps to manage the Nomad cache, remove aged and irrelevant content and minimize its impact on the host machine.

The cache clean cycle is turned off by default, so the registry entries must be set before it will start to regularly clean the cache.

9.4.2.4.5.2.1 Configuration options

This option is configured by setting the following registry values or installer properties:

Registry Value	Default Value	Installer Property	Description
CacheCleanCycleHrs	0 (turned off)	CACHECLEANCYCLEHRS	The first automatic cache clean runs randomly between 10 to 60 mins of service start up. Subsequent

Registry Value	Default Value	Installer Property	Description
			cache clean cycles run after the number of hours specified. 0 means feature turned off. No cache cleaning cycle would run. Changing this registry entry performs an internal restart. The minimum value is 4. The maximum value is 168 (Once a week)
CacheCleanSubnetLookup	1 (turned on)	CACHECLEANSUBNETLOOKUP	Before deleting content, Nomad checks if it is on any other client in the same subnet, and will only delete local content if the same is present on at least one other client on the same subnet. To disable subnet lookup, set the value to 0. Its value can be 0 or 1. The default value is 1, subnet lookup is enabled. New setting introduced in 8.0.
MaxCacheDays	0 (turned off)	MAXCACHEDAYS	Set to delete application or package content that last triggered Nomad elections before the specified number of days from the date the cache cleaner runs. This ensures that only application or package

Registry Value	Default Value	Installer Property	Description
			content that have triggered elections recently will be kept in the cache. 0 means that application and package content will not be deleted automatically when the cache cleaner runs.
MaxCacheDaysThreshold	0 (turned off)	MAXCACHEDAYSTHRESHOLD	This is the maximum number of days content is present on a client. If it's not zero, then content will be deleted without any other checks once it reaches the threshold. If the threshold has a value greater than zero and less than 30, Nomad uses the threshold of 30 days and creates an associated log. Default value is 0. New setting introduced in 8.0.
MaxPreCacheDays	0 (turned off)	MAXPRECACHEDAYS	Set to delete pre-cached content that last triggered Nomad elections before the specified number of days from the date the cache cleaner runs. This ensures that only pre-cached content that has triggered elections recently will be kept in the cache. 0 means that pre-cached content will not be deleted

Registry Value	Default Value	Installer Property	Description
			automatically when the cache cleaner runs.
MaxSUCacheDays	0 (turned off)	MAXSUCACHEDAYS	Set to delete software updates that last triggered Nomad elections before the specified number of days from the date the cache cleaner runs. This ensures that only software updates that have triggered elections recently will be kept in the cache. 0 means that software updates will not be deleted automatically when the cache cleaner runs.
DpCacheCleanupEnabled	0 (turned off)	DPCACHECLEANUPENABLED	Deletes all LSZ files in a Distribution Point (DP) cache whose content is no longer distributed, that is not present in ContentLib. To enable DP Cache Cleaner, set the value of registry to 1 (any value except for 0 enables this feature).

9.4.2.4.5.2.2 Cache clean cycle delete conditions

When the cache clean cycle runs, it will check the type of each content and the last election date associated with it. There are four main types of content, and these will be marked for deletion if the following delete conditions are true:

Content type	Delete condition
Pre-cached	last election date + MaxPreCacheDays > cache clean cycle run date
Application or package	last election date + MaxCacheDays > cache clean cycle run date
Office 365 update byte-range	last election date + MaxSUCacheDays > cache clean cycle run date
Software updates related to SMSTSNomad jobs	

The cache clean cycle will then also check the following, for all content other than Office 365 update byte-ranges:

The content should be present on at least one of the Nomad subnet peers with an equal or a higher percentage of content

The network has broadcasts enabled

If both of these conditions are also true, the content will be deleted.

9.4.2.4.5.2.3 Caveats

The following points describe various caveats related to the way that the cache clean cycle works:

If pre-cache content is deleted by the cache clean cycle, but the corresponding pre-caching job still exists, Content Distribution will send the download notification again to the client

> **Note**
>
> If your Nomad policy is to not delete pre-caching jobs, you should turn off deletion of pre-cached content by setting the MaxPreCacheDays registry value to 0.

Application upgrades and uninstallation via Software Center require content to be present on the machines (the current version is required for uninstallation and the previous version is required for upgrade scenarios). If the content has been deleted by the cache clean cycle, the content would be downloaded again at uninstall or upgrade time. Because of the way that the cache clean cycle delete conditions are applied Nomad retains one copy of the content per subnet, so even if such a download request comes the content would be downloaded from a Nomad peer and not a DP

ByteRange content is not checked to be present on subnet peers

Cache optimization does not work for content that is to be activated later on

Cache optimization does work on Sensitive Servers.

9.4.2.4.5.3 Cleaning the cache using CacheCleaner

To maintain the cache Nomad uses a set of basic rules that lets you decide the cache's effect on overall disk usage and performs automatic cleaning when necessary. When a job is advertised, automatic cache cleaning could occur under the following circumstances:

If the percentage of available disk space is less than the PercentAvailableDisk setting after downloading an incoming package, according to its download package size, automatic cache cleaning is initiated before the download takes place

Nomad then assesses how much space could be cleared by deleting cache folders that are eligible for deletion. A cache folder is deemed eligible for deletion if its cache priority value is lower than or equal to the cache priority value of the incoming package. The cache priority value is set on the Nomad command-line using the pc argument, or set in the Nomad properties page when using Configuration Manager. By default, if no value is specified, packages have a cache priority of 1

If the assessment determines there would still not be sufficient space available: no deletion will take place, the download is aborted and an error logged, which may be one of:

Insufficient disk or cache space available to download the Program...

Insufficient cache space available to achieve a Max Cache Size of X

If the assessment determines there would be sufficient space available in the cache: the folders are deleted in order according to their cache priority until the required disk space is available.

9.4.2.4.5.3.1 Cache cleaner and Configuration Manager

When Nomad is used with Configuration Manager the cache cleaner will also:

Purge linked contents from the Configuration Manager cache

Purge older versions from the Configuration Manager cache before downloading the content for a newer version.

The cache cleaner mechanism also works with the priority job control to ensure that suspended lower priority job caches are not cleaned to make way for the higher priority job unless absolutely necessary.

9.4.2.4.5.3.2 Command-line switches

CacheCleaner is an executable that can be used to explicitly purge the Nomad cache. By default, the Nomad cache is not purged unless there is an active download. In most cases, available disk space is not really an issue, but there may be circumstances where you may want to manage the cache to keep the disk usage overhead to a minimum. Please refer to Cache management for further information about managing the cache.

It is installed as part of Nomad and the format of the command-line is:

```
CacheCleaner.exe -switch
```

For a complete reference of Nomad command-line switches refer to Command-line switches.

Note

If the Nomad cache is deleted while another client is accessing it, the other client will recover by downloading directly from the DP. This is by design and ensures recovery occurs in order to complete a successful download.

9.4.2.4.5.3.3 CacheCleaner examples

In the following examples, there is no requirement to specify the path to CacheCleaner.exe because the path to Nomad executables is set in the PATH environment variable:

Example	Description
Set the cache cleaner to run as a Configuration Manager program.	You can set the cache cleaner to run as a Configuration Manager program and advertise it to all Nomad systems in a single operation. You can also schedule this as a regular housekeeping job, ensuring that the cache is kept under control automatically. To purge the cache when the total free disk space is at 20% run: `CacheCleaner.exe –PercentAvailableDisk=20`
Ensure that content in the cache is not kept for more than 30 day.	To ensure that content in the cache is not kept for more than 30 days, run: `CacheCleaner.exe –MaxCacheAge=30`
Delete a particular package and version.	To delete a particular package and version, run: `CacheCleaner.exe –DeletePkg=L0A00001 –PkgVer=1`
Purge the contents of a cache with a priority of 3 or lower.	To purge the contents of a cache with a priority of 3 or lower, run: `CacheCleaner.exe –DeleteAll -Force=3`
Purge the contents of a cache with a particular priority and size.	To purge the contents of a cache with a particular priority and size, run: `CacheCleaner.exe –PkgSize=10485760 –CachePriority=6`

9.4.2.4.6 Peer copy over HTTP or HTTPS

Nomad peer-to-peer content transfer uses SMB by default, which requires File and Print services to be enabled in order for it to share the content. For better security Nomad can be configured to use HTTP or HTTPS for peer-to-peer content transfer, removing the requirement for file shares. When Nomad is configured to use HTTP/S, if Peer Backup Assistant is enabled it will also use HTTP/S.

For some example deployment scenarios and how you can monitor those deployments using the Nomad app refer to:

Deploying software with Configuration Manager

Deploying software in large networks

Deploying updates for Office 365.

9.4.2.4.6.1 Enabling HTTP/HTTPS

Enabling HTTP/S for peer-to peer content transfer (including Peer Backup Assistant) is done by modifying the relevant bits of theP2PEnabled registry value as shown in the following table:

Bit	Hex	Decimal	P2P Protocol used
0	0x01	1	SMB
5	0x20	32	HTTP
6	0x40	64	HTTPS

Note

P2PEnabled is a numeric value where, when represented in binary, each bit represents a configurable option, The table above only shows the bits that are relevant to P2P protocol selection. These values can be combined with other P2P settings, refer to P2PEnabled for full details.

It is important to ensure all clients are configured to use the same protocol, as a mismatch in protocol will prevent Nomad peers copying content from the elected master. You can enable multiple protocols on a client - for example P2PEnabled = 0x61 enables the peer to connect to the elected master using either HTTPS, HTTP or SMB. In this scenario, the peer will attempt the most secure protocol (HTTPS) first, followed by HTTP and finally falling back to SMB if it is unable to connect using HTTPS or HTTP.

9.4.2.4.6.1.1 HTTP and HTTPS Ports

When you enable HTTP and/or HTTPS, by default Nomad will use port 5080 for HTTP and 5443 for HTTPS, If these ports are already in use in your environment, you can define custom port numbers using the following registry values,

Registry value	Default value	Notes
P2PHttpPort	5080	Default HTTP port to use for peer copy. If you are using a custom port, ensure that all Nomad clients use the same custom port.

Registry value	Default value	Notes
P2PHttpsPort	5443	Default HTTPS port to use for peer copy. If you are using a custom port, ensure that all Nomad clients use the same custom port.

9.4.2.4.6.2 Client authentication

Client authentication is required when Nomad peers connect to the elected master. Nomad supports two client authentication methods,Windows authentication and certificate-based authentication.

9.4.2.4.6.2.1 Windows authentication

By default, Nomad peers use the local SMSNomadP2P& account, which is created by Nomad on each client, to authenticate with the elected master (when the master is elected, it shares a key that enables them to determine the credentials for this local account on the master). This requires each client to allow their local SMSNomadP2P& account to access the computer from the network. Alternatively, Nomad peers can be configured to use their Computer Account to authenticate with the elected master using the SpecialNetShare setting. If the Computer Account is used, the Domain Computers group at a minimum must be configured to access the computer from the network on all clients.

By default, the elected Nomad master will allow connections from its own SMSNomadP2P& account and all authenticated Users (Authenticated users is required when using the peer's Computer Account to authenticate). You can restrict this further to just the SMSNomadP2P& account using the AuthenticatedUsers setting.

9.4.2.4.6.2.2 Certificate-based authentication

When Nomad is configured to use HTTPS for peer-to-peer content transfer, peers can use a PKI Client authentication certificate to authenticate with the elected master. This is more secure than Windows authentication as it does not require any local accounts to be granted 'Access this computer from the network' permissions. To enable certificate-based client authentication:

Configure clients to use HTTPS for peer-to-peer content transfer through the P2PEnabled client setting.

Ensure clients have enrolled a client authentication certificate from a PKI in the Local Computer Personal certificate store. (Self-signed certificates cannot be used for client authentication). If you are using Configuration Manager with HTTPS site systems, you should already have a suitable PKI client authentication certificate enrolled on all CM clients that Nomad can use for P2P client authentication.

Optionally (but recommended) configure CertIssuer client setting to assist Nomad in selecting the correct client authentication certificate if there are several in the Local Computer Personal certificate store

Configure P2PSslSettings to enable certificate-based client authentication. When this option is enabled, Nomad does not create the local SMSNomadP2P& account.

Warning

If you enable certificate-based authentication for peer-to-peer content transfer, you must ensure that a valid client authentication certificate is available at all times. If the certificate expires, Nomad will return ERROR_CLIENT_CERT_MISSING (0X209A). This error code has been added to the Nomad SuccessCodes default setting, which means that Nomad will fail the download job and CM will not fall back to BITS to download the content from the DP. Nomad will not be able to download any content until a valid certificate becomes available on the client.

If you have configured Nomad to use a PKI certificate for server or client authentication, when Nomad starts it will look for an appropriate certificate in the Local Computer Personal certificate store. In most cases Nomad will be able to select an appropriate certificate without any additional configuration. In some cases you may need to specifyCertIssuerand possiblyCertSubject.

9.4.2.4.6.2.2.1 Client authentication certificate selection

Nomad will select a client authentication certificate for peer-to-peer authenticationfrom the Local Computer Personal certificate store using the following criteria if:

If the first certificate is issued by one of the issuers specified in CertIssuer but the next certificate is not, then the first will be selected. If both match or do not match the CertIssuer, then the next step is evaluated.

If the first certificate has a subject specified in CertSubject but the next is not, then the first will be selected, otherwise the next step is evaluated.

If the first certificate has a subject specified as an FQDN and the second does not, the first will be selected, otherwise the next step is evaluated.

The certificate with the latest expiry will be chosen.

Nomad will select the first certificate that matches the above criteria. CertIssuer should only be required if the CM client is using a self-signed certificate for client authentication with CM site systems and there are certificates from multiple Certificate Authorities. When CertIssuer is defined, Nomad will select the first certificate issued by that CA that matches the other criteria.

Note

Nomad also requires a client authentication certificate for authenticating with CM HTTPS Site Systems. In most cases, it will use the same certificate for authentication with peers and CM site systems, which will typically be the PKI-issued CM client authentication certificate.

If for any reason a different certificate should be used for authentication with CM site systems, you can additionally specify CertSubject.

9.4.2.4.6.2.2.2 Caching of certificates

Once a certificate is selected using the above criteria, it is cached and is provided for any subsequent client certificate requests until the certificate is expired or no longer present in store. Once the certificate is expired or no longer present, another certificate is chosen by using the above selection criteria.

9.4.2.4.6.2.2.3 Exception

If the registry value "thumbprint" is specified under HKLM\Software\1E\NomadBranch\Platform then the certificate with this thumbprint will be chosen (if it is valid, if not then the above selection criteria is used) if the download URL is a background channel URL or if both registry values CertIssuer and CertSubject are not specified.

9.4.2.4.6.2.2.4 Missing or invalid client authentication certificate

If Nomad is unable to select a valid client authentication certificate for any reason (for example if no certificate present, or is expired, or the certificate is not from the specified issuer), then Nomad returns ERROR_CLIENT_CERT_MISSING(0x209A) for the download job. This error code is included in the default SuccessCodes, so if it occurs, Configuration Manager will not revert to downloading using BITS, thereby protecting the network from potential congestion.

In Windows PE, Nomad fails the job immediately.

In the full OS, Nomad retries every 10 minutes until a valid client certificate is available in the Local Computer Personal certificate store or timeout (defined by P2PClientCertWaitPeriodMins, 24 hours by default) occurs.

If a client certificate becomes available before timeout occurs, a new election is initiated and Nomad tries downloading the content again.

If no certificate becomes available within the timeout period, Nomad will fail the job.

During the timeout period, if the Nomad service is reset, the download job is paused or the system goes to sleep, Nomad will continue to wait for the timeout period to expire. Any other interruption (the for example, if Nomad service is stopped, or the download job is cancelled or expires) will cause the download job to fail with the appropriate error condition.

While the download job is waiting for a valid client certificate, Nomad will not process any other download jobs.

9.4.2.4.6.3 Server authentication

Server authentication is required when Nomad is configured to use HTTPS for peer-to-peer content transfer. In this scenario, Nomad binds a server authentication certificate to the HTTPS endpoint to secure the communication between the elected master and peers. This certificate can be generated either by Nomad (self-signed) or through a Public Key Infrastructure (PKI). Use the P2PSslSettings to configure Nomad to use either self-signed (default) or PKI certificate.

9.4.2.4.6.3.1 Server authentication certificate selection

Nomad will select a server authentication certificate in the Local Computer Personal certificate store using the following criteria

Store = MY (the default certificate store)

Usage = Server Authentication

Subject/DNS = Host name or FQDN

Valid (NotBefore is in the past) and not expired (NotAfter is in the future)

Issuer = CertIssuer (Optional).

In most cases, the built-in criteria are sufficient to determine a single applicable certificate. If multiple certificates are likely to match these criteria, you can optionally specify CertIssuer to limit the certificates that Nomad will consider to those issued by one or more specific Certificate Authorities. Note that CertIssuer also affects the selection of the Client Authentication certificate. If the server and client authentication certificates are issued by different Certificate Authorities, you can specify multiple CAs with CertIssuer, either using a sub-string that is common to the desired CA names, or a comma-separated list of CA names.

If multiple certificates match the criteria above, Nomad uses the following order of precedence when matching the Subject Name:

Hostname and FQDN

Hostname

FQDN

If a single certificate matching the criteria still cannot be resolved, the matching certificate with the longest validity is used.

Note

When using Net literal names (3rd bit in P2PEnabled is set), clients ignore mismatch in host names during the SSL handshake – this is because IP addresses are generally not included in certificates

When using self-signed certificates for server authentication, clients do not validate the certificate issuer since it is issued by *NomadBranch* and it is not a valid CA

Due to the nature of how proxy servers can be implemented, some of which can be quite complex, you may need to consult your networking specialist to see if exceptions need to be added to enable Nomad's peer-copy over HTTP or HTTPS.

9.4.2.4.6.4 Firewall exceptions

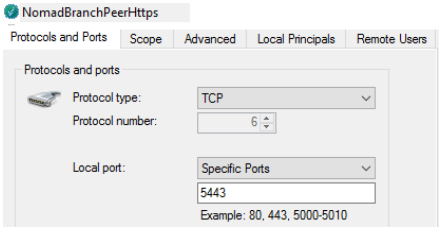
Depending on your preferences (protocols, ports) during installation, the installer will add the exceptions to Windows firewall.

Note

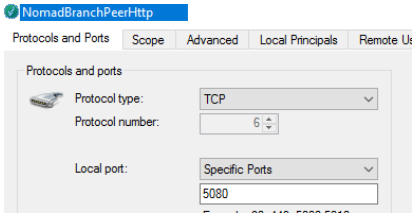
If for some reason these exceptions are removed post-installation, Nomad service will automatically re-add them. You'll just have to restart the service. Nomad service checks and fixes required firewall exceptions whenever it starts.

You can verify these in its Inbound Rules:

For HTTPS (port 5443)



For HTTP (port 5080)



Note

Firewall exceptions are added against the program "system" not NomadBranch.exe. This is because Nomad uses Windows HTTP Server API (https://docs.microsoft.com/en-us/windows/win32/http/http-api-start-page?redirectedfrom=MSDN)to create the HTTP server and under this API all requests are handled by Windows kernel's "system" program not by Nomad directly. In some third-party firewalls you may have to use the program name "ntoskrnl.exe", since "system" is actually an alias for ntoskrnl.exe.

9.4.2.4.6.5 Windows PE support

When running in Windows PE, Nomad can download content from peers over HTTP/S, but is not able to serve content to others (a Windows PE client will not be elected as a master). However, Nomad still needs to be configured correctly (port usage and certificate type) or it will not be able to connect peers.

9.4.2.4.6.5.1 Certificate-based P2P Client Authentication in Windows PE

When Nomad is configured to use certificate-based client authentication for peer-to-peer content transfer, to support running in Windows PE you will need to update the Windows PE boot image(s) to include a client authentication certificate in the Windows PE boot image (as Windows PE will not be able to enrol a Client Authentication certificate, typically done through Active Directory). If you are using 1E PXE Everywhere and have prepared boot images using UpdateBootImage with a PKI-issued client authentication certificate, no further action is required. If you are not using PXE Everywhere, or have prepared boot images using a CM self-signed certificate you will need to update your boot images to use a PKI-issued Client Authentication certificate.

If CM is using PKI-issued certificates for Client Authentication, you can use (export) the certificate that CM will have already prepared for use with boot images. If CM is using self-signed certificates, you will need to export a suitable PKI-issued Client Authentication certificate. In either case, you will need to export the appropriate certificate and provide the path to the exported certificate in the UpdateBootImage UI / command line. Even if you are not using PXE Everywhere, you can use the UpdateBootImage tool by installing just the PXE Everywhere Admin Tools on a device that has the CM console and Windows 10 ADK (version corresponding to the version of

Windows PE you are using for your boot images). You can download PXE Everywhere from the 1E Support Portal.

9.4.2.4.6.5.1.1 Certificate-based P2P Client Authentication in the full OS

When a Task Sequence reboots from WinPE into the full OS, Nomad will usually fail to find a certificate in the Microsoft certificate store. This is not an issue. Default logging level logs this fact, but does not show that Nomad successfully gets the BootImage certificate which the Task Sequence had previously stored in its variables list while in WinPE. Nomad uses this BootImage cert to authenticate with peers, and also with the Background Channel proxy to read data from Content Distribution if SSD is enabled and required. The log goes on to show the "Peer Connected OK" and gets the content.

Whilst Nomad Branch and 1E Client are separate services, Nomad depends on 1E Client to post events via the Tachyon Switch. However, the Client connection to the Switch depends on finding a certificate in the Microsoft certificate store, which does not exist, and 1E Client logs this error (not in the Nomad log). The 1E Client is unable to use the BootImage cert that Nomad uses. Inability to post events while the Task Sequence is running is not an issue, and any errors logged should not be of any concern. When the Task Sequence completes, your normal process of certificate enrollment will complete and the 1E Client will connect to the Switch and the backlog of Nomad events will be posted.

Whilst unnecessary, if you want Nomad events to be posted sooner in full OS, you can modify your Task Sequence to enrol a certificate into the Microsoft certificate store earlier. One method is to add a step to enable AutoEnrollment after 1E Client (and Nomad) is installed. For example, a Run command-line:

```
reg add HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Cryptography\AutoEnrollment /v AEPolicy /d 7 /t REG_DWORD /f /reg:64
```

9.4.2.4.6.5.2 Configuring Nomad to use HTTP/S in Windows PE

Nomad uses a custom Install and Configure Nomad in WinPE Task Sequence step to install Nomad after the Task Sequence has booted into Windows PE. The settings highlighted below are related to configuration for HTTP/S.

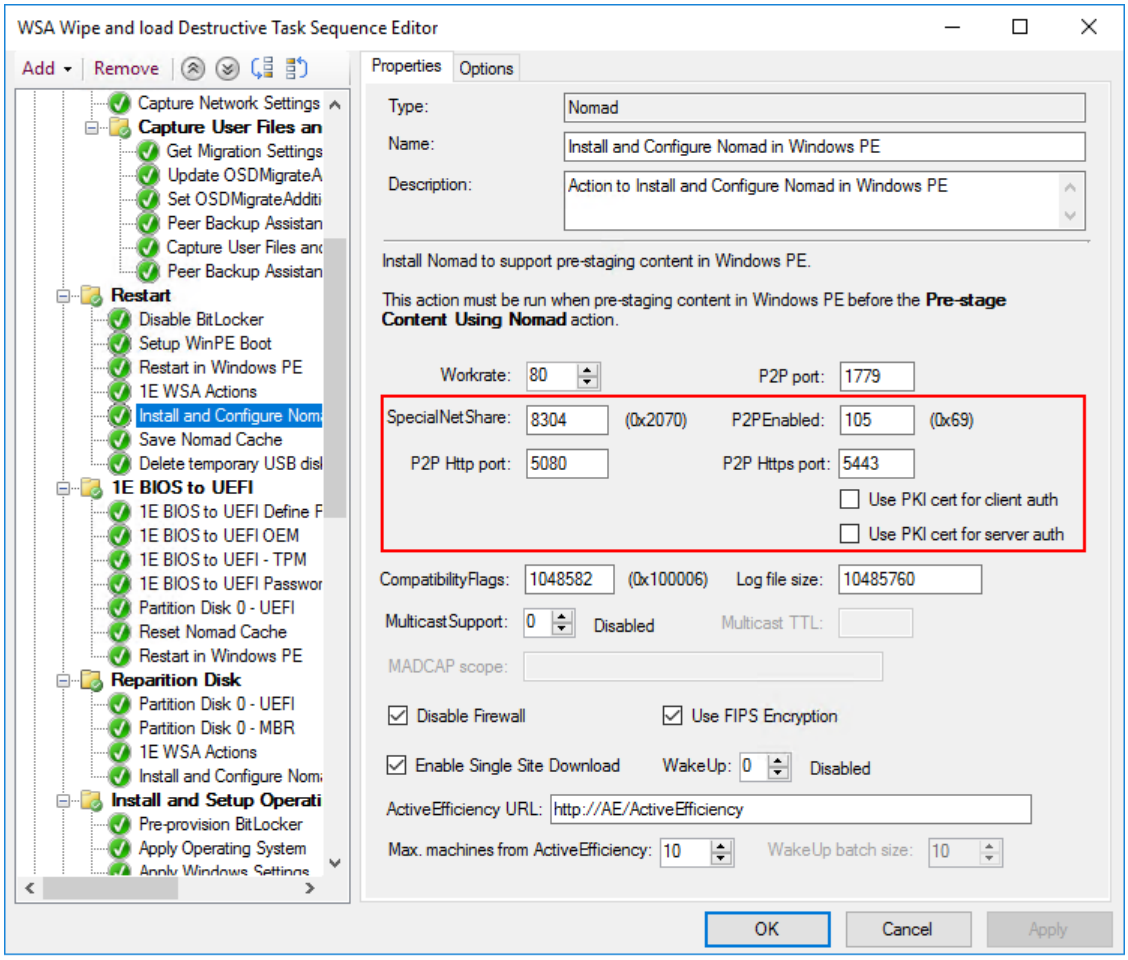
P2PEnabled must be set to include HTTP or HTTPS. By default, this is set to 0x9, which disables HTTP/S

P2PHttpPort is disabled unless HTTP is enabled (bit 0x20 set in P2PEnabled). It defines the port that is used for Nomad P2P communication over HTTP (default 5080)

P2PHttpsPort is disabled unless HTTPS is enabled (bit 0x40 set in P2PEnabled). It defines the port that is used for Nomad P2P communication over HTTPS (default 5443)

Use PKI cert for client auth enables certificate-based client authentication, which requires a PKI-issued certificate. Selecting this option sets bit 0x2 of P2PSslSettings

Use PKI cert for server auth configures Nomad to use a PKI certificate for server authentication when HTTPS P2P is enabled (bit 0x40 set in P2PEnabled). If this option is not checked and bit 0x40 in P2PEnabled is set, Nomad will use a self-signed certificate for server authentication.



9.4.2.4.6.6 Configuring use of PKI-issued certificates post-installation

If Nomad was originally installed to use HTTPS with self-signed certificates for server authentication and you want to switch to using PKI-issued certificates, do the following:

Deploy the certificate to all Nomad clients. Ensure that the certificate's usage is Server Authentication and the certificate Subject is the client's host name or FQDN.

Enable HTTPS (Bit 6 - 0x0040) in P2PEnabled.

Update CertIssuer with the name of the certificate authority.

P2PSslSettings set to 1 to enable PKI certificate for server authentication.

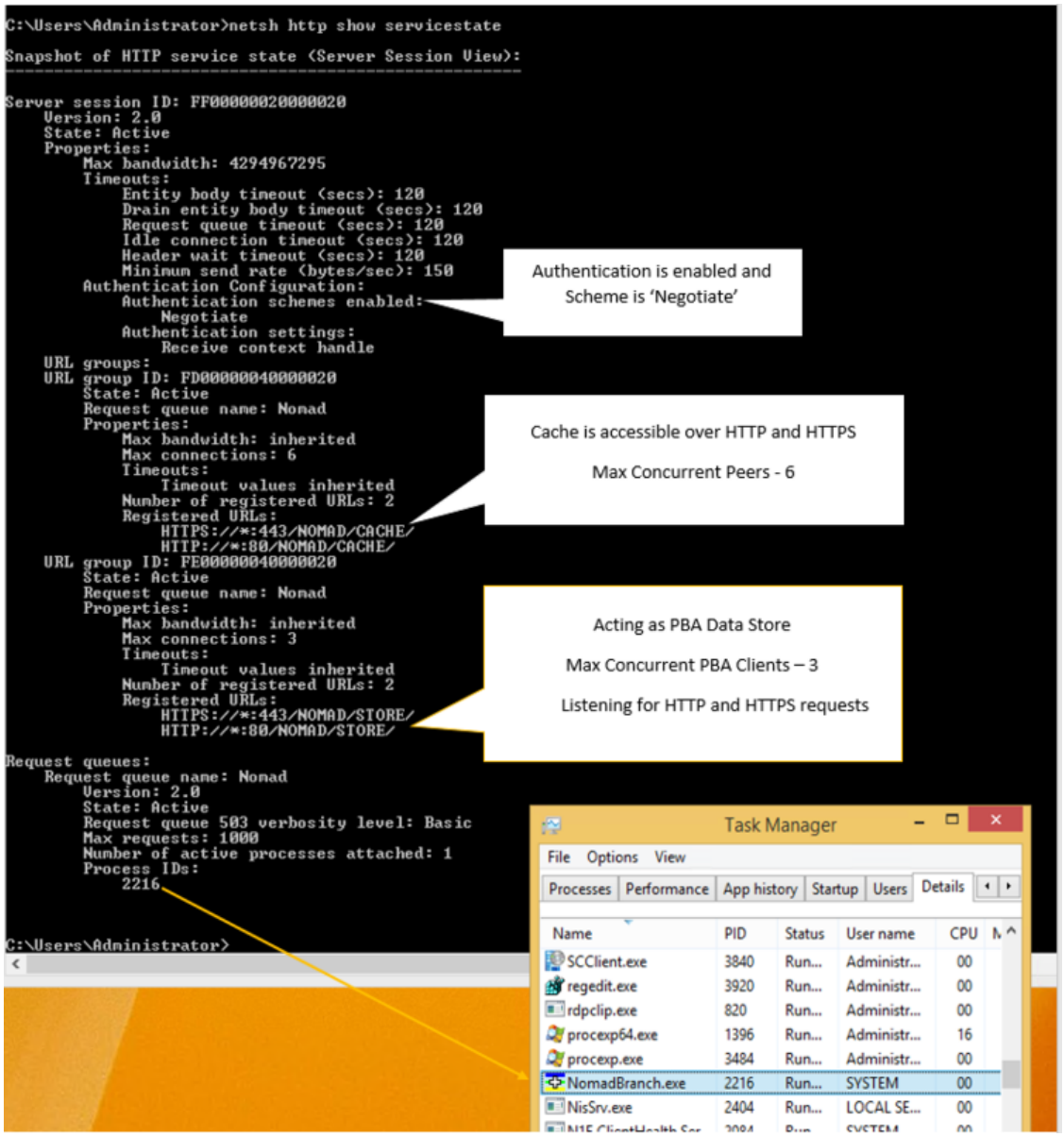
Restart the Nomad service.

9.4.2.4.6.7 Checking the status of your Nomad P2P HTTP server

To check the status of the P2P HTTP server, open the NomadBranch log. When the Nomad service starts, it logs a list of URLs it listens to, as shown in the example opposite.

1/25/2017 7:45:05 PM	Starting Http(P2P) Server
1/25/2017 7:45:05 PM	Http Initialized
1/25/2017 7:45:05 PM	Http Create Request Queue: 'Nomad'
1/25/2017 7:45:05 PM	listening for http requests on 'Http://*:5080/Nomad/Cache'
1/25/2017 7:45:05 PM	listening for http requests on 'Https://*:5443/Nomad/Cache'
1/25/2017 7:45:05 PM	listening for http requests on 'Http://*:5080/Nomad/Store'
1/25/2017 7:45:05 PM	listening for http requests on 'Https://*:5443/Nomad/Store'

Alternatively, run *NETSH* to check the status of the P2P HTTP server, as shown in the example opposite.

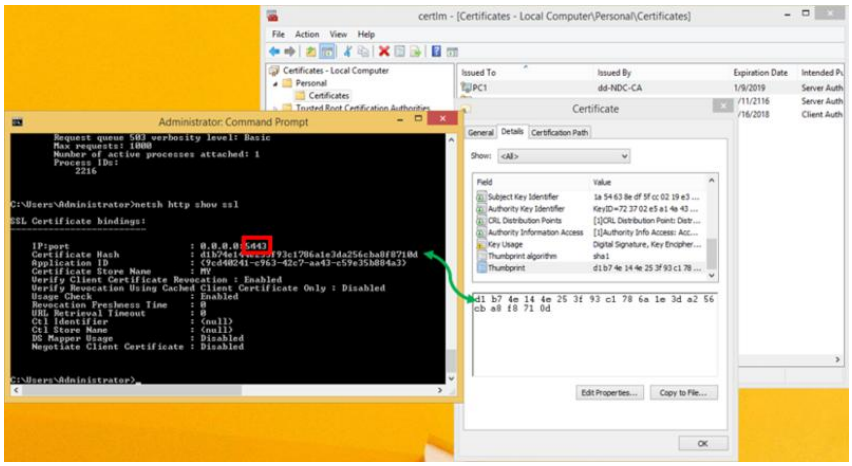


9.4.2.4.6.8 Checking SSL certificate bindings

To check the bindings of your SSL certificates, open the Nomad log. When the Nomad service starts, it logs the name of the certificate and its issuer, as shown in the example opposite.

```
1/27/2017 1:17:13 PM    Http Initialized
1/27/2017 1:17:13 PM    Http Create Request Queue: 'Nomad'
1/27/2017 1:17:13 PM    listening for http requests on 'Http://*:5080/Nomad/Cache'
1/27/2017 1:17:13 PM    listening for http requests on 'Https://*:5443/Nomad/Cache'
1/27/2017 1:17:13 PM    listening for http requests on 'Http://*:5080/Nomad/Store'
1/27/2017 1:17:13 PM    listening for http requests on 'Https://*:5443/Nomad/Store'
1/27/2017 1:17:13 PM    Software\1E\NomadBranch\P2PSslBindingId=""
1/27/2017 1:17:13 PM    Using Certificate (Issuer) NomadBranch "NomadBranch Authentication Certificate"
1/27/2017 1:17:13 PM    Set Software\1E\NomadBranch\P2PSslBindingId="36599882-0096-4e03-a4ff-fe7a5890196d"
1/27/2017 1:17:13 PM    Precache polling disabled. PlatformURL not set.
1/27/2017 1:17:13 PM    Nomad Http(P2P) Listener started
```

Alternatively, run *NETSH* to check the bindings for the certificates. In our example, the bindings for port 5443 are shown in the example opposite.

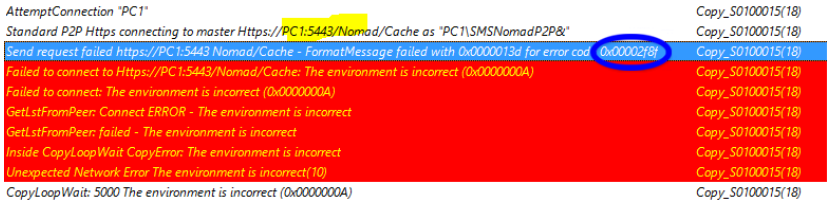


9.4.2.4.6.9 Troubleshooting failures during HTTP/HTTPS downloads

The most likely causes of HTTP/HTTPS download failures occur during a connection to a master. The most common errors are detailed below:

Error codes	Reason
0x00002efd 0x00004CF	HTTP/HTTPS is not enabled on the master or HTTP/HTTPS server on the master is listening on different port. In our example, the log illustrates that HTTPS had not been enabled on the PC1 master. *AttemptConnection "PC1"* — *Copy_S0100015(18)* *Standard P2P Https connecting to master Https://PC1:5443/Nomad/Cache as "PC1\SMSNomadP2P&"* — *Copy_S0100015(18)* *Send request failed https://PC1:5443 Nomad/Cache - FormatMessage failed with 0x0000013d for error cod 0x00002efd* — *Copy_S0100015(18)* *Failed to connect to Https://PC1:5443/Nomad/Cache: The network location cannot be reached (0x000004CF)* — *Copy_S0100015(18)* *Failed to connect: The network location cannot be reached (0x000004CF)* — *Copy_S0100015(18)* *GetLstFromPeer: Connect ERROR - The network location cannot be reached* — *Copy_S0100015(18)* *GetLstFromPeer: failed - The network location cannot be reached* — *Copy_S0100015(18)* *Inside CopyLoopWait CopyError: The network location cannot be reached* — *Copy_S0100015(18)* *Unexpected Network Error The network location cannot be reached(1231)* — *Copy_S0100015(18)* Possible solution: Double-check the values of P2PEnabled on both the client and remote peer - they should be the same.

Error codes	Reason
0x00002f8f	Invalid Certificate on master.
0x000000A	In our example, issues with certificates causes the download to fail with 0x00002f8f (security error) and the logging does not identify the cause of the failure.



Where errors like this occurs, check the following on master:

Expiry date

Subjects – should contain hostname or its FQDN

Issuer must be trusted via the trust chain on the peer machine

SSL Binding – ensure it exists for the HTTPS port.

9.4.2.4.7 The Nomad share

The Nomad cache is configured as a share that enables peer-to-peer distribution of downloaded content. Nomad provides control over the accounts that have access to the share and also provides an advanced Nomad FanOut mechanism that can overcome the connection limit to shares on workstations to ensure that content is distributed efficiently and securely.

> **Note**
>
> If Nomad is configured to use exclusively HTTP/HTTPS for peer copy, then the Nomad share is not created by the NomadBranch service.

For some example deployment scenarios and how you can monitor those deployments using the Nomad app refer to:

Deploying software with Configuration Manager

Deploying software in large networks

Deploying updates for Office 365.

9.4.2.4.7.1 Enhanced Nomad share security

Nomad leverages native Windows security to define which accounts have access to the Nomad share. In Nomad's default configuration, a Nomad share is created when the Nomad service is

started and removed when it is stopped. The default Nomad settings also grants both Authenticated Users and the *SMSNomadP2P&* Nomad share account read-only access to the share.

In early versions of Nomad, further restricted access to the Nomad share could only be done using custom share permissions. The major disadvantage to this approach was that the Nomad service no longer managed the Nomad share, and it had to be created and managed through other methods. So, if you wanted to exclude Authenticated Users from the Nomad Share permissions, you must take over the management of the share.

In Nomad, a cache access security option has been implemented that is controlled using the AuthenticatedUsers registry value. This optionally restricts access to the Nomad share to just the *SMSNomadP2P&* Nomad share account, thereby excluding Authenticated Users from the Nomad share permissions but still leaves Nomad in control of the creation, management and removal of its share.

9.4.2.4.7.2 Nomad Branch service and the Nomad share

The Nomad share is created each time the Nomad Branch service starts and removed when it stops. When the Nomad Branch service starts:

A share called *NomadSHR* for the Nomad cache folder is created. The share is removed when the Nomad Branch service stops. If this share is created on a workstation, only 6 concurrent users can access it. If the share is created on a server, there is no limitation.

A local user account called *SMSNomadP2P&* is created with its password attribute set to Password Never Expires. This account is not removed when the Nomad Branch service stops. The password for this account is changed each time the Nomad service restarts and is made up of 14 characters using a combination of upper and lower case alpha-numeric characters. This account is not a domain user and does not have the logon locally privilege. Account details are requested by peer clients during the master election process.

If the AuthenticatedUsers registry value is configured to use the built-in security principal Authenticated Users, the NTFS permissions on the Nomad cache folder are updated so that Authenticated Users is granted Read and Execute, List folder contents and Read permissions for the folder, its subfolder and files. These NTFS permissions are not removed when the Nomad Branch service stops.

Share Permissions for *NomadSHR* is configured as Read-only for the local *SMSNomadP2P&* user account and optionally a built-in security principal as specified by the AuthenticatedUsers registry value. The default is:

local user account *SMSNomadP2P&*

built-in security principal Authenticated Users.

The default location for the Nomad cache is `C:\ProgramData\1E\NomadBranch`. The MODULE.NOMAD.CACHEPATH installer property is also used to configure the location of the Nomad Cache, which is stored in the registry value LocalCachePath.

You can use the MODULE.NOMAD.SPECIALNETSHARE installer property or update the SpecialNetShare registry value so that Nomad hides the Nomad share. If you do this, the share will be renamed *NomadSHR$* and you will need to update all Nomad installations to use the hidden share.

Nomad can also be configured to use the machine account for peer connections instead of the local SMSNomadP2P& account by using the MODULE.NOMAD.SPECIALNETSHARE installer property or by updating the SpecialNetShare registry value. If the machine account is used, the local *SMSNomadP2P&* account is not

created. *Machine$* accounts in trusted domains are considered as Authenticated Users – the AuthenticatedUsers registry value must include Authenticated Users. Peer clients must be in trusted domains.

Use the MODULE.NOMAD.AUTHENTICATEDUSERS installer property or update the AuthenticatedUsers registry value to configure read-only access to the Nomad share for Authenticated Users (default), Everyone or neither in addition to the Nomad Share Account (SMSNomadP2P&). If Authenticated Users is selected, additional NTFS permissions are also configured for Authenticated Users on the Nomad cache folder.

The difference between Authenticated Users and Everyone depends on the OS version but in general Everyone includes Authenticated Users plus Guest.

Note

Domain controllers

When Nomad is installed on a domain controller (DC), it does not create the *SMSNomadP2P&* account and does not create the Nomad share. This is because it is not possible to create a local account on a DC. Nomad will not respond to elections and cannot be elected as a master.

If software is targeted at a DC, Nomad downloads the content from the distribution point (DP)

If the DC is also a DP, Nomad continues to process LsZ files and respond to Nomad clients as normal.

9.4.2.4.7.3 Custom share permissions

The SpecialNetShare registry values enables administrators to create their own share called *NomadSHR*, set the user limit and permissions. The Nomad cache is shared as *NomadSHR*, giving read access to the local Nomad share account and authenticated users. This enables new peer connections to be established and also allows access to the cache for computers with existing connections.

Share permissions can be configured on the share and requires the minimum read-only permission for

the local user account *SMSNomadP2P&* if not using the machine account

Built-in security principal Authenticated Users if using the machine account

NTFS security can also be set on the Nomad cache folder and requires these minimum permissions:

Built-in security principal SYSTEM requires Full control permission (because the Nomad Branch service uses the local system account)

Local group Users requires Read & execute, List folder contents and Read permissions

Local group Administrators requires Full control permission.

In addition, if using the built-in security principal Authenticated Users, as required when using the machine account, it requires NTFS security permissions Read & execute, List folder contents and Read.

9.4.2.5 Cloud Support

Nomad supports the following Configuration Manager (CM) on Azure scenarios:

Infrastructure as a Service (Iaas) - your host CM infrastructure servers are in Azure virtual machines

Cloud based Distribution Points - CM distribution points are hosted in Microsoft Azure as a cloud service

Cloud Management Gateway (CMG) - CM management points are hosted in the cloud, including support for CMG VM scale sets.

9.4.2.5.1 Infrastructure as a Service (IaaS)

Nomad 6.3 and later supports integration with Configuration Manager (CM) and Active Directory (AD) infrastructure servers in Azure virtual machines (Infrastructure as a Service). This is where CM and AD are being run in Azure, managing local clients network on organization's premises and this local network is connected to Azure using Microsoft Azure Site-to-Site Connectivity. Tachyon Platform may be hosted on a virtual machine hosted in the Azure cloud or locally on the on-premises network, with Nomad as usual installed on all client devices.

9.4.2.5.2 Cloud based Distribution Points

Configuration Manager (CM) now supports Distribution Points (DP) that are hosted in Microsoft Azure. The DP Site system role hosted on Windows Azure is referred to as a site system cloud service. The site system cloud service contrasts to a site system server, which refers to an on-premises computer that is managed in the local network environment. Nomad also support Cloud Management Gateway (CMG) for management point roles to manage CM clients on the Internet.

When a CM Client (ContentTransferManager) requests Nomad to download the content from a cloud based Distribution Point, Nomad performs the following tasks:

Downloads the encrypted content.

Decrypts the content before copying it to its own cache.

When the download is complete, Nomad encrypts the content and copies it to the CM cache.

Nomad peers looking for the original content in the subnet, perform an election for the decrypted content and then copy it from an elected master.

When the peer copy is complete, the peer Nomad encrypts the content and copies it to the CM cache.

> **Note**
>
> Unlike other content, for content downloaded from a cloud based Distribution Point, Nomad does not create hard links between the Nomad cache content and the CM cache, but the Nomad cache cleaner is able to delete the content from both the Nomad cache and the CM cache.

> **Note**
>
> Support is not yet available for Delta downloads, like Office 365 or Windows 10 software updates in Nomad. Microsoft does not recommend using distributing software update

content on Cloud Distribution Points, for more information refer to docs.microsoft.com/en-us/mem/configmgr/core/clients/manage/cmg/plan-cloud-management-gateway#content-storage.

9.4.2.5.2.1 Cloud based DP content and LSZ/LST file generation

Nomad content distribution relies on having access to an LSZ file that provides metadata regarding the download content. With on-premises Distribution Points, the LSZ file is normally generated by a local Nomad service. That option is not available for cloud based DP as they run as a service in Azure, and a Nomad service cannot be installed. Instead, the LSZ file is generated locally by mimicking the process used by CM agent, which queries the content's metadata from the DP directly.

Note

Be aware that:

Cloud based Distribution Points are not currently supported for Office 365 updates

RDC is not supported on cloud-based Distribution Points

If content is marked to be delivered as 1 (Compressed) or 2 (Encrypted) under Nomad SECure and needs to be downloaded to the client from a cloud based distribution point, these settings are ignored and content is downloaded in the original format. For the same reason, Ahead Of Time (AOT) LSZ generation is also not supported for cloud-based distribution points.

9.4.2.5.3 Cloud Management Gateway (CMG)

From Configuration Manager (CM) version 1610 and above, the cloud management gateway provides a simple way to manage CM clients on the Internet. The Cloud Management Gateway (CMG) service is deployed to Microsoft Azure and requires an Azure subscription. It connects to your on-premises CM infrastructure using a new role called the Cloud Management Gateway connector point. Once deployed and configured, clients will be able to access on-premises CM site system roles regardless of whether they're on the internal private network or on the Internet. Currently, CMG only supports management point and software update point roles, and Nomad has only been tested with management points.

When a client is on the Internet, the CM Client requests Nomad to download the content from a cloud based distribution point. Nomad gets the management point list (including cloud management gateway enabled Internet management points) from WMI and uses those to determine the appropriate distribution points. The rest works as usual.

9.4.2.5.4 Configuration Manager Enhanced HTTP Support

Enhanced HTTP is a feature implemented in Configuration Manager (CM) to enable administrators to secure client communication with site systems without the need for PKI server authentication certificates. Primarily this feature is used to support a Cloud Management Gateway (CMG) or to support Azure AD joined devices, both of which scenarios would otherwise require Management Points to be configured to use HTTPS with a PKI Server Authentication certificate.

Enhanced HTTP also allows clients to download content from a Distribution Point without the need for a Network Access Account, PKI client authentication certificates or Windows authentication as it establishes a new endpoint on the Distribution Point (CCMTOKENAUTH) that uses token-based access.

Refer to the Microsoft documentation for a full explanation of Enhanced HTTP and how to configure site systems to use it - https://docs.microsoft.com/en-us/mem/configmgr/core/plan-design/hierarchy/enhanced-http

9.4.2.5.4.1 Supported scenarios

Nomad supports downloading content from Distribution Points configured to use Enhanced HTTP without the need for a Network Access Account in the following scenarios.

> **Note**
>
> These scenarios assume the Management Point is configured to use HTTP (not HTTPS) as required for Enhanced HTTP.

9.4.2.5.4.1.1 Clients and site systems on the corporate network

Scenario	Clients supported	Notes
Configuration Manager Package, Application, Software Update and Task Sequence Deployments	Workgroup AD Domain-joined Azure AD-joined Hybrid-joined	When content is deployed through CM, Nomad needs to obtain the access token for the Enhanced HTTP DP endpoint from the Management Point, which it is able to do using HTTP. For Task Sequences, the access token is available in the _SMSTSDPAuthToken Task Sequence variable, so Nomad does not need to obtain it from the MP.
Nomad Pre-caching	Workgroup AD Domain-joined Azure AD-joined Hybrid-joined	Pre-caching requires Nomad to access the Management Point to locate the content and DP access token, which it is able to do using HTTP.

These scenarios are also supported if the client on the corporate network gets a Cloud DP as a source.

9.4.2.5.4.1.2 Internet clients with CMG / Cloud DP

For the purpose of this discussion, Cloud DP refers to either a classic Cloud DP or a content-enabled CMG.

Scenario	Clients supported	Notes
Configuration Manager Package, Application, Software Update and Task Sequence Deployments	Workgroup AD Domain-joined Azure AD-joined Hybrid-joined	When content is deployed through CM, Nomad is able to obtain the access token for Cloud DP from the CM client [(1)]. If there are multiple Cloud DPs, the client will be able to download content from the Cloud DP for which the CM client queued the download job using the Cloud DP access token provided by the CM client. If that DP becomes unavailable, Nomad will attempt to connect to the other Cloud DPs in the list and will query the CMG for the new Cloud DP access token. If Nomad is unable to authenticate with the CMG[(1)] it will continue to retry the available DPs returned by the CM client until it is able to connect to the original DP.
Nomad Pre-caching	Workgroup AD Domain-joined Hybrid-joined	Pre-caching requires Nomad to access the CMG to locate the content and obtain the Cloud DP access token[(1)].

[(1)] If the CM client is not using a PKI client authentication certificate to authenticate with the CMG, Nomad will not be able to request content location or obtain the Cloud DP access token from the CMG. Note that CM requires Workgroup and AD Domain-joined clients to have a PKI client authentication certificate (refer to https://docs.microsoft.com/en-us/mem/configmgr/core/clients/manage/cmg/certificates-for-cloud-management-gateway#bkmk_mphttps), so this will only affect Azure AD Joined / Hybrid devices that use Azure AD or token-based authentication with the CMG.

9.4.2.6 App-V support

Nomad supports application virtualization (App-V) applications which are deployed as streamed content by Configuration Manager.

> **Note**
>
> Nomad only handles App-V applications that use Configuration Manager as the App-V server. It does not integrate with the standalone App-V server.

App-V streaming is a way of providing centrally managed applications to many enterprise users. The majority of the application's content is not downloaded until a user actually invokes the application for the first time, thus not wasting network bandwidth or the user's time until they

need the content. The icons etc. for the application appear on the user's desktop, but the executable part of the application is held back until it is required.

> **Note**
>
> The executable part of the application is downloaded by the App-V client when required, it is not downloaded by Configuration Manager. This means that Nomad is not involved and the App-V client fetches it directly from the DP.

Nomad respects the Configuration Manager settings for fast and slow networks. For example, an App-V application's deployment type may specify streaming on a fast network but a full download on a slow network.

9.4.2.6.1 App-V supported versions

These versions of App-V are supported:

4.6 SP2

5.0 RTM, 5.0 SP1, 5.0 SP2

In fact Nomad is not even aware of App-V as such, just that certain files should be excluded from the application's content.

9.4.2.6.2 Partial content and Nomad elections

When Nomad downloads the non-executable part of a streamed application, it recognizes that it only has part of the entire content even when it has downloaded everything it has been told to. For App-V streamed applications, this initial download amount is reflected in the final job statistic as less than 100%. Typically, the non-executable part of a streamed application is less than 1% of the entire application. This percentage is accurately reflected when Nomad clients hold an election, including where Single Site Download is involved.

For example, if client A has a complete streamed download but then client B wants the entire download for some reason, B will fetch the partial download from A and then the rest (the executable part of the content) from the DP (if no other client has more content). In keeping with standard Nomad behavior, a client which has previously downloaded all the content will always win an election over clients that have downloaded partial content, even if the requesting client only requires the partial content.

Nomad FanOut mode is also supported for streamed applications.

9.4.2.6.3 Forcing a full download

App-V streaming support is enabled by default. If it needs to be disabled, update the CompatibilityFlags registry value. This will cause the entire content to be downloaded by rather than just the XML configuration files.

9.4.2.6.4 Restrictions

Multicast is not supported for streamed App-V applications

Space reserved in the Nomad cache will be for the entire package content size, not just the streamed content size

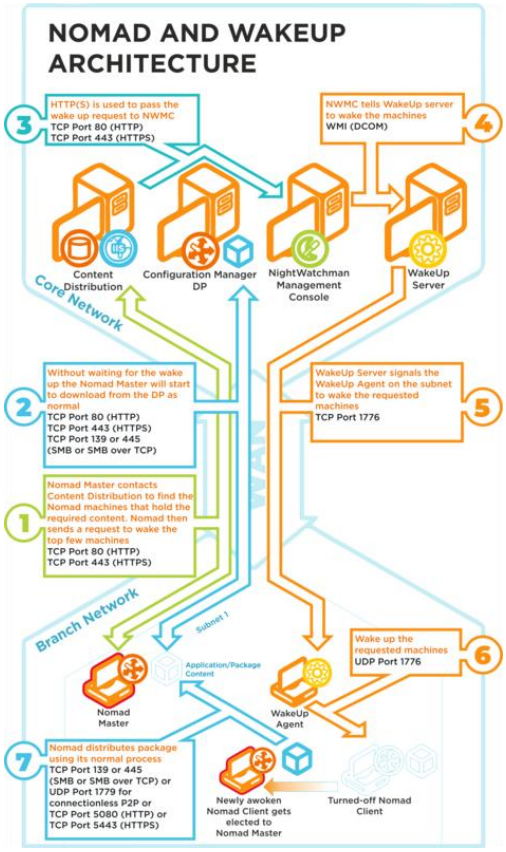
Full elections will take place if the partial content is re-requested for download by the Configuration Manager client even if that partial content has already been downloaded.

9.4.2.7 Integrating Nomad with WakeUp

Nomad integration with WakeUp enables Nomad to share content from its devices that are holding particular content, even if those devices are offline. One reason why peers in the local subnet may not respond to the request even though they have content in their caches is that they are offline (shutdown, in hibernate or sleep mode). However, if WakeUp is integrated, the Nomad client would know which offline device has the content and can wake it up when it queried Content Distribution.

The wake up list is maintained by Content Distribution and is the same list that Single Site Download (SSD) uses. Separate lists of peers are returned for subnet and site. This feature requires Nomad SSD to be enabled, Content Distribution and a NightWatchman infrastructure. The feature is enabled during installation of NightWatchman Management Center. Please refer to Nomad Preparation for requirements.

9.4.2.7.1 Nomad and WakeUp architecture and ports



Ports	Description
TCP 80 (HTTP) TCP 443 (HTTPS)	**Step 1**

Ports	Description
	Nomad Master contacts Content Distribution and gets a list of Nomad devices that hold the content it requires. Nomad sends a request to wake the top 5 devices on the list. Refer to WakeUpBatchSize for details about how you can set the maximum number of machines to wake up in a single call.
TCP 80 (HTTP) TCP 443 (HTTPS) TCP 139 (SMB) TCP 445 (SMB over TCP)	**Step 2** Without waiting for any devices to be awoken, the Nomad master starts to download content from the DP. This communication depends on how the DP is configured. It may be one of the following: HTTP HTTPS SMB SMB over TCP For Configuration Manager, the default setting is HTTP or HTTPS.
TCP 80 (HTTP) TCP 443 (HTTPS)	**Step 3** Content Distribution posts the wake message from Nomad to the NightWatchman Management Center Web API.
WMI (DCOM)	**Step 4** NightWatchman Management Center tells the WakeUp server to wake the requested devices.
TCP 1776	**Step 5** WakeUp Server signals the WakeUp Agent on the appropriate subnet to wake the requested devices.
UDP 1776	**Step 6** The WakeUp agent on the subnet sends a wakeup request to the requested devices.
TCP 139 (SMB)	**Step 7**

Ports	Description
TCP 445 (SMB over TCP) UDP 1779 (connectionless P2P)	As part of its standard behavior, Nomad holds regular elections (every 5 minutes) to determine the most appropriate master. If a device is found (i.e. one that has been recently awoken) that holds more of the required content, it stops downloading from the DP and fetches the content from the new device's cache. This may be via SMB or via connectionless P2P, depending on the configuration of Nomad.

9.4.2.7.2 How it works

When a Nomad client wants to download content it broadcasts a request for peers in the local subnet, if no peers respond then:

If Single Site Download (SSD) is enabled, it queries Content Distribution for peers on other subnets for the content.

If SSD is not enabled, it downloads from the DP.

WakeUp integration can be for peers on the local subnet, in the site (i.e. neighboring subnets not the local subnet), or on the local subnet and in the site.

These lists are sorted in descending order by:

Highest percentage of content.

Server, followed by desktop, then laptop. (for Nomad's purposes, whether a device is a server or a desktop depends on the operating system, not the hardware.)

Most recent timestamp on the content (because recent information is more likely to be correct than older data).

Nomad sends a wake up request to Content Distribution, which relays it through NightWatchman Management Center to WakeUp servers and ultimately the 1E agents to wake these devices up.

> **Note**
>
> Nomad does not wait for devices to wake at this point. It carries on immediately after sending the wake up requests and starts downloading from the DP. Nomad also uses a fire and forget policy: it does not keep track of which devices do and do not get woken.

Meanwhile, periodic elections occur and when a master is elected, the download from the DP is interrupted and the download process begins again. The difference this time is that Nomad will not query Content Distribution again, as some subnet and/or site devices will have woken up and is able to provide the content.

> **Note**
>
> In addition, Content Distribution will not return devices that do not match the following criteria:

The network adapter registered for the device matches the criteria for local subnet or site wakeups

Device must be enabled as a content provider

Device is not an unknown device.

Reasons for not being a content provider are:

Running under WinPE

A domain controller

Content not to be registered with Content Distribution (ContentRegistration = 0)

Peer-to-peer communication disabled (P2PEnabled = 0)

Sensitive server (P2PElectionWeight = 0)

SSDEnabled = consumer-only

Using wireless adapter (so cannot be woken)

Inhibited subnet being used

Inhibited AD site being used.

9.4.2.7.2.1 Batching WakeUp requests and other configuration

WakeUp can be enabled for just the local subnet, the site (of neighboring subnets), or both. This is configured by the WakeUpEnabled setting. Note that if site wake up is required, then SSD consumer mode must also be enabled (SSDEnabled is 1 or 3).

If WakeUp integration is enabled, the number of devices in each list (subnet and site, separately) is specified by MaxDevicesFromAE.

Not all devices need be woken at once. After all, it is desirable to awaken as few devices as necessary because they were shut down in the first place for a good reason – to save power. They can be collected into batches (separately for subnet and site wake ups), controlled by the WakeUpBatchSize setting.

By default, this is the same as MaxDevicesFromAE so there is usually just one wakeup iteration. But if *WakeUpBatchSize* is less than *MaxDevicesFromAE* (obviously it cannot be greater), then some devices will be left over after the first batch of wake ups has been sent (assuming that at least *MaxDevicesFromAE* devices were actually found in Content Distribution), and these remainders will be woken if Nomad falls back to the DP on its second and subsequent periodic elections.

Note

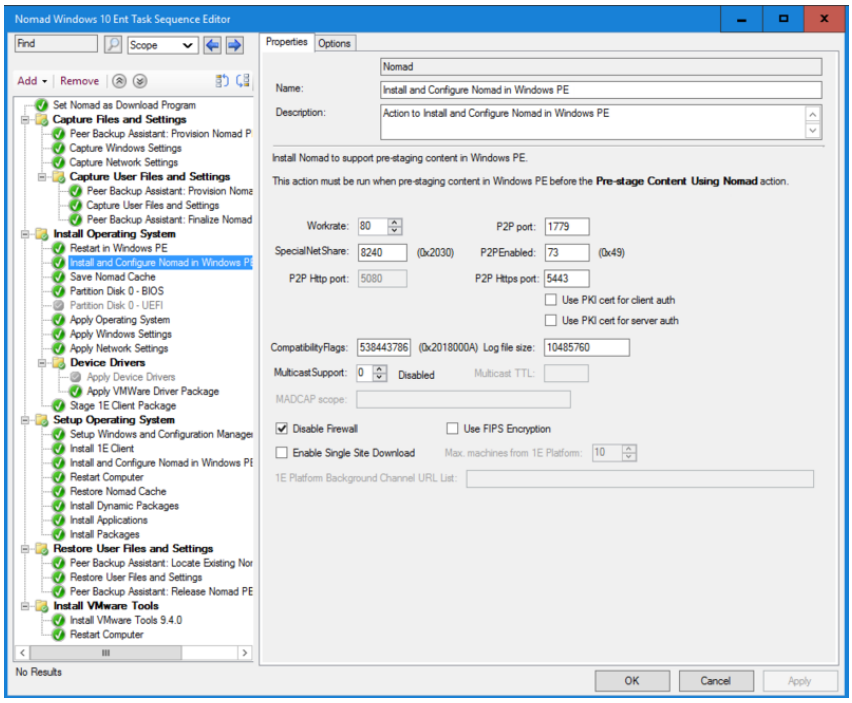
MaxDevicesFromAE and *WakeUpBatchSize* are applied to the subnet and site lists separately, but different values for site and subnet cannot be specified – the same are used for both. For example, if *MaxDevicesFromAE* is 10 then up to 20 devices will be fetched (if there are sufficient registered in Content Distribution with the content), 10 for the subnet plus another 10 for the site.

Finally, if the content is small then there might not be time for a periodic election to occur, because Nomad gets everything from the DP in the first iteration. In this situation, there is no

point waking up devices because they will not be ready in time. For this reason the WakeUpMinPackageSizeMB setting controls the lower cutoff size limit at which wake ups occur.

9.4.2.7.3 Support for Nomad running under WinPE

WakeUp integration, like SSD, can be used when running under WinPE to download the full operating system. WakeUp is particularly useful in this case because OS *.wim* files tend to be large. WakeUp integration is not enabled by default. This example shows a task sequence action where it has been enabled.



9.4.2.7.4 Restrictions

Please note the following restrictions.

Restriction	Explanation
Nomad running under WinPE cannot use wake up if Windows authentication is enabled in Content Distribution.	This is because a WinPE device is not in a domain.
The WakeUpMinPackageSizeMB setting is effectively always 0 in WinPE and for standalone Nomad downloads, so WakeUp will be invoked even for small packages.	This is because the size of the content cannot be easily determined (under normal conditions the size can be found from Configuration Manager policy. And in the situations where *WakeUpMinPackageSizeMB* is used, even if enough of a package has already been

Restriction	Explanation
	downloaded to take it under the limit, wake up requests are still sent.
Even if just local wake up is used (i.e. within the local subnet but not the site), the *Locations* table in the Content Distribution database must be populated.	The *Locations* table must always be configured for Nomad WakeUp integration to work.
If, when a periodic election occurs, a different master host is elected, the whole WakeUp process starts again.	The new host queries for devices with the content and the batched wake up requests start from the beginning. However, in practice, if a given host gets elected as master, it is very likely to be re-elected when a periodic election occurs. Also, if a master is shut down while a transfer is running, when it is restarted it will start the WakeUp process again.
The mechanism does not support alternate source copy downloads.	i.e. downloading an older version of a package from a LAN neighbor then filling in the changes.
IPv6 is not supported.	n\a

9.4.2.8 Deploying Office 365 updates

Configuration Manager introduced support for Office 365 agents in Current Branch 1602, and Nomad introduced support in version 6.1.100. This section describes how Office 365 deployments differ in terms of ACP requirements and goes on to describe how Nomad behaves during the download.

Refer to Deploying updates for Office 365 for an example scenario about deploying Office 365 updates and how you can monitor those deployments using the Nomad app.

9.4.2.8.1

9.4.2.8.1.1 Configuration

Downloading the following type of updates is enabled by default in the Nomad client (1E Client 4.1 and later). Downloading from Microsoft Update is also enabled by default.

The settings are defined in CompatibilityFlags and you will need to ensure the relevant bits remain set if you are using that registry value to configure other options, as follows:

Type	Enable Nomad to download	Enable Nomad to download from Microsoft Update
Software Updates (including Windows 10 feature updates)	Always enabled	Set bit 27 (0x08000000, 134217728 in decimal)
Office 365 updates	Always enabled	Set bit 28 (0x10000000, 268435456 in decimal)
Windows 10 Express Installation Files and Delta Content for Updates	Set bit 26 (0x04000000, 67108864 in decimal)	Set bit 28 (0x10000000, 268435456 in decimal)

To enable all the above, then AND bits 26, 27 and 28 with whatever you have already set in CompatibilityFlags.

Please refer toDistributing software with Nomad and Configuration Manager: Enabling Nomad for Applications and Software Updatesfor how to configure client settings to set Nomad as a download provider for applications and software updates.

Note

Please note, there is no configuration is required on Distribution Points.

9.4.2.8.2 How it works

The Office 365 Click to Run agent (CTR) will process the update metadata obtained from the Configuration Manager Software Update Point and pass a request for content to the Configuration Manager agent. As with non-Office download requests, the same Alternate Content Provider API is used by the Configuration Manager agent; with the Configuration Manager agent Content Transfer Manager (CTM) thread invoking Nomad to download the requested content. When Nomad receives a download job with a manifest file from the CTM it will:

Parse the manifest to retrieve the content description.

Download the content described in the manifest either from a DP or peer cache.

Copy the downloaded data to the destination folder described in manifest.

Notify Configuration Manager that the download job is complete.

Wait for the next job.

For Office 365 updates the CTM passes different information to Nomad, when compared with other types of content download. The other types typically provide a content identifier i.e. Package ID and version. For Office 365 updates, a manifest file is also passed with the request. It is the manifest file that contains details of the content to be downloaded and its destination path (typically C:\ProgramData\Microsoft\ClickToRun\...). A single update may require multiple download jobs, resulting in multiple manifests being passed to Nomad while it is obtaining the content. Once the content has been downloaded, it is copied into the destination specified in the manifest file. Nomad does not configure hardlinks for Office 365 updates.

9.4.2.8.2.1 Hash checking and communication with the CTR agent

Another difference is that Office 365 updates do not have a Configuration Manager-generated hash associated with the content. For other types of content, Nomad performs an AES256 hash check prior to, and immediately after, download and compares this with the Configuration Manager hash in order to establish the content's validity. For Office 365 updates, there is no comparison hash made available to Nomad. Nomad therefore depends on the CTR for the validity status of the Office 365 update installation (the CTR performs its own hash check). Nomad also listens to the status API exposed by the CTR agent to check if the installation succeeded. If the installation fails, Nomad deletes the update from its cache and retries the download. As soon as Nomad receives a download success status, it sends a status message and stops listening to the CTR agent.

9.4.2.8.2.2 Byte-ranges

In order to make the download process more efficient, Microsoft has implemented a process of byte-range requests rather than (or sometimes in addition to) requesting entire files. Nomad treats byte-range requests in just the same way as files and will initiate a local election for each to minimize the impact of any download across the WAN.

To process and download these byte-ranges, Nomad divides each Office 365 package file into pages of 128MB, for example a 300MB file has 3 logical pages. If we think of a file as a book, then each page of the book is 128MB with each line of a page being 32KB. The byte-ranges described in the manifest indicates the start and end position within our lines of the page. Nomad normalizes these byte-ranges to 32KB blocks, adjusting the start and end positions so that the byte-range contains complete lines and no line is truncated.

9.4.2.8.2.3 Nomad elections

Elections may occur when a Nomad client requires content that is not resident in its cache. An election is not always necessary, with Nomad storing active download broadcast notifications in memory and then connecting direct to these hosts if itself requires the byte-range or file at some later time. All responses peers receive are stored in its Query Result Store (QRS). Before initiating an election, a Nomad client will first verify its QRS to see if relevant peers are available for content downloads. If relevant peer(s) are found in the query store, an election does not occur.

When elections do occur and Nomad clients respond, the receiving Nomad client sorts the list of responders top-down based upon the following criteria:

Longest byte-range on disk starting from requested offset

Longest relevant active downloader

Election weighting

NomadBranch service start-up time

Machine name.

Under certain circumstances, a Nomad client will not reply to an election request, even if it has the data in its cache. This happens when:

Request comes from an inhibited network

P2P SMB is disabled [Connectionless mode is not supported for Office 365 update deployments]

The Nomad Account (*SMSNomadP2P&*) is locked out

The Nomad Account (*SMSNomadP2P&*) is not active

The machine is a domain controller and *SPECIALNETSHARE_MACHINEACCOUNT* is not set in *SpecialNetShare*

The *P2PElectionWeight* registry value is set to zero

The Nomad share not available.

9.4.2.8.3 Which other Nomad features are supported by the Nomad Office 365 feature?

The following Nomad features are supported:

Nomad feature	Definition
Peer copy over HTTP or HTTPS	Nomad can be used to enable the Office 365 update byte-range request content to be shared amongst Nomad peers.
Single Site Download (SSD)	SSD can be used to locate byte-range request content across different subnets on the local branch.
Peer-to-peer SMB	Peers can download data from other peers using the SMB protocol.
Work rates and cache priority	Work rates determine the amount of bandwidth Nomad utilizes for the download and cache priority determines when the cache is purged.
Download timeout	The timeout in seconds after which a job will be cancelled if the download has not been successful.
Save and restore Nomad cache	Custom task sequence action to Save Nomad Cache either in WinPE or a full Microsoft Windows operating system and a custom task sequence action to Restore the Nomad cache in the new Operating System during provisioning after Nomad has been installed.
Status messages for download events	Status messaging for specific download events.
Inhibiting subnets and sites	Defining subnets and AD sites where machines download from the DP and not participate in Nomad elections (status messages are not relayed).
SpecialNetShare	Options for the Nomad share.

Nomad feature	Definition
Custom ports	Enables the use of custom ports for data transfer and communications.
Cache cleaning	Enables cache management.

The following are not supported by the Office 365 feature:

Cloud-based DP

Connectionless P2P

Nomad FanOut

SMB downloads from the DP

Remote differential compression (RDC)

Nomad Pre-caching

Hash or CRC validation

LSZ or metadata creation or download

Failover to BITS (SuccessCodes includes 0x9999).

> **Note**
>
> Download from Microsoft Updates is only supported if Downloading content for CM Software Updates from Microsoft Update is enabled (default). Set bit 28 (0x10000000, 268435456 in decimal) in CompatibilityFlags.

9.4.3 OS Deployment

Nomad support for Configuration Manager OS Deployment.

9.4.3.1 OS deployment task sequences

Nomad can integrate with OSD strategies to maximize the efficiency of distributing large OS content across the network. It does this by providing a number of Task Sequence steps that can be integrated directly into your OSD Task Sequences.

Refer to Using Nomad with Operating System Deployment OSD for an example scenario about how Nomad can integrate with Operating System Deployment (OSD) strategies to maximize the efficiency of distributing large OS content across the network and how you can monitor those deployments using the Nomad app.

> **Tip**
>
> Big Bang have integrated Nomad into their Universal Imaging Utility (UIU) product to search for driver content on peers. Check out the 1E blog Taking the worries out of managing drivers during Windows 10 upgradesfor a quick overview, take a look at

https://www.bigbangllc.com/The-UIU or reach out to https://www.bigbangllc.com/Support for further information.

9.4.3.1.1 Nomad and OS deployments

The three areas where Nomad integrates with OSD are:

WinPE support – to provide Nomad functionality when imaging a machine

Custom task sequence actions – enables Nomad functionality to be integrated directly into OSD task sequences

Configuring PBA hosts – enables Nomad functionality to be used during OSD to back up user files and settings (USMT data)

> **Note**
>
> When Nomad AdminUI Extensions are upgraded from an older version to a newer version, you must ensure that the Nomad task sequence actions have correct values set including modified as well as default values.

9.4.3.1.1.1 OSD Enhancements

Nomad includes OSD enhancements that increase Nomad's integration with OSD task sequence. These enhancements drastically simplify the task sequence engineering process and the steps that are required to integrate Nomad with OSD.

These enhancements are:

Enhancement	Description
SMSTSNomad.exe	An executable that's part of the OSD tool-set, allowing Nomad to leverage the Configuration Manager **SMSTSDownloadProgram**option and act as Alternate Content Provider during OSD.
Preserving Nomad logs	The **Save Nomad Cache**and**Restore Nomad Cache**task sequence actions ensure that Nomad logs are preserved across all OSD phases.
Nomad cache handling	The functionality of the **Save Nomad Cache** and **Restore Nomad Cache** task sequence actions reduces the risk of the copy/move content behavior leading to task sequence failures.

9.4.3.1.1.2 SMSTSNomad.exe

SMSTSNomad.exe supports the use of Configuration Manager's **OSDDownloadContent.exe** directly from a Run Command Line step in a Task Sequence, as well as the previously supported **Download Package Content Native** Configuration Manager Task Sequence Step. No additional configuration is required to make this work. NomadBranch.exe supports SMSTSNomad.exe.

Nomad leverages the Configuration Manager SMSTSDownloadProgram task sequence variable. When this variable is set to the path to an executable, the task sequence engine calls the executable whenever it has to download some content. For this to work effectively, Nomad uses SMSTSNomad.exe.

To avoid the overhead of having to manually set the SMSTSDownloadProgram variable to SMSTSNomad.exe in your task sequence, use the custom task sequence action Set Nomad as Download Program. The following are the content types that are supported by SMSTSNomad.exe:

Packages

OS Images

Boot Images

Applications

Driver packages

Drivers (via Auto apply drivers TS action).

9.4.3.1.1.3 Preserving Nomad logs

Save Nomad Cache preserves the Nomad log files long with the contents of the Nomad cache. They are restored again after the OS has been deployed when **Restore Nomad Cache** runs. **Save Nomad Cache** also appends a time stamp to the name of the Nomad log files to prevent any possibility of name conflicts during the subsequent **Restore Nomad Cache** step.

For more detail about these Task Sequence steps, please refer to Save Nomad Cache and Restore Nomad Cache.

9.4.3.1.1.4 WinPE support

Nomad can be used in an OSD task sequence to find OSD packages required by WinPE that are located on pre-cached Nomad peers on the local subnet rather than downloading them from the nearest DP. Using Nomad in WinPE as part of an OSD bare metal task sequence has a number of distinct advantages:

Multiple connections are supported by Nomad caches maximizing the number of machines that can be built concurrently

Multiple pre-cached locations can be supported (we recommended at least 2 per subnet to increase the number of simultaneous imaging jobs are supported)

Nomad in WinPE supports all the Nomad features, so elections, failover, and bandwidth efficiency are all on hand to maximize the resilience and performance of the imaging process.

These advantages become important when you plan a rapid OS refresh over a relatively short time. Nomad must be installed as part of a task sequence in order to support the use of pre-staged content from within WinPE and managed through custom task sequence actions,

9.4.3.1.1.5 Pre-caching content

Pre-caching packages used during OSD is important because:

Image packages, especially for Windows, tend to be several gigabytes in size and downloading these across the WAN as part of an OSD is undesirable and slow

Bandwidth Protection is enforced if Nomad senses that the WAN link is getting congested with other network traffic, this ensures that any impact on the WAN during pre-caching is kept to a minimum.

Nomad in WinPE automatically locates local pre-cached content and uses these to avoid WAN traffic to ensurer that once the image package is on the branch there is no impact on the WAN and the time taken to retrieve the image is minimized because everything is local.

> **Note**
>
> If there is no pre-cached content on the local branch and multicast is not enabled, we recommend you configure Nomad to use connectionless P2P using the P2PEnabled value. This is because WinPE does not have File and Print Sharing services, so Nomad machines cannot use their default P2P communications. Enabling connectionless P2P ensures that multiple WinPE Nomad machines only download their content once and then share it locally.

Nomad pre-caching is directly integrated with the Configuration Manager Console, is fully compliant and works with Role Based Access in Configuration Manager.

To start the pre-cache wizard, right-click any of the following types of content in the Configuration Manger console and from the context menu, choose Pre-cache content using Nomad.

Applications

Packages

Driver packages

Operating system images

Operating system upgrade packages

Boot images

Task sequences.

Refer to Nomad Pre-caching for more information about using the Nomad pre-cache wizard.

> **Note**
>
> Performing this step will update the Nomad settings for the OS image properties as well. This will affect the use of Nomad in every location this image is referenced.

9.4.3.1.1.6 Adding binaries to an existing boot image

The *NBCacheActions.exe*, *NomadPackageLocator.exe*, *TSEnv2.exe*, *NomadBranch.exe*, *SMSNomad.exe* and *SnoItfPS.dll* files are placed in the Microsoft Configuration Manager installation folder by **NomadBranchTools.msi** , they copy the 32-bit tools to *OSD\bin\i386* and the 64-bit tools to *OSD\bin\x64* and then modify the *osdinjection.xml* file to include these in the WinPE boot images when DPs are updated.

On Configuration Manager, the *NomadBranchTools.msi* installer must be used.

9.4.3.1.2 Custom task sequence steps

Nomad has a number of custom task sequence steps that can be integrated with Configuration Manager Task Sequences. These custom task sequences are located in the Task Sequence editor.

> **Note**
>
> When Nomad AdminUI Extensions are upgraded from an older version to a newer version, you must ensure that the Nomad task sequence actions have correct values set including modified as well as default values.

To add a Nomad custom task sequence step:

Navigate to **Software Library** → **Overview** → **Operating Systems** → **Task Sequences**

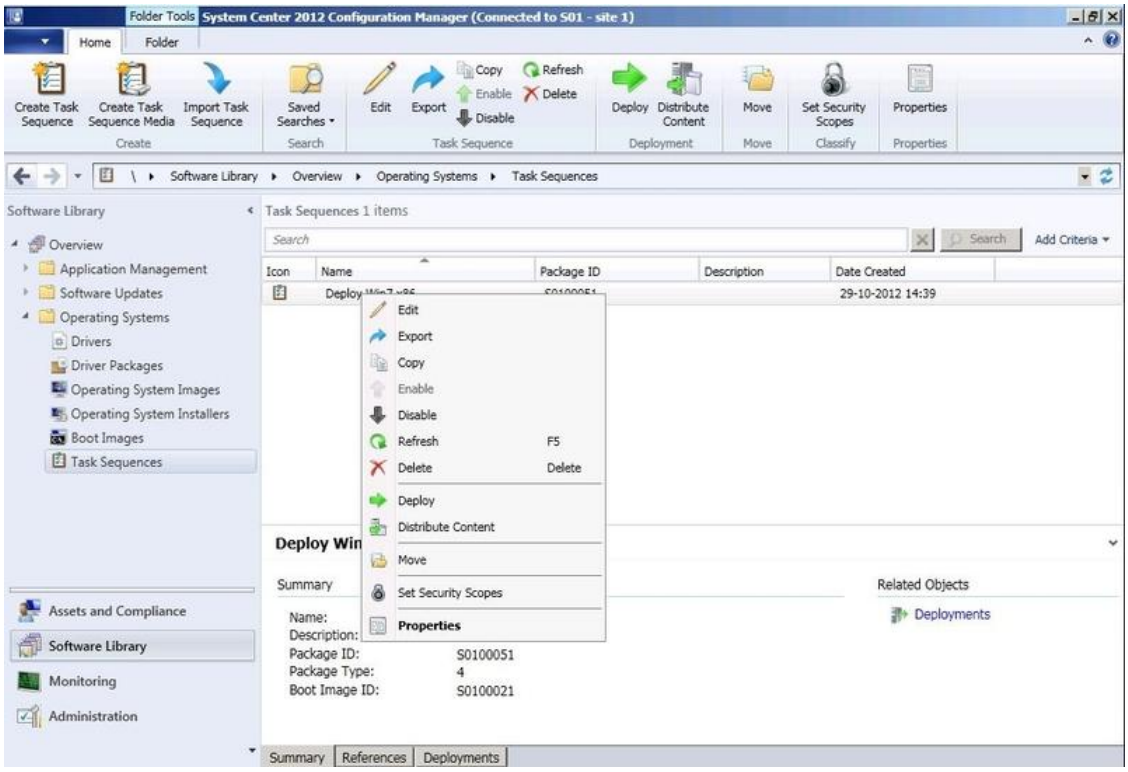
You can create a new Task Sequence or edit an existing one, which opens the **Task Sequence Editor**

For an existing Task Sequence, click on an existing step, to create a group or step above it

In the Task Sequence editor menu, click **Add**

This opens a menu showing a range of different Task Sequence sets

Click on one of the sets and select a Nomad Task Sequence step - the names of sets and steps are listed opposite.



9.4.3.1.2.1 1E Nomad task sequence actions

Set Nomad as Download Program — Sets SMSTSNomad.exe as the download program during a task sequence. This is accomplished by setting the SMSTSDownloadProgram task sequence variable to SMSTSNomad.exe.

Create Nomad Application Policy — Creates a Nomad application policy and is used in a task sequence during the provisioning phase prior to any applications being installed. It uses the NomadPackageLocator.exe command-line switches tool to enable Nomad to be used as an Alternative Download Provider during provisioning. When the application policy is no longer required it can be removed using the Delete Nomad Application Policy action.

Delete Nomad Application Policy — Deletes a Nomad application policy previously created using the Create Nomad Application Policy action. It uses the NomadPackageLocator.exe command-line switches tool to remove the previously created Nomad application policy.

Install and Configure Nomad in WinPE — Installs and configures Nomad in WinPE. Typically, to support the use of pre-staged content.

Save Nomad Cache — Saves the Nomad cache either in WinPE or a full Microsoft Windows operating system. It copies, links or moves previously downloaded content to the protected task sequence runtime folder so that it is not deleted by the standard Apply Operating System task sequence action.

Restore Nomad Cache — Restores the Nomad cache in the new Operating System during provisioning after the 1E Client has been installed with the Nomad module enabled. This action only needs to be included in the task sequence if Save Nomad Cache is run prior to applying the new Operating System.

Get Migration Settings — Provides support for optional encryption in Nomad PBA, and Provides computer association details in 1E Application Migration. Used in computer Replace and Refresh (Wipe and Load destructive and non-destructive) scenarios, it is configured to run under either the capture phase or the restore phase, depending on the scenario.

Stage 1E Client Package — Downloads the 1E Client package ready for installation by the Install 1E Client Task Sequence step. It's typically executed in Windows PE and must be included before the Install 1E Client step in the task sequence.

Install 1E Client — Installs the 1E Client. The Stage 1E Client Package step must be to be included before this step in the Task Sequence. The 1E Client installer and any Transform or Patch that should be applied during installation must be included in the 1E Client Package referenced in the Stage 1E Client Package step.

9.4.3.1.2.2 1E Nomad PBA task sequence actions

Peer Backup Assistant: Provision Nomad PBA Data Store — Provisions a PBA data store prior to saving user state using USMT. It is the first step of the Peer backup assistance sequence (USMT Capture User State follows).

Peer Backup Assistant: Finalize Nomad PBA Data Store — Closes the connection to the PBA data store after user state is saved with USMT Capture User State.

Peer Backup Assistant: Locate Existing Nomad PBA Data Store — Finds saved user data, prior to restoring user state using the USMT Restore User State action.

Peer Backup Assistant: Release Nomad PBA Data Store — Releases saved user data in the Nomad cache, after restoring user state with USMT Restore User State.

Peer Backup Assistant: Close Nomad PBA Data Store (deprecated) — This step has been replaced by Peer Backup Assistant: Finalize Nomad PBA Data Store. Existing deployments will still work, but you cannot modify them. Going forward, we recommend using its replacement.

Peer Backup Assistant: High Availability (deprecated) — This step is deprecated, and you should use the Peer Backup Assistant: Finalize Nomad PBA Data Store instead. Existing deployments will still work, but you cannot modify them. Going forward, we recommend using its replacement.

9.4.3.1.2.3 1E OSD task sequence actions

1E WSA Actions — The 1E WSA Actions action is an essential component of the WSA deployment task sequence. Its position and configuration within the task sequence is critical to ensuring the task sequence completes successfully. The action performs one or more of the following functions depending on the selection made when configuring the step:

9.4.3.1.3 Using Nomad for an OSD refresh

An operating system deployment (OSD) refresh typically uses two Configuration Manager site systems – a distribution point (DP) and a state migration point (SMP). A standard OSD refresh uses task sequences as follows:

The user state is captured and either stored locally or on a SMP.

The Configuration Manager client downloads the Windows Preinstallation Environment (WinPE) boot image to the local workstation while the Configuration Manager client is still running.

If the task sequence is deployed as Download all content before starting, all content is downloaded into the Configuration Manager cache (not suitable for dynamic packages).

The boot record is updated to enable the computer to reboot to WinPE.

If the task sequence is deployed as Access content from DP as required or Download content as required, the content is obtained from the DP.

The new OS is applied.

The saved user state is reapplied to the new OS and the process completes.

9.4.4 Nomad Management

Real-time visibility of what content is downloading or available in each location, subnet and client. Real-time visibility of Delivery Optimization downloads and content availability in each location, subnet and device.

9.4.4.1 Nomad app overview

The app provides visibility of activity and cache status for content distributed by both the Nomad and Delivery Optimization.

9.4.4.1.1 Explaining content versions

In Configuration Manager (CM), the content associated with a Package or Application Deployment Type may be updated by an administrator. In the case of Packages, CM increases the Package

Version property, and for Application Deployment Types, CM generates a new Content ID for the Deployment Type.

The Nomad Overview page displays summarized distribution data for a selected period. The displayed data shows all downloads and download activity for all versions of content for that period. For example, if a device downloaded Package A version 1 a month ago and later downloaded version 2 of the same Package, the Overview page would reflect both downloads.

In this version it has not been possible to reflect previous versions in the **Content Titles** summary in the top status bar, or in the **Content Titles Count by Content Type** and **Download Volume by Content Type** tiles. These will only represent download activity for the latest version of content. This may result in apparent 'loss' of data (e.g. a reduction in the number of content titles or download volume) when content for an existing Package or Application is updated in CM, as these metrics will only include download activity for the latest version. This will be addressed in a later version of Nomad.

> **Note**
>
> Other pages in the app, such as the Content page, only show the latest version of any given **Content Title**. Those pages concern the current state of things (e.g. where content is available) because only the latest version is usable by CM deployments. As a result, showing older versions would be misleading for users.

The **Overview** page gives a brief snapshot of download activity. The page has multiple tiles showing:

Content Titles by Content type

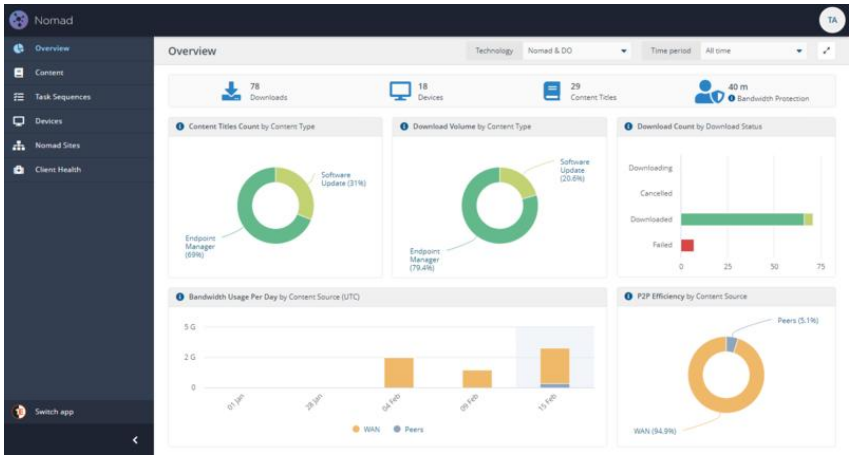
Download Volume by Content Type

Download Count by Download Status

Bandwidth Usage Per Day by Content Source (UTC)

P2P Efficiency by Content Source (Peer to Peer - P2P).

The results can further be narrowed down by using the **Technology** and **Time period** filters on the page.



9.4.4.1.2 Navigation and Filtering

By default, the view shows activity and status for all time and will show activity and status for both Nomad and Delivery Optimization. These defaults can be modified using the **Technology** filter and the **Time period** filter.

> **Note**
>
> Each content tile can be expanded using the **Expand** button on the top right-hand corner of each tile.

9.4.4.1.2.1 Time period filter

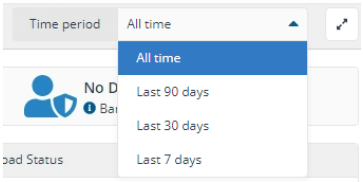
Using the **Time period**filter at the top of the page, you can narrow down the results by date. You can choose from the following options:

Last 90 days

Last 30 days (Default)

Last 7 days.

> **Note**
>
> If these filters are applied to any app page, it is reflected on all other pages in the Nomad App.



9.4.4.1.2.2 Technology filter

You can use the **Technology** filter to differentiate between downloads through Nomad or Delivery Optimization (DO).

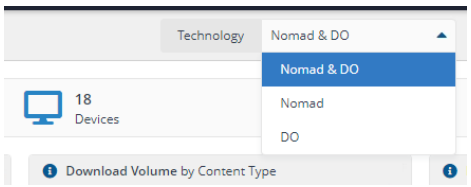
The following options are available:

Nomad & DO (Default)

Nomad

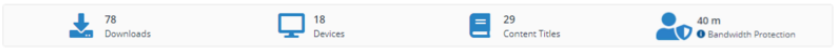
DO.

> **Note**
>
> If this filter is applied to any app page, it is reflected on all other pages in the Nomad App.



9.4.4.1.3 Top status bar

The status bar along the top of the page shows high-level statistics for the currently selected **Technology** (Nomad or DO) and **Time period**. The bar is shown on the Overview page and includes four icons, **Downloads**, **Devices**, **Content Titles** and **Bandwidth Protection**.



Item	Description	Icon
Downloads	Downloads reflect the total number of content downloads. This includes both Delivery Optimization (DO) and Nomad downloads. The results can be filtered on the **Time period** and **Technology** filters and display the total number of downloads of any version of content that occurred in the selected period. A download counts as any download activity for a given Content Title on a given device. For example, if there are 10 content titles downloaded by 50 devices, the total count of download instances would be 500. For CM Applications, each Application Deployment Type counts as a separate Content Title. Clicking on this icon navigates to the **Content** page filtered to show **Content Titles** reporting download activity within the selected **Time period**.	
Devices	Displays the total number of devices that have reported download activity for any content version in the selected **Time period**, including: Packages Applications Updates from Configuration Manager. Clicking this icon navigates to the **Devices** view, filtered to show devices where download activity was reported within the selected **Time period**.	

Item	Description	Icon
Content Titles	Displays the total number of unique **Content Titles** where download activity of the latest version of the content titleis reportedin the selected**Time period.** For CM content, a**Content Title**is a single Application or Package. Clicking on this icon navigates to the Content view filtered to show the **Content Titles** that have reported download activity within the selected**Time period.** **Note** Applications in CM may have many Deployment Types. This summary counts an Application as a single Content Title.When viewing the Content view, Content Titles for CM Applications are further identified with the Deployment Type thatwas downloaded. So, the total number of Content Titles identified on the top status bar may be lower than the corresponding list of Content Titles on the Content page. This is because the Content page reports download activity for individual Deployment Types of CM Applications.	
Bandwidth Protection	Displays the total time that Nomad backed off when downloading content to protect end-user bandwidth. **Bandwidth Protection** allows Nomad to adjust the speed of ongoing downloads to save bandwidth for other business use. Bandwidth Protection ensures Nomad doesn't consume excess bandwidth and hinder other business activity.It does that by tracking the download time of data packets. If the time increases, it slows itself down (backing off) by sleeping for a few moments before downloading another packet.	

9.4.4.1.4 Content tiles

Content tiles display statistics for content download activity in the following panes:

Content Titles Count by Content Type

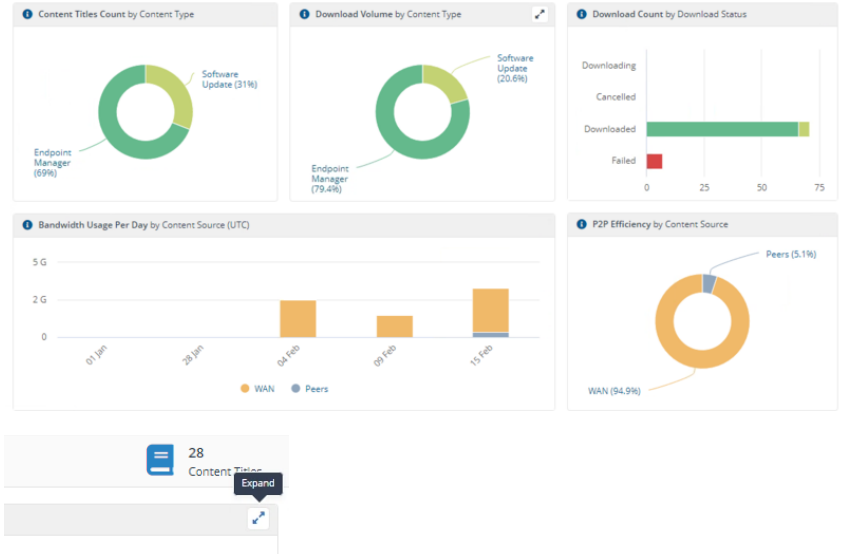
Download Volume by Content Type

Download Count by Download Status

P2P Efficiency by Content Source

Bandwidth Usage Per Day by Content Source UTC.

> **Note**
>
> Each content tile can be expanded using the **Expand** button on the top right-hand corner of each tile.



9.4.4.1.4.1 Content Titles Count by Content Type

The **Content Title Count by Content Type** tile shows the total number of unique **Content Titles** for where there is download activity reported for the latest version of the content within the selected **Time period**.

The data is grouped by **Content Type** and displayed as a donut chart. The app currently reports on two **Content Types**:

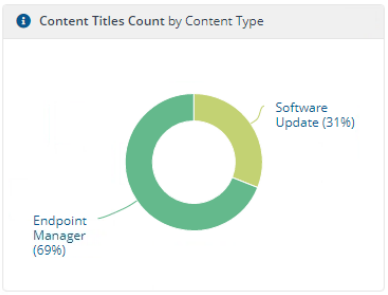
Endpoint Manager - CM applications and packages that are not delivered by DO

Software Update - includes any Microsoft Software Updates deployed through CM or Windows Update.

> **Note**
>
> Applications in CM may have multiple **Deployment Types**. This tile counts an Application as a single **Content Title**. When viewing the **Content view**, **Content Titles** for CM Applications are further identified with the **Deployment Type** that was downloaded.
>
> As a result, the total number of **Content Titles** identified on the top status bar may be lower than the corresponding list of Content Titles on the Content page (which reports download activity for individual **Deployment Types** of CM Applications).

Hovering over a **Content Type** segment of the chart displays the count of **Content Titles** of that type, also represented as a percentage of all **Content Titles**.

Clicking on a **Content Type** segment of the chart will navigate to the **Content** view, filtered to show related **Content Titles**.



9.4.4.1.4.2 Download Volume by Content Type

The **Download Volume by Content Type** tile shows the cumulative volume of content of the latest version of content downloaded by all devices within the selected **Time period**. The data is grouped by **Content Type** and displayed as a donut chart.

The chart enables you to see the effect that different types of content have on your network, in terms of the volume of data associated with them. It shows the percentage of packages and software updates by volume for:

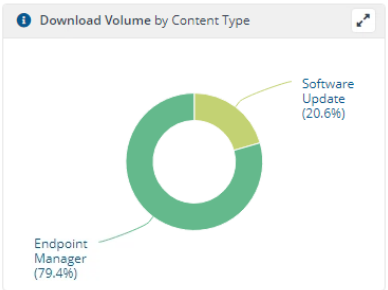
Endpoint Manager - CM applications and packages that are not delivered by DO

Software Update - content that can be delivered by Nomad, or DO if you're using Windows Update directly.

For example, if a single content title is 100MB and it is downloaded by 100 devices, the cumulative **Download Volume** reported for that particular **Content Title** would be 10,000MB. The chart shows the cumulative volume for all **Content Titles** on all devices, grouped by **Content Type**.

Hovering over a **Content Type** segment of the chart displays the total volume of downloaded content of that type. This is also shown as a percentage of total volume of downloaded content.

Clicking on a **Content Type** segment of the chart navigates to the **Content** view, filtered to show **Content Titles** of the selected segment.



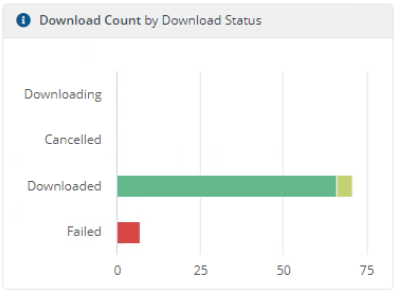
9.4.4.1.4.3 Download Count by Download Status

The **Download Count by Download Status** tile shows the status of download activity within the selected **Time period**, displayed as a bar chart by:

Status	Description
Downloading	Number of downloads currently in progress, where a download has been reported as started but has not yet reported complete, failed or cancelled.
Cancelled	Number of downloads whose last reported status was **Cancelled**, downloads may be cancelled by the user, or by the system, for example if the system is shut down or higher priority downloads are queued.
Downloaded	Number of successful downloads, if the downloaded content is still cached on a given device, it's represented by the dark green part of the Downloaded bar labelled **(Downloaded (Cached)** when you hover over it. If the downloaded content was subsequently deleted from the cache on a given device, it's represented in the light green part of the **Downloaded** bar labelled **(Downloaded (Deleted)** when you hover over it.
Failed	Number of downloads whose last reported status was **Failed**.

Hovering over any of the bars displays the number of downloads in the selected download state.

Clicking on any of the bars navigates to the **Content** view, filtered to include **Content Titles** where one or more devices is in the selected download state.



9.4.4.1.4.4 Bandwidth Usage Per Day by Content Source (UTC)

The **Bandwidth Usage Per Day by Content Source (UTC)** tile represents daily download activity throughout the entire network during the selected **Time period**.

A column is displayed for each day when there was download activity. Each column indicates the volume of content downloaded over the WAN (in orange) or from peers (in grey). Hovering over a segment of the column will display the volume of content downloaded on that day.

This view demonstrates the value that Nomad and Delivery Optimization are providing through reduced WAN traffic. If the majority of content is being downloaded over the WAN, it could indicate that peers are simply not available (e.g. users working from home) or it could be an indication that Nomad or Delivery Optimization are not correctly configured to optimize content from peers.

The columns on this chart are not clickable, they are for data visualization only and do not navigate to another view of the data.

Tip

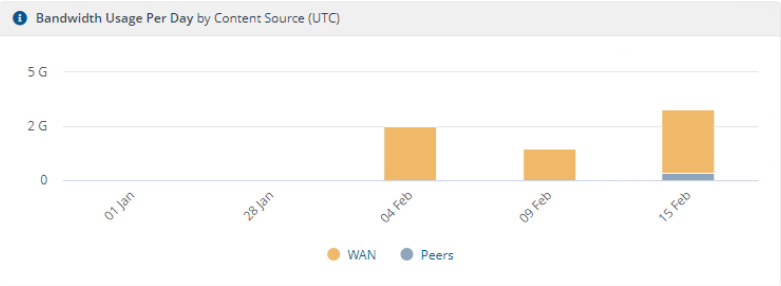
On the Overview page, when you select the **All Time** filter, the **Bandwidth Usage Per Day by Content Source (UTC)** graph displays a maximum 365 days of data.

Note

This chart only displays content that was downloaded over the network either from a peer or from the source (e.g. a CM Distribution Point), if a device:

Requests content that is already in its cache, it will not be represented in this chart

Only has some content in its cache and downloads the remainder of the content from peers or the source, the content that was downloaded will be shown.



9.4.4.1.4.5 P2P Efficiency by Content Source

The **P2P Efficiency by Content Source** tile represents the overall peer-to-peer efficiency across the entire network during the selected **Time period**.

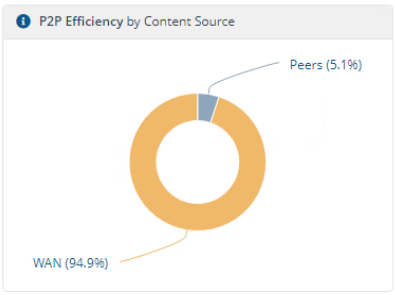
The data is grouped by source (Peers and WAN) and displayed as a donut chart showing the volume of content downloaded from peers (in grey) and from the source over the WAN (in orange). This gives an indication of the overall value of Nomad and Delivery Optimization across your organization.

Ideally, more content will be downloaded from peers than from the source over the WAN, which saves network bandwidth. Where this is not the case, it could be due to many users working remotely without any local peers, or it could be due to configuration settings on the client that are not optimized for peer-to-peer caching and availability.

This chart is not clickable, it is summary data visualization only and does not navigate to another view of the data.

Note

In this chart, the volume of content downloaded from peers includes any content requested by a device during the selected **Time period** and was already in the cache at the time (i.e. 'already cached' is represented as content obtained from a peer). If the content was downloaded from a peer or over the WAN during the selected **Time period**, it will be represented accordingly.



9.4.4.2 Nomad Download Pause

Nomad integrates with Tachyon to enable pausing or resuming Nomad downloads throughout the estate. This feature provides a safety measure for situations when a faulty or harmful deployment is made by mistake. In such situations, pausing Nomad downloads on all targeted devices can prevent or limit the potential damage.

It can also be used to facilitate troubleshooting, making it possible to pause all Nomad downloads across the network and enable IT teams to eliminate content distribution from their assessment of network bandwidth usage.

> **Note**
>
> Support for this feature was originally introduced in Tachyon 3.3 and requires the Tachyon client (Tachyon Agent or 1E Client) deployed to all the devices where you want the pause feature enabled.
>
> The latest version requires Tachyon Platform 8.x and a valid Tachyon license.

The Nomad Download Pause feature lets you immediately pause or resume current and future Nomad downloads at the press of a button. It is integrated directly into the Configuration Manager console and lets you select the collections you want to control. The feature works by pausing Nomad's job queue and effectively pauses all downloads on that agent and those added later, until the queue is resumed. Tachyon is used as the medium to send the pause and resume actions to the devices in the selected collection in real-time.

The feature is designed with a fail-safe in mind such that when a pause is triggered it is only active *for the next 24 hours*. After 24 hours, Nomad service automatically resumes the queue. This prevents the situation where a device receives a pause command but then fails to receive a corresponding resume command for an extended period due to network problems or because it is switched off.

> **Note**
>
> Refer to Using Nomad for example scenarios about how systems administrators use Nomad to deploy software, software updates and operating system upgrades, and how you can monitor those deployments using the Nomad app.

9.4.4.2.1 Installing Nomad Download Pause

To use the Nomad Download Pause feature, you will need to use the Nomad Branch Tools installer (**NomadBranchTools.msi**). For more details, refer to Installing Nomad Branch Tools.

9.4.4.2.1.1 Before you start

All users require the following permissions to install and use the Nomad Configuration Manager console extensions:

Local administrator rights on the computer – to install the console extensions

Configuration Manager console installed on the computer – to install and use the console extensions

Configuration Manager user with **Full Administrator** rights – to be able to use the Download Pause feature

Tachyon (or later) installed and working – you must know and enter the full URL for the Tachyon website in the installer.

The feature requires:

Tachyon Platform 8.x installed

Uploaded Tachyon instructions

Permissions allowing Configuration Manager (CM) administrators to execute the uploaded instructions.

These steps should be completed by a user that has Global Admin role in Tachyon, refer to Installing the Nomad app and 1E Content Distribution for details about Tachyon Platform setup, **Nomad Administrator** role and the 1E Nomad product pack.

Upgrading

If you are upgrading Nomad or Tachyon and you have previously installed **Nomad Download Pause** then you can continue using your existing setup, you do not need to do anything further, and you can ignore the information and steps below.

However, you are recommended to rename the old instruction set from**Nomad Core Instructions**to**1E Nomad**to match the name used in the steps below for new installations. The renamed set will retain the permissions you previously configured.

Prior to Nomad 7.0.200, you were advised *not* to change the name of the instruction set. This was because the **NomadBranchAdminUIExt.msi** installer uploaded the instructions into an instruction set named **Nomad Core Instructions**. From version 7.0.200 onwards, this restriction no longer applies, because the instructions are no longer in the installer, and instead are only available in the **1E-Nomad** product pack.

The installation steps below use the Settings app to create the **1E Nomad** instruction set and upload instructions for a new installation. However, if you instead use the **Tachyon Product Pack Deployment Tool** to upload the **1E Nomad** product pack, the tool will create an instruction set called **1E Nomad** and place *new* instructions there. If the instruction set **Nomad Core Instructions** has not been renamed, any *existing* instructions in it will remain or be updated if they are new versions. You may end up with two instruction sets. You can keep both sets, or you can do the following, which will retain the permissions you previously configured:

move the new instructions from **1E Nomad** to **Nomad Core Instructions**

delete the now empty instruction set **1E Nomad**

rename the old instruction set from **Nomad Core Instructions** to **1E Nomad**

The **1E-Nomad** product pack is provided in the Tachyon Platform download zip, and includes new versions of the same instructions. A list of these instructions is provided below under the heading 1E-Nomad product pack, which include the two instructions required by Nomad Download Pause.

9.4.4.2.1.2 Installing Nomad Branch Tools

The following steps describe how to run the Nomad Branch Tools installer interactively, for more details and how to install from the command line, refer to Installing Nomad Branch Tools.

9.4.4.2.1.3 Installing interactively

Note

You can download the 1E Content Distribution Tools from the **Releases** page for your platform version at https://support.1e.com/.

Install Nomad Branch Tools on the same device as the Configuration Manager Console, you can do this is done by running **NomadBranchTools.msi** from an elevated command prompt.

Note

The Configuration Manager Console must not be running when you run **NomadBranchTools.msi**

To install, start a Command Prompt with elevated rights, navigate to the location where you extracted **NomadBranchTools.msi** and run it with the following command-line:

```
> msiexec /i NomadBranchTools.msi /l*v NomadBranchInstall.log REBOOT=REALLYSUPPRESS
```

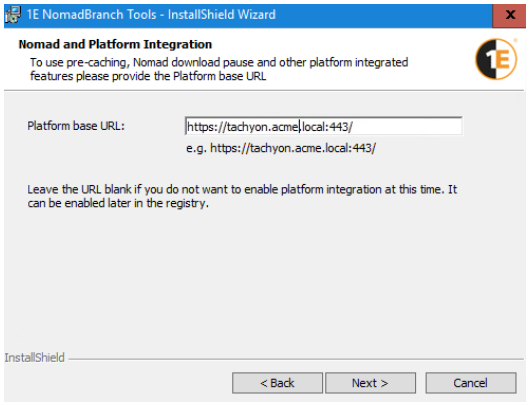
9.4.4.2.1.3.1 Nomad and Platform Integration

Note

Before installing this feature, please refer to Nomad Download Pause, for steps on configuring the prerequisites.

You need to supply the root URL to the Tachyon API. Which will be in the form: **https://<Tachyon DNS Alias FQDN>** using the Tachyon DNS Alias FQDN defined when you installed Tachyon.

For example if you installed Tachyon using **tachyon.acme.local** as the DNS Alias FQDN then the Tachyon API Root URL should be set to:



`https://tachyon.acme.local`

Note

The Tachyon API is Tachyon's Consumer API. You can learn more about Tachyon in Introducing Tachyon.

Note

From Nomad 8.1 there is support for providing alternate credentials to authenticate with the Tachyon Platform. If your Tachyon Platform instance resides in another domain or the cloud, you will be prompted to enter alternate credentials for that location, which get stored in the credential store for any future requests.

Click **Next** to continue.

9.4.4.2.2 Confirming Nomad Download Pause installation

It is good practice to confirm the installation of the **Nomad Download Pause** components in both Tachyon and Configuration Manager (CM).

9.4.4.2.2.1 Confirm the installation in Tachyon

Logon to Tachyon Platform as a user with at least **Consumer Administrators, Instruction Set Administrators** and **Permissions Administrators** roles and click the **Settings** app from the Tachyon Portal

On the **Consumers** page check the following:

A consumer with the name **Nomad** is already listed.

Note

This consumer name will have been registered already by one of the following methods:

installation of the **Nomad Configuration Manager console extensions,** if the installation account had the correct Tachyon user permissions

a previous installation of **Nomad Configuration Manager console extensions**

installation of the **Nomad app** and **Content Distribution** by Tachyon Setup

On the **Instruction→Instructions sets** page check the following:

A **1E Nomad** instruction set exists, and contains the following two instructions:

Pause the Nomad job queue for <PauseDurationMinutes> minutes

Resume the paused Nomad job queue.

On the **Permissions** page check the following:

On the **Roles** tab check that the **Nomad Administrators** role has been created with **Actioner** permissions on the **1E Nomad** set.

Click on the **Nomad Administrators**→**Management Groups** tab, and click on the **Add** button. Select **All Devices** in the **Add management group** popup, and then click **Add**.

> **Note**
>
> If other management groups are selected instead, then members of this role can only use the instructions on devices belonging to those management groups.

On the **Permissions**→**Users** tab check that all Configuration Manager users and groups that have the **"Full Administrator"** role have been added to Tachyon as users.

> **Note**
>
> You may remove users if you know they do not require Tachyon permissions. However, they will be re-added the next time the installer is run, and the installation account has permissions to add users.
>
> You may add additional users and groups manually.

Select each of the added Configuration Manager users in turn and check that they have the **Nomad Administrators** role added.

> **Note**
>
> These permissions ensure all current CM **"Full Administrators"** are able to use the **Nomad Download Pause** feature by allowing them to execute the Tachyon instructions. Any other users or groups will need to be manually added to the **Nomad Admins** role.

9.4.4.2.2.2 Confirm the installation in Configuration Manager

On the **Administration Client Settings** page, check the following:

Right-click on **Default Client Settings** and check that a **1E Nomad** sub-menu has been added to the context menu, containing a **Nomad Properties** menu item

On the **Assets and Compliance**→**Device Collections** page, check the following:

Two Nomad related buttons have been added to the **Home** ribbon:

Pause Nomad Downloads

Resume Nomad Downloads

If all these checks have passed, you should have a working installation of the Nomad Download Pause feature.

9.4.4.2.3 Using Nomad Download Pause

9.4.4.2.3.1 Pausing Nomad downloads

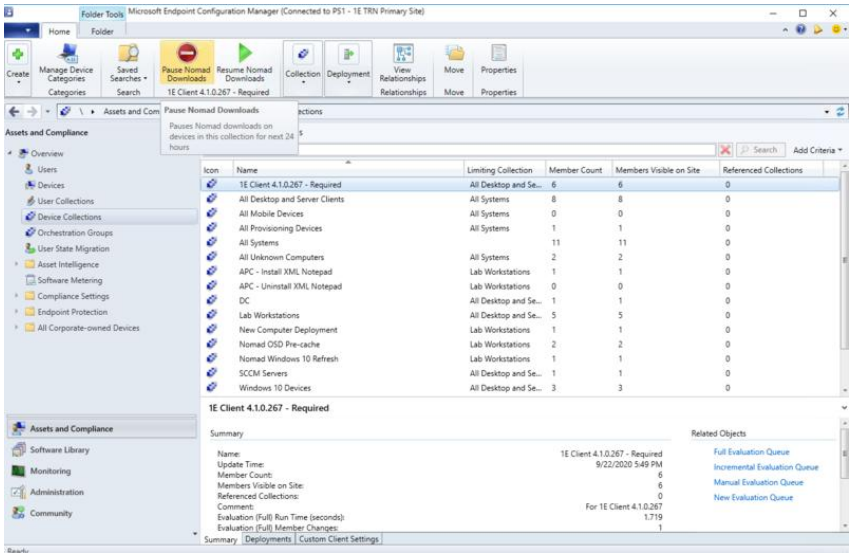
The Nomad Download Pause feature can be applied to a collection of devices. To do this:

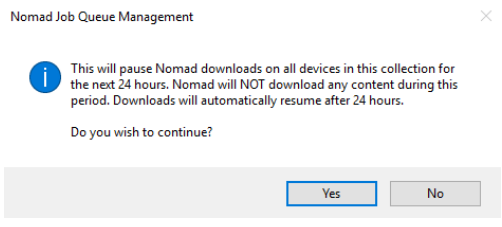
Select the collection you want and click the **Pause Nomad Downloads** button or select the **Pause Nomad Downloads** menu item from the collection's right-click context menu.

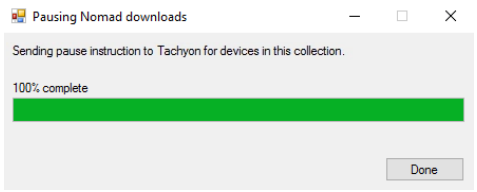
A **Nomad Job Queue Management** dialog will appear asking explaining the consequences of continuing. If you want to continue. Click **Yes** to proceed and **No** to cancel.

If you click **Yes**, a **Pausing Nomad downloads** dialog will appear showing the progress of the process. This should reach 100% with no errors, at this point click **Done** to close the dialog.

When applied, the Nomad downloads on the selected collection will be paused for a period of 24 hours - after which they will resume automatically.







9.4.4.2.3.2 Checking paused collections in Configuration Manager

When a collection has been successfully paused an entry will appear on the **Monitoring→1E Nomad→Paused Collections** page, as shown in the picture opposite.

From here you can view the following information:

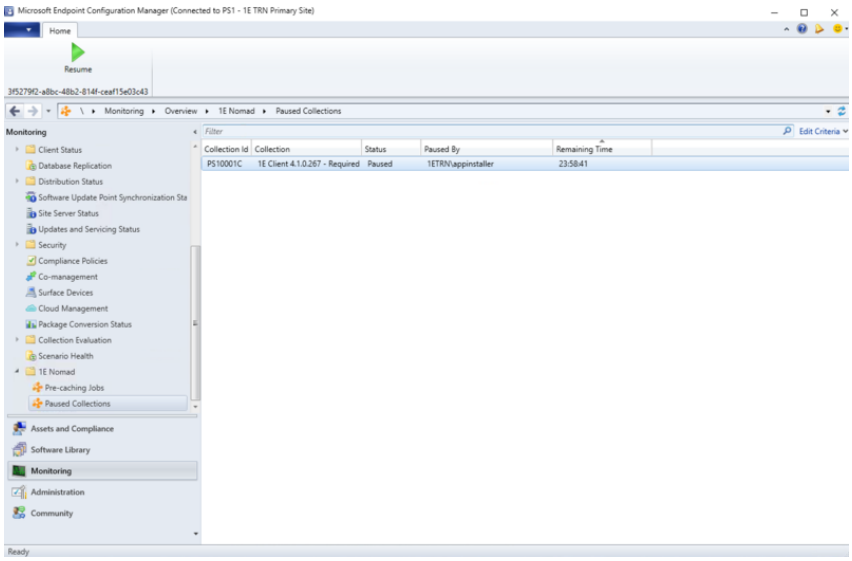
Column	Description
Collection Id	The Configuration Manager ID for the device collection
Collection	The friendly name of the device collection
Status	The current paused status for the collection. The values in this column can show one of two states:

State	Description
Paused	This state indicates that all the devices in the collection have been paused.
Partially Paused	This state indicates that some but not all the devices in the collection have been paused. This may happen if some devices in the collection are currently offline or the pause action is interrupted while Nomad is sending the instruction request to Tachyon.

Remaining Time	This column shows the time remaining for the pause to be in effect. After the stated time the devices in the collection will automatically resume their Nomad job queues.

From this page you can also select to resume the paused collection by clicking on the **Resume** button or by selecting the **Resume** menu item from the collection's right-click context menu.

As soon as the Nomad job queue for the entire collection has been resumed the entry will disappear from the **Monitoring→1E Nomad→Paused Collections** page.



9.4.4.2.3.3 Checking the Pause instruction in Tachyon

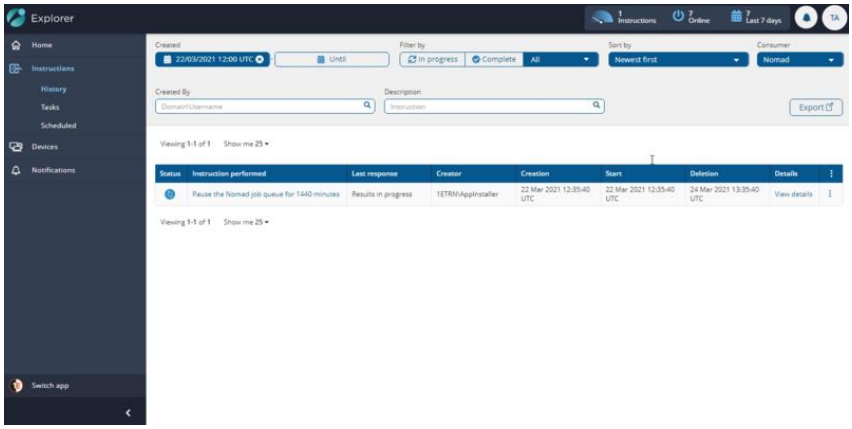
You can check the progress of the pause process by looking at the instruction history in Tachyon:

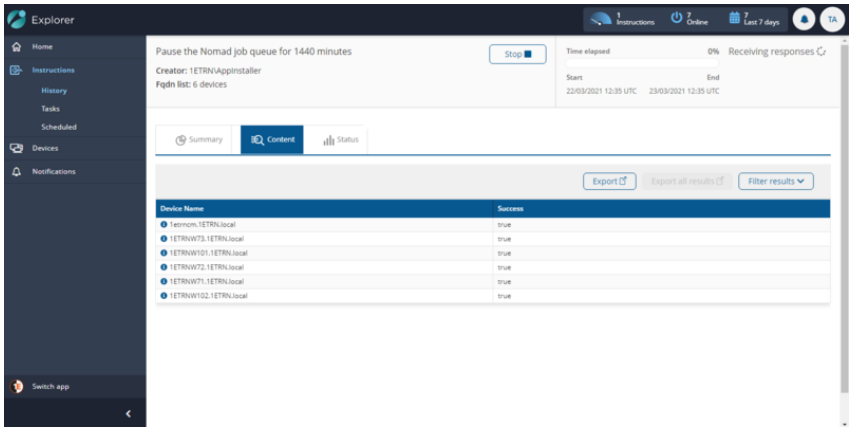
Log onto Tachyon using an account which has full Configuration Manager administrator access.

Navigate to **Explorer→Instructions→History**, in the example shown we have filtered the **Consumer** to only show results related to **Nomad**.

You should see an entry for the **Pause the Nomad job queue for 1440 minutes** instruction.

Clicking on the instruction shows a detailed breakdown of the response from each device in the selected collection.





9.4.4.2.3.4 Resuming Nomad downloads

If you want to resume the Nomad downloads for a collection at any time during the 24 hours, you can

Select the collection you want and click the **Resume Nomad downloads** button.

A **Nomad Job Queue Management** dialog will appear asking explaining the consequences of continuing. If you want to continue. Click **Yes** to proceed and **No** to cancel.

If you click **Yes**, a **Resuming Nomad downloads** dialog will appear showing the progress of the process. This should reach 100% with no errors, at this point click **Done** to close the dialog.

When applied, the Nomad downloads on the selected collection will be immediately resumed from where they left off.

As soon as the Nomad job queue for the collection has been resumed the paused collection entry will also disappear from the **Monitoring 1E Nomad, Paused Collections** page.

9.4.4.2.3.5 Checking the Resume instruction in Tachyon Platform

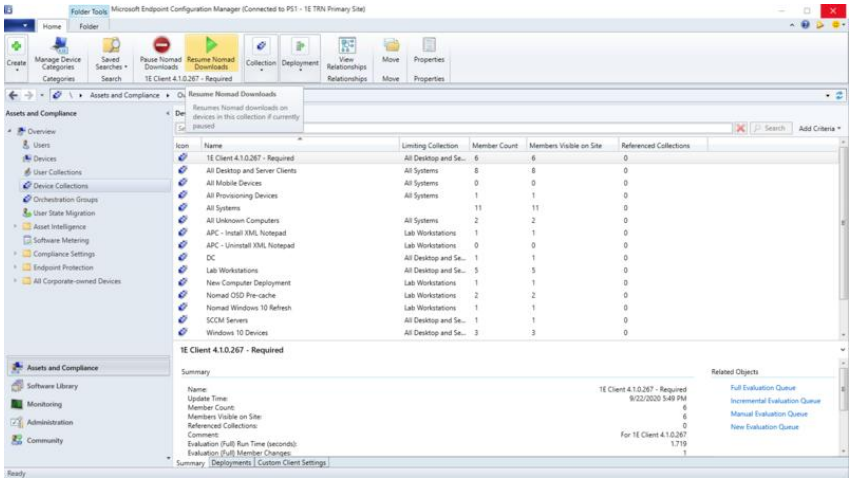
You can check the progress of the resume process by looking at the instruction history in Tachyon, using the same steps as Checking the Pause instruction in Tachyon:

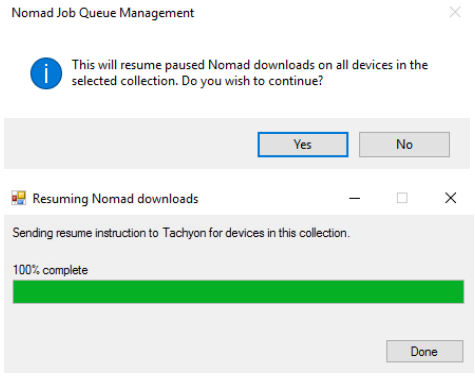
Log onto Tachyon using an account which has full Configuration Manager administrator access.

Navigate to **Explorer→Instructions→History**, in the example shown we have filtered the Consumer to only show results related to Nomad.

You should see an entry for the **Resume the paused Nomad job queue** instruction.

Clicking on the instruction shows a detailed breakdown of the response from each device in the selected collection.





9.4.4.2.4 Troubleshooting

A typical error that can occur during the pause or resume process is if any of the devices in the selected collection do not have the 1E Clients installed. You can fix this by installing the 1E Client on all devices in the collection, refer to Installing the 1E Client for Nomad for details.

9.4.4.2.5 1E-Nomad product pack

This product pack is used to create the **1E Nomad** instruction set required by the Download Pause feature.

Instruction text (ReadablePayload)	Type	Description	Instruction file name	Version
Pause the Nomad job queue for <PauseDurationMinutes> minutes	Action	Pause Nomad job queue. Required by **Nomad Download Pause** feature.	**1E-Nomad-PauseNomadJobQueue.xml**	15
Resume the paused Nomad job queue	Action	Resume paused Nomad job queue. Required by	**1E-Nomad-ResumeNomadJobQueue.xml**	12

Instruction text (ReadablePayload)	Type	Description	Instruction file name	Version
		Nomad Download Pause feature.		

9.4.5 Client Health

The purpose of Client Health is to ensure the success of your Content Distribution deployments.

The Client Health page of the Nomad app shows rule status and device status from two Guaranteed State policies.

Nomad Client Health

MEMCM Client Health.

You can also use Guaranteed State's Windows Client Health policy.

9.4.5.1 Nomad Client Health

Nomad is included as part of the 1E Client, and as part of that integration, we offer a Nomad client health compliance policy in Guaranteed State. This verifies common Nomad requirements such as ACP registration, disk availability, firewall exceptions, crash notifications and cache monitoring.

The Nomad client health policy replaces the client health tile in the Nomad dashboard, plus additional remediation steps:

Keeps content distribution services up and running on Nomad clients, so that users are secure and productive

Ensures Alternative Content Provider (ACP) registration configuration is set

Maintains optimal disk availability and monitors cache size for storage capacity planning

Enforces Firewall exceptions.

For full details, refer to Nomad Client Health Policy.

> **Note**
>
> This policy is intended for deployment to Windows devices only.

9.4.5.2 MEMCM Client Health

Many businesses rely on Microsoft Endpoint Configuration Manager (MECM) to deploy software, patches and updates across their company networks. It is crucial that Configuration Manager is working effectively. Configuration Manager is part of the Microsoft Endpoint Management suite and is often referred to as MEMCM as well as MECM.

The MEMCM Client Health policy monitors Configuration Manager client health and performance. It checks for cache availability, inventory cycles, service availability and Configuration Manager WMI integrity - common causes of Configuration Manager client problems on devices.

The MEMCM Client Health policy replaces the previous SCCM Client Health policy and covers the following:

Ensure the correct version of the CM client is installed and running and assigned to the correct site

Ensure the CM client is not stuck in provisioning mode

Ensure that heartbeat discovery, inventory and state messages are being sent regularly

Ensures the CM client cache is set to the correct size

Ensure the CM client log settings are correct

Ensure the BITS service exists, is configured to start up automatically and is running

Ensure the Windows Time service exists with the correct startup settings

Ensure the Windows Management Instrumentation (WMI) service exists, is configured to start automatically and is running

Ensure WMI is healthy, the core CIMv2 and ccm namespaces and classes exist and that the WMI repository is consistent

Ensure the Windows Update service exists with correct startup settings, is configured to use the correct source (CM, WSUS or Microsoft Update) and that the service can connect to the source.

For full details, refer to MEMCM Client Health Policy.

Note

This policy is intended for deployment to Windows devices only.

9.4.5.3 Windows Client Health

Over time Windows devices can develop performance problems related to device or service availability. This policy verifies the available storage capacity on devices, notifies of application crashes, monitors WMI health and service function, and also checks the behavior of core Windows services.

The Windows client health policy covers all of the following:

Manages Windows devices and service availability performance problems

Safeguards disk space integrity, ensuring sufficient storage capacity

Ensures optimum performance of the Configuration Manager client and that WMI is active and integrated

Notifies of application crashes and remediation assists. Investigates root cause for specific issues.

For full details, refer to Windows Client Health Policy.

Note

This policy is intended for deployment to Windows devices only.

9.5 Troubleshooting

A general methodology for investigating issues as well as identifying key issues and their resolutions.

9.5.1 1E Support contact details

9.5.1.1 Support Web portal

Maintenance support customers can log onto the 1E Support Web Portal at https://support.1e.com/ using the login details provided with their maintenance contract. This provides issue tracking, product hotfixes, and knowledge base articles related to each product.

9.5.1.2 Telephone support

Maintenance support customers can contact the technical support department at 1E through the following support numbers for the US and UK. Just phone the relevant number for your area and use the support code provided with your maintenance contract to get your call routed quickly and efficiently to the correct support group:

US: 1-866-349-4032

UK: 0208 326 3499

9.5.1.3 Email support

Maintenance customers can use the following email for additional support. Evaluation customers can also use this email with the temporary access code that is provided through customercare@1e.com as part of their evaluation:

support@1e.com

9.5.2 The technical support process

Read through the issue pages in the Nomad Troubleshooting section to see if there are any quick resolutions to any problems you may have encountered. After that, if you are still encountering problems, you should create a technical report and then contact the 1E technical support team.

The process of getting the issue to 1E support should be as follows:

Gather all the information relevant to the issue and create a technical report, see heading below.

Maintenance customers contact 1E via the online support portal, using the log-in provided at purchase.

Maintenance customers follow up with emails using their case support number and evaluators contact 1E via the following email address: support@1e.com.

Further follow up via phone to the technical support department at 1E at the following numbers for the US and UK Just phone the relevant number for your area and use your case number and support access code to get your call routed quickly and efficiently to the correct support group:

US: 1-866-349-4032

UK: 0208 326 3499

9.5.2.1 Creating a technical report

To help determine the cause of technical problems Nomad and associated products keep a number of log files that report on the behavior of each component. These can be found under %PROGRAMDATA%\1E\Nomadbranch.

The technical report should also contain the following information:

Version number of Nomad

The OS, version number and patch level of the Tachyon Platform that Nomad is installed on.

You should then email the details of the problem encountered along with the above information to support@1e.com and a technical consultant will contact you to help find a suitable solution.

9.5.3 The technical support process

Read through the Troubleshooting pages to see if there are known issues, or quick resolutions to any problems you may have encountered.

Maintenance support customers can use the 1E Support Web Portal to review knowledge base articles and download hotfixes.

If still encountering problems, create a technical report (log files and details) and then contact the 1E technical support team.

9.5.3.1 Creating a technical report

If possible, please obtain the following details and log files before contacting 1E, to include in your technical report.

9.5.3.1.1 Version details

The OS, version number, and patch level for:

Tachyon Servers

1E Client

Configuration Manager - if used

Other 1E Server software, for example, Shopping, Nightwatchman, and WakeUp.

For Nomad and Shopping, please provide OS, version number, and patch level for:

Configuration Manager DPs

Nomad extensions used on Configuration Manager Consoles

ActiveEfficiency Server.

9.5.3.1.2 Environmental details

If there were any recent changes made to your configuration

The name of the machines, Configuration Manager Application and/or Package IDs for when the issue occurred

9.5.3.1.3 Problem details

When did the issue occur, ensure log files cover this period

The scope of the issue – did it affect a particular geographical location, group of users, or client machines

Details of any self-help troubleshooting steps you carried out

In the event of a service crash or if you are experiencing high CPU or memory usage, provide us with the dump file, event viewer logs, and traces. We will provide you with FTP details to upload these files.

9.5.4 Log files

1E needs details of the recorded time when the issue took place. To ensure logs contain relevant details, please try to rerun the steps to replicate the issue. The table below details the log files we require:

The default location for all Nomad logs is the folder *%ALLUSERSPROFILE%\1E*

For issues relating to	Required log files	Location of log files
1E Client	*1E.Client.log* *NomadBranchUninstall-YYY-MM-DDThh_mm_ss_000Z.log*	Default location: %ALLUSERSPROFILE%\1E\Client\
Nomad client	*NomadBranch.log*	Default location: %ALLUSERSPROFILE%\1E\NomadBranch\ Optional location if installed using 1E Client Deployment Assistant (CDA): C:\WINDOWS\CCM\Logs\
OS deployment	*NomadPackageLocator.log* *NBCacheActions.log* All Configuration Manager logs including *SMSTS.log*	The path changes at the different stages of an OS deployment.

For issues relating to	Required log files	Location of log files
Nomad and ContentDistribution integration	*ContentDistribution.log*	%ALLUSERSPROFILE%\1E\ContentDistribution\
Delivery Optimization monitoring and reporting	*NomadBranch.DO.log*	Default location: %ALLUSERSPROFILE%\1E\NomadBranch\ NomadBranch.DO.log is created when Delivery Optimization monitoring and reporting are enabled using the DeliveryOptimizationReportingEnabled registry value.

9.5.5 Known issues

Lists of the current known issues when installing Nomad and using the Nomad features.

9.5.5.1 Installing 1E Client

Issues	Description	Workaround
1E Client installer adds Nomad registry settings even when Nomad module is NOT enabled while installation. If someone deletes those registry settings and enables Nomad module later, Nomad won't function right.	The installer is currently creating the majority of Nomad registry values because the service doesn't create them all and Nomad doesn't tolerate the absence of all the settings that the service doesn't create. If someone deletes those settings and enables Nomad module later, Nomad won't function right.	In such a scenario, we recommend reinstalling the 1E Client with a new set of properties / transform that enables the Nomad module. This will be fixed in a future release of 1E Client.
On Windows XP, 1E.Client.log displays a warning "Unsupported OS	Nomad is not support on Windows XP therefore when 1E Client is installed with Nomad module, the	None.

Issues	Description	Workaround
version. Will not install Nomad." however the very next log lists that "Module 'Nomad' has been installed".	module is not enabled, and the Nomad Branch service is not installed.	
Nomad may be downgraded by active Application deployments in CM, which may cause issues with behaviour of the 1E Client Nomad module.	If there is an active Application deployment in CM of an earlier version of Nomad, clients that have been upgraded with the 1E Client with the Nomad module enabled may be downgraded when the Application Enforcement cycle runs. In this scenario, if the 1E Nomad module is subsequently disabled in the 1E Client, the Nomad service will be removed. This is because once the Nomad module has been enabled, it is not aware nor does it check for older versions. If the Nomad module is subsequently disabled, the service is removed as the Nomad module believes it is not longer required.	To avoid this situation, always define Application Supersedence on the 1E Client Application such that it supersedes any Applications that install previous versions of Nomad (and the 1E Client when introducing new versions of the 1E Client). To resolve this issue should it occur, first address the Application Supersedence to prevent it from recurring. Then run the following command from the 1E Client installation directory on the affected devices. *1E.Client.exe -reconfigure MODULE.NOMAD.ENABLED=false -restart & 1E.Client.exe -reconfigure MODULE.NOMAD.ENABLED=true -restart* This will disable the Nomad module and remove the Nomad service, then re-enable the Nomad module, which will in turn uninstall the earlier version of Nomad and install the Nomad module. The settings defined by the earlier Nomad install will be migrated - these may differ from the settings with which the Nomad module was initially configured with.
1E Nomad Branch and 1E Client Health services may be stopped if upgrading to Nomad 8.0 if previous version of Nomad installer is no	The 1E Client installer stops the 1E Nomad Branch and 1E Client Health services if the Nomad module is enabled. The 1E Client installation completes	In this scenario, to immediately restore Nomad functionality simply start the services. To fix completely you will need to remediate the installer source for the old version of Nomad on the affected client, then run the following command from the

Issues	Description	Workaround
longer in source folder or the Windows Installer cache.	successfully, after which the Nomad module attempts to uninstall the older version of Nomad. The uninstallation fails as Windows Installer cannot find the original source installer. The Nomad module is not enabled and the Nomad and Client Health services remains stopped.	1E Client installation directory to restart the 1EClient service. *1E.Client.exe -restart*
Uninstalling 1E Client doesn't delete Nomad's P2P server certificate.	When P2PEnabled value was set to 79 then NomadBranch server certificate does not get deleted after uninstallation.	
NomadBranch - 1EClient - Creation of Nomad COM object failed with 0x80070424	Install the latest build with Nomad. Creation of Nomad COM object failed with 0x80070424-	Disable the Nomad module and restart the 1E Client service. Enable Nomad again and restart the 1E Client service. Nomad should install successfully.
Nomad users see the 1E Client UI in the device system tray even when the Tachyon module is not enabled.	The 1E Client UI runs despite only the Nomad or Shopping modules being installed, without the Tachyon feature enabled.	None.

9.5.5.2 Working with Nomad

Issues	Description	Workaround
Nomad crashes while downloading an application in original content having source path greater than 290 length.	When the source path of an application is longer than 290 chars and Nomad starts downloading	Use Nomad SECure when a package has source path greater than 255 characters in length. Compressing and/or

Issues	Description	Workaround
	application in original format (that is format 0) then Nomad crashes in between but successfully downloads the content and passes the hash check as well.	encrypting content results in a single file which the possibility of an overly long path.
PBA find will fail if P2PEnabled registry changes on host machine	After PBA capture when data is sent to host over https, pause the task sequence and change the value of P2PEnabled=9 on the host machine. On resuming task sequence would get failed.	None. This is as per design and so is not suggested to change the value of P2PEnabled in between.
Installer log file may not be launched after installation	In Windows Server 2019 when installation was initiated by the Built-in Domain Administrator and "Show the Windows Install log" option was selected after installation then log file does not get launched. However it works with other admin users.	Initiate the installation from elevated command prompt using /l*v properties to generate the log file, for example: *msiexec /i <installer.msi> /l*v <filename.log>*
By default NomadBranchGui is upgraded into Basic mode	If previous version was setup in the Advanced mode and user upgrades it to the latest release then it does not recognize the previous setup mode and so gets upgraded	Reinstall NomadBranchGui.

Issues	Description	Workaround
	into Basic mode by default.	
Nomad is not able to download from CCMTOKENAUTH_SMS_DP_SMSPKG$ co ntent location virtual directory on Distribution Point, which is created when Distribution Point is configured to communicate over HTTPS starting CM CB 1810.	Enhanced HTTP was first introduced in CM1806 as a pre-release feature and it became a standard feature in CM1810. It allows administrators to use secure communication between clients and DP without the need for PKI-generated certificates or a Network Access Account. Nomad currently can't use the new Enhanced HTTP features when downloading from the DP, but it will continue to work when there are still Network Access Accounts available to allow it to authenticate non-Domain joined machines (such as those in WinPE and Workgroup machines).	None. We are working with Microsoft to determine the best approach to enabling download from the Enhanced HTTP virtual directory. You can upvote our request at https://aka.ms/AA63jc3
Nomad download halts for some time if block size is different on a machine acting as a master.	Nomad may not be able to download whole content from the master and stuck in a loop for some time if the master has incomplete content	None.

Issues	Description	Workaround
	and different block size.	
Different block sizes on DP and Clients may leads to RDC failure.	RDC may not work properly if distribution point and client has different block size.	To fix this, have same block size on all Distribution Points and clients.
Nomad would fail to download content when client switches from Intranet to Internet DP having higher content version.	Nomad may fail to download the content when switching from Intranet to Internet DP and Internet DP has higher version of content than required.	None.
Nomad fails to use already precached content in secure format even if same content is requested in original format.	Nomad won't convert the secure format content into the original format on the client side and downloads the content again.	None.
Nomad settings on Configuration Manager client policies don't replicate between CAS and primaries	Nomad settings do not replicate between CAS and Primary site, the user has to manually do settings on both the sites.	Change the settings manually on both sites.
Nomad won't handle SUSPEND by CM when in PauseJobQueue state	When Nomad JobQueue is paused using Download Pause and during the pause if CM sends suspend for a job then Nomad won't honor that instruction and would continue to run that	None.

Issues	Description	Workaround
	job once JobQueue resume.	
NomadBranch GUI does not work when File sharing is connected with Remote machine	When NomadBranch GUI is installed on machine and connected to remote machine then it may not show any download progress and remains in paused state.	None.
NomadAdminUIExtension always give "stopped working" error but installs successfully on Windows Server 2012.	Installing NomadAdminUIExtension on Windows Server 2012 would give error "stopped working" however installs successfully.	Ignore the error message and click OK.
Incorrect protocol status download reported in the *NomadBranch.Log* for SMB downloads in SSD	The *NomadBranch.Log* erroneously logs a SMB download as SM_HTTP over SSD.	Ignore the error message.
The correct installer may not be picked up by the Install 1E Client custom task sequence action if there are multiple installers in the content source for the Nomad package.	The Install 1E Client custom task sequence action randomly selects a Nomad MSI if there are multiple installers in the content source for the Nomad package.	We recommend having only one installer in the Nomad package source.
Job fails if disk space is low when compress/encrypted content is uncompressed.	For compressed/encrypted content, Nomad reserves disk space equivalent to size of compressed/encrypted content only before	None.

Issues	Description	Workaround
	download. When disk space is low the, job will fail when it uncompresses the content in the Configuration Manager cache.	
Status messages are not sent when Nomad runs in WinPE mode.	When Nomad is installed in WinPE and starts downloading packages, send status messages are not sent to CM server as it does not have Configuration Manager client.	None.
Peer-to-peer transfer fails if one of the machine name is longer than 50 characters.	When on a subnet, machine1 has hostname longer than 50 characters with content A, and machine2 requests content A, P2P transfer fails and content will be downloaded from DP.	Do not use hostnames longer than 50 characters. https://support.microsoft.com/en-us/help/909264/naming-conventions-in-active-directory-for-computers-domains-sites-and
Attempting to downgrade nomad using Configuration Manager puts the machine in such a state that any further upgrades would fail.	When a downgrade is attempted using a ConfigMgr job, the rollback doesn't happen cleanly and a few traces are left in the system leading to failure in future upgrades.	To fix this, please contact 1E support.
Log files may contain a large number of error messages if a mixture of encryption	It is possible to configure different installations of Nomad to use different	You should ensure that all the installations of Nomad

Issues	Description	Workaround
methods is used for Nomad communications.	encryption methods. Nomad 6.0 supports two options: the default encryption method and a new FIPs compliant encryption method. The error messages in the log files indicate that Nomad communications are being impacted and the fault should be rectified. This state is liable to occur if hybrid installations are allowed with unsupported versions of Nomad, because encryption is required in Nomad 6.0 owards.	are set to the same encryption method.
Clients may not be able to download content using HTTP/HTTPS from the Distribution Point if the content URL contains hidden segments or double-escape sequences.	This issue is specific to Distribution Points running IIS 7.0 and above and may occur when the requested content URLs contain hidden segments or double-escape sequences. When this happens the client displays HTTP error 404.8 (Hidden Namespace) and 404.11 (Double Escaping) in the NomadBranch.log file while processing the content.	Modify the IIS Request Filtering settings on the DP to allow download of such content. Please refer to Post-installation tasks#installationtasks-IISrequestfiltering.

Issues	Description	Workaround
Using Nomad on multihomed machines results in extraneous network traffic.		Please contact 1E Support for a detailed workaround if you have multihomed machines in your environment.
Disk Full error retries with Configuration Manager Client	If the Nomad job returns with the error Disk Full, the Configuration Manager Advanced Client regards this as a non-fatal error and will retry the deployment on a scheduled basis.	None. This is by design.
Nomad Provider Settings overwrite Third party Provider settings in Task Sequences	When making changes to Nomad Properties for a Task Sequence the settings are written to all the Task Sequence's reference Packages. This does not take into account any third party configurations that may already be in place.	To avoid this you should set Nomad Provider settings for each of the reference Packages individually.
Nomad encounters problems when WebDAV is used to connect to a server.	Use of WebDAV is not supported by Nomad. WebDAV may be present because older versions of Configuration Manager required it, but not any longer.	None. Remove WebDAV from the server.

Issues	Description	Workaround
Uninstalling and reinstalling Nomad results in unverified cached data.	When uninstalling Nomad, cache content is not deleted as files may still be required (for example for Windows Installer repairs). If you subsequently reinstall Nomad on the same machine, Nomad will enumerate the existing cache and will be aware that it has cached content for certain packages. It is not possible to verify that the package content has not been altered in the interim period, therefore these are referred to as zombie packages i.e. they have returned from the dead. The Nomad client will be able to participate in elections for zombie packages, but will only win an election if other machines do not have verified content. This ensures minimum WAN utilization. Prior to execution, package content is verified by Configuration Manager.	To manually force verification of the cache after upgrading Nomad or uninstalling and reinstalling Nomad, please use the command: `NomadBranch.exe -activateall` If you wish to delete cache content, please use the CacheCleaner.exe utility prior to uninstall.
Nomad fails to download the content, which has one or more empty file (of	In this case, Nomad gets stuck in a loop and won't be able to	None.

Issues	Description	Workaround
zero file size), from a cloud distribution point.	download the content from cloud distribution point due to blocks mismatch errors.	

9.5.5.3 Configuration Manager

Issues	Description	Workaround
User cannot go back to Configuration Type page in the Create Nomad Baseline Wizard.	If user moves forward with 'Configure settings using MSI Transform' option then he cannot go back to Configuration Type page in the Create Nomad Baseline Wizard without selecting MSI and MST files. A popup would be displayed with message: *Please use valid MSI and MST files*.	Start again.
The Nomad Content Pause feature is not visible in the Configuration Manager console after upgrading the Nomad Admin UI extensions.	The page: **Installing the Configuration Manager console extensions** was not found. Please check/update the page name used in the 'multiexcerpt-include' macro.	You will need to ensure that this checkbox is checked in the installation wizard or that the **ENABLETACHYONINTG=true** installer property is set on the installer command-line if you want the Nomad Download Pause feature to work.

Issues	Description	Workaround
The Nomad Content Pause feature is not working after installation.	If the site server does not have a local SMS Provider, the Nomad Branch Admin UI Ext installer does not create the Nomad Custom Role, required Instruction set and add the Nomad Core instructions in Tachyon.	The feature requires: Tachyon Platform 8.x installed Uploaded Tachyon instructions Permissions allowing Configuration Manager (CM) administrators to execute the uploaded instructions. These steps should be completed by a user that has Global Admin role in Tachyon, refer to Installing the Nomad app and 1E Content Distribution for details about Tachyon Platform setup, **Nomad Administrator** role and the 1E Nomad product pack. **Upgrading** If you are upgrading Nomad or Tachyon and you have previously installed **Nomad Download Pause** then you can continue using your existing setup, you do not need to do anything further, and you can ignore the information and steps below. However, you are recommended to rename the old instruction set from**Nomad Core Instruction s**to**1E Nomad**to match the name used in the steps below for new installations. The renamed set will retain the permissions you previously configured. Prior to Nomad 7.0.200, you were advised *not* to change the name of the instruction

Issues	Description	Workaround
		set. This was because the **NomadBranchAdminUIExt.msi** installer uploaded the instructions into an instruction set named **Nomad Core Instructions**. From version 7.0.200 onwards, this restriction no longer applies, because the instructions are no longer in the installer, and instead are only available in the **1E-Nomad** product pack. The installation steps below use the Settings app to create the **1E Nomad** instruction set and upload instructions for a new installation. However, if you instead use the **Tachyon Product Pack Deployment Tool** to upload the **1E Nomad** product pack, the tool will create an instruction set called **1E Nomad** and place *new* instructions there. If the instruction set **Nomad Core Instructions** has not been renamed, any *existing* instructions in it will remain or be updated if they are new versions. You may end up with two instruction sets. You can keep both sets, or you can do the following, which will retain the permissions you previously configured: move the new instructions from **1E Nomad** to **Nomad Core Instructions**

Issues	Description	Workaround
		delete the now empty instruction set **1E Nomad** rename the old instruction set from **Nomad Core Instructions** to **1E Nomad** The **1E-Nomad** product pack is provided in the Tachyon Platform download zip, and includes new versions of the same instructions. A list of these instructions is provided below under the heading 1E-Nomad product pack, which include the two instructions required by Nomad Download Pause.
Dynamic packages in Task Sequences sometimes remain in Installing state.	When SMSTSNomad is used to download Dynamic Packages, through using the Set Nomad as Download Program action in a Task Sequence, they may remain in Installing state.	
Download using Nomad during a Task Sequence occasionally reverts to using the default Configuration Manager	When SMSTSNomad is used in a Task Sequence by using the Set Nomad as Download Program action, certain error conditions that would normally be translated to success codes by the list held in the SuccessCodes registry value are instead being returned as failures, thereby causing Configuration Manager to revert to the use of BITS for the transfer when those errors occur.	

Issues	Description	Workaround
download process.		
Task Sequence downloads may failover to using the default Configuration Manager download process if any errors occur during the Nomad download.	Due to a problem in Configuration Manager the Always return success option in the Set Nomad as Download Program action is not working. This means that downloads may failover to using the default Configuration Manager download process.	You will need to regularly check the Nomad logs to check that this is not occurring in order to address any issues that may have arisen.
The Nomad properties dialog in the Configuration Manager console does not save changed values when focus moves to	Where the Nomad Admin UI extensions are installed, in any of the dialogs in the Configuration Manager console where the Nomad properties appear as a tabbed pane (e.g. in the properties of a package), if a Nomad property is modified but the "Apply" button is not clicked before moving to another tab, the value is not saved and reverts to the original value.	Save the values by clicking the "Apply" button before moving to another tab.

Issues	Description	Workaround
another tab.		
An exception may be seen when Nomad Admin UI extensions are upgraded and Task sequence editor is immediately launched.	A rare exception may occur when Nomad Admin UI extensions are upgraded and Task sequence editor is immediately launched.	Launch the Task sequence editor after 30 minutes once the upgrade has completed.
Resume and Pause GUI menu items in CM Console is not available to all users who are Full Admin in CM and assigned to Nomad Admins role in Tachyon.	It happens with users who belong to a security group which is Full Admin in CM. The same users should be able pause and resume from Tachyon Explorer app.	

Issues	Description	Workaround
Offer ID status message attribute is missing in some of the Nomad Status Messages .	The status messages sent by Nomad in case of content download for application and software update deployments, have missing Offer ID attribute.	

9.5.5.4 Multicast

Issues	Description	Workaround
Nomad may not check available disk space in a timely fashion during a Multicast transmission.	If a PC joins the multicast session mid-way through, it immediately starts to cache data locally and is not aware of the Package size. This is by design.	In environments where disk space is critical this issue is mitigated by: Ensuring that machines have enough disk space prior to sending the deployment Deferring the deployment start time to ensure that a Policy refresh has occurred on all the machines. This enables all the machines to start at same time, and they will therefore check for sufficient disk space.
“Slow sockets” log message.	This error message occurs during distributions using multicast if some datagram packets are lost. Some packet loss is to be expected, especially if a network traffic peak occurs, Nomad is designed to fill in the lost data at the end of the distribution. If excessive logging of this error message occurs and the statistics are returning a low percentage of data multicast, your network	

Issues	Description	Workaround
	infrastructure may not be suited to efficient multicast. This can occur if you have an infrastructure with mixed network speeds for example.	
Using MADCAP over very slow links with pre-cached data.	In scenarios with very slow WAN links (i.e. <256kbps) and pre-cached package data, peer copying is used instead of local multicast. If this occurs the following warning message will be displayed in the log file. WARNING: MADCAP_Request for PACKAGE_ID discarded $$<MCastControl><datetime> This happens due to the time taken to get a MADCAP address over the WAN. Package data is still shared at the branch and only copied once over the WAN successfully, however local network traffic will be higher as peer copying is used instead of local multicast.	MADCAP performance can be improved by specifying the MADCAP server IP address in the Nomad *MULTICASTMADCAPSCOPE* registry value.
Multicast continues after deployment has expired.	If the deployment expires during a multicast transmission, the transmission will continue.	
Multicast is not supported on FAT file systems.	Nomad with Multicast is not currently supported on FAT file systems. This may be addressed in a later version, pending customer feedback.	None.

9.5.5.5 SMSNomad.exe as a program command-line

Issues	Description	Workaround
Using “Start in” Configuration Manager Program property.	SMSNomad.exe assumes the working folder is the Distribution Point. If a “start in” location is specified as an Configuration Manager Program property then	

Issues	Description	Workaround
	SMSNomad.exe is unable to locate the package source and fails to distribute software.	

9.5.5.6 Single-Site Downloads

Issues	Description	Workaround
Nomad registers with ActiveEfficiency platform using network interface other than primary interface on multihomed machines.	On multihomed machines Nomad may register with a network interface other than the primary network interface. This may result in the machine becoming unavailable for single site download to other machines in the same site since it has registered itself with a network interface other than the intended one.	

9.5.5.7 Nomad Pre-caching

Issues	Description	Workaround
Download may fail for Pre-caching jobs that are setup for content that is still being distributed to distribution points	Download may fail for Pre-caching jobs that are setup for content that is still being distributed to distribution points.	It is always advisable to setup Pre-caching jobs for content that has been successfully distributed to distribution points.

9.5.5.8 Office 365 updates

Issue	Description	Workaround
Office 365 download does not resume and fails when Nomadbranch service is restarted or when machines resume from a restart or shutdown.	A single Office 365 installation leads to multiple Nomad jobs which follows following this sequence: *- Begin Job .. - End Job - Wait For Next Job - Begin Job .. - End Job - Wait For Next Job ....* If the Nomad service is restarted while waiting for the next job, there is no persisted job (if there is , it picks it up from the WMI). If the Nomad service is restarted	

Issue	Description	Workaround
	between Begin and End, it should pick the persisted job on startup.	
NightWatchman may be able to shutdown the machine when an Office 365 job is running.	Office 365 updates comes as a collection of multiple jobs. When a job completes and another is yet to start, there is small time gap. During this gap, In between the job, ByteRange job manager queue is empty. If at this time, "Nomadbranch -canshutdown" is triggered, it will return "TRUE".	
Corrupt Content is downloaded successfully, transferred to Office 365 cache and update installation succeeds	As Nomad doesn't receive hashes to validate downloaded contents so user can get the corrupted contents downloaded.	
ClickToRun stuck in Cancelling Job.. and further install request from Software centre does not triggers any Office Job	ClickToRun is part of Microsoft office 365 and sometimes it stuck while cancelling a job. Also, each new job is provided and handed over to Nomad by ClickToRun. So if ClickToRun is stuck then user won't be able to proceed further.	
While Running cachecleaner command, user faces "Error: CreateInstance-IUIResourceMgr <FAILED> - Class not registered".	It is caused by UIResource.dll getting unregistered. So workaround is to run the following command(Administrator user context): "regsvr32 UIResource.dll"	
NomadBranch switches "Activateall" and "Activate=(Content ID)" fails to verify Office 365 content in Nomad Cache.	Office 365 Cache is activated on Nomad service start up. So if, Manually copied some (Valid) data in Nomad Cache, Service needs restart to activate data. - Activate cmd does not impacts office cache.	
Nomad Office Job keeps on going even after reserve space got full.	This is happening in a particular scenario and is related to the case when a full file is being downloaded by Nomad office 365 job. As for full file download, the	

Issue	Description	Workaround
	information about content size is not with Nomad so it keeps on downloading.	
Nomad Cache refused to clear cache on Peer when other client downloading it from P2P.	The behavior is that the ByteRanges content might or might not get deleted depending on whether it's content is being accessed at that point in time or not. If it does get deleted, the Peer move next available peer and if not then move to DP for downloading.	
Intermittent issue: Non office job is not cancelling with command line properly.	This issue is a randomly occurring one and sometimes when user tries to cancel a job using nomad command line(Nomadbranch -cancel) then sometimes(randomly) the job is not cancelled.	User can rerun the command or in rare case restart the nomadbranch service and then rerun the Cancellation command.
Office 365 Update might fail if during download of Office 365 update SMSAgent service is restarted.	Office 365 Update might fail if during download of Office 365 update SMSAgent service is restarted. When download of failed job is re-initiated from Software Center the job download fails. Again ClickToRun being stuck in cancelling is causing this issue.	
Office 365 Update will sometimes fail if during download of Office 365 update requests a file which does not exist or folder reference does not exist.	This issue is specific to "Office 365 Client Update - Current channel(1609-4)" update. Here it is observed that wrong path is being generated in manifest file from Office 365 which results in update failure due to resources not found. All updates prior to this update were generating correct content path in the manifest file but this specific(Latest update by the time of writing this information) the content path is wrong in manifest file. Also this issue is not limited to Nomad alone but even the	

Issue	Description	Workaround
	CM software center triggered and CM managed update download is also failing.	
Nomad failed to delete cache with Percent Available disk space value.	This issue has two parts to it: Only one content is deleted to reserve the space and not all, whereas it should delete all to make sure percentavailabledisk is 10%. dummyAutoDelete gets added to cache and 1 byte is reserved for it. So when you again run, it won't' even delete one content.	
Nomad office updates doesn't support failover to BITS.	Nomad is not supporting "Failover to BITS" scenario in this release.	

9.5.5.9 Tachyon Platform

Issue	Description	Workaround

9.5.5.10 Content Distribution and Nomad app

Issue	Description	Workaround
After setting a new pre-set, a user cannot switch between the default columns and the columns chosen in the new pre-set.	Users have an option to select columns to be displayed in the list at different places in the Nomad Application. When using the Nomad application, the user may want to choose which columns they want to see in the detail tables. This provides consistency with other Tachyon applications. After setting a new pre-set, a user cannot switch between the default columns and the columns chosen in the new pre-set. There is no option to go	The workaround would be to either create a default preset or again refresh the browser.

Issue	Description	Workaround
	back to the default view unless by refreshing the browser.	
Task Sequence Details page - multiple registration entry for a single device.	Content shows multiple registration entries for a single device.	
Devices Page - Arrow keys are not giving hint "Expand" for main Pages while it is giving hint "Expand" for other chart and items.	When a user opens the Nomad app, for example the Devices page and they move the mouse cursor to the double arrow expand button in the right hand top corner of the page, there is no 'Expand' hint shown. If the mourse cursor is moved to other page tiles like Content Type, then the 'Expand' hint is then displayed.	
Installation/Upgrade - Installation/Upgrade fails when .mdf file already exists on the database server.	Case 1: When ActiveEfficiency (AE) is upgraded to ContentDistribution (CD). The AE DB got renamed to CD DB but its .mdf and .ldf files didn't get renamed. If an uninstall of CD is tried, and then the AE install is tried again, the attempt fails. Case 2: When CD was uninstalled and the existing CD DB is renamed. When the CD install is tried again, the attemt fails.	
Nomad App - Page expansion is not being retained on Details Pages of Overview, Contents, Task Sequences and Network locations pages.	Open Nomad App Dashboard > Click on Expand arrow key (present in right side top corner), now click on Devices Tab, then: Open Contents Tab > Click on Expand arrow key to expand page now click on any contents from list	

Issue	Description	Workaround
	Open Task Sequence page > Click on Expand arrow key to expand page now click on any TS from list Click on Network Location > Click on Expand arrow key to expand page now click on any Site from list. Only devices details page is retains the page expansion , rest of the pages do not retain the page expansion.	
NomadBranch - SMSNomad could not register to CDC when content is downloaded is a from peer share.	Create a share on peer machine, place some content on it. Uninstall nomad from there. On a peer machine, download content using standalone cmdline - smsnomad.exe --pp="\\W2004-32\MyNomadCache" --s --prestage The contents gets downloaded but logs some error regarding Content Distribution Consumer reporting failure. It should get reported to Content Distribution Consumer.	
Preset configuration - Unnecessary spacing on scrolling bookmark bar.	If a user creates multiple bookmarks and then scrolls back and forth, there is some extra spacing on scrolling.	
Content page - Missing scrollbar in bookmark preset window.	If a user creates multiple bookmarks, and then opens manage preset, there is no scrollbar. There should be a scrollbar in the preset window itself than using the application's/browser's scrollbar.	
Network location page - Nomad Application - In subnet drawer, Even if no record was available user can also select other	A user accesses the Nomad Application, then navigates to the Network Location	

Issue	Description	Workaround
options of no. of records on the page e.g. 100, 250	page and verifies the subnet drawer window. Even if no record was available, a user can also select other options for the no. of records on the page e.g. 100, 250-	
Nomad Application - In preset window, selected filters values are not identical to ones displayed on the page.	Go to any page where the Preset window is applicable e.g. Contents page and apply all the available filters. Click on the bookmark icon to open the Preset window. Then verify values under selected filters.	
Content - When any Software Update is downloaded from WUMU, on the dashboard, the size of the content is showing 0 Bytes.	When any Software Update is downloaded from WUMU, on the dashboard, the size of the content is showing 0 Bytes.	
Nomad Application - Content Distributiondoes not display contents details downloaded from sources other than Configuration Manager and Delivery Optimization.	If a share is created on a peer machine, and some content is placed on it, then uninstall nomad from there. Then on a peer machine, content is downloaded using a standalone cmdline. The 1EClient reports the content but Content Distribution does not display it.	
Nomad Application - Nomad App - New Preset - no option to go back to the default view unless by refreshing the browser.	When a user uses the new preset feature on: Content Task Sequences Devices Nomad Sites.	The workaround would be to either create a default preset or again refresh the browser.

Issue	Description	Workaround
	After they select a few columns, there is no option to go back to the default view unless they refresh the browser.	
Nomad Application - Labels used for the filters disappear on resizing the window.	When the application window is resized, the labels used for the Technology and Time period filters disappear.	
Nomad did not raise package deletion event (using -PkgVer=*) and throws an error.	If a version 1 package is download on client-1 device. The package is updated. And then version 2 is downloaded on client 2. When version 1 is deleted from client 1 using cmdline - cachecleaner.exe -DeletePkg=CAS0007A -PkgVer=* Nomad fails to raise the event for the deleted package.	
RBAC - Configuration Manager (CM) Ext - Even after an error message, the paused job was removed from the CM console	When a collection is already paused for the download and a user only has read permission. In the Configuration Manager console, go to Monitoring > 1E Nomad > Paused Collections And the user tries to resume the existing paused job. An error popup is displayed, but the paused job disappears. Note: A user has to revisit the page to see the existing job.	
1EClient installer - Platform features are working even if "Enable 1E Platform features"	If the 1E Client is installed with Nomad and "Enable 1E Platform features" checkbox is unselected.	

Issue	Description	Workaround
was not selected during installation.	After the installation completes, verify Content Registration, DO Reporting, SSD etc. The 1E Client was still able to use every feature of the Tachyon Platform.	
NomadBranch - Shows incorrect processor details.	Verify NomadBranch log file for the correct OS version and details.	
Content state is not getting updated by CDsync if 0 version of the same content is reported in between.	A downloaded event generated for SMSNomad download reports content version 0, which later gets deleted when cdssync run. But on the server side, the package remains in a cancelled state. Its state did not change although the client has 100% content in its cache. Content Distribution sync is unable to generate an event to correct its state.	
Download event gets generated for content version 0 if version is not provided in smsnomad cmdline.	Content downloads successfully and the corresponding event is generated for content version 0. The event should be generated for the correct version.	

Peer-Backup Assistant

Issue	Description	Workaround
Client does not participate in PBA Polling when two clients with the same name exist in two different domains.	If a client machine with same hostname name exists in two different domains, during PBA Polling the client does not participate.	

9.5.5.11 Nomad elections

Issue	Description	Workaround
Peer replying first in election is elected as Master irrespective of start-up time.	When None of the replying peer is current Master for Given Package and all the replying peers have same weight-age, also all the peers have 100% content for the given package. During download for the given package Elections is triggered and Peer replying first in election is elected as Master irrespective of start-up time of Nomad service	
Nomad shows incorrect logging indicating connection limit is over.	When there network disconnection during P2P download over http(s), sometimes incorrect logging appears indicating connection limit is over.	
Elections don't correctly honour uptime.	When election weight is same on all peers and one of the peer has greater uptime than everybody else then Nomad may not elect the machine with better uptime as master.	
In some cases high election weight peer loses election despite same content percentage.	When all the peers have almost same content percent then sometimes peer with higher election weight does not win elections.	

9.5.5.12 Nomad and Windows Servicing Assistant

Windows Servicing Assistant (WSA) is a feature of the 1E Client (with Shopping client enabled).

Issue	Description	Workaround
WSA deployment may restore data, which was captured by a different user.	When Replace capture WSA deployment is executed on source machine multiple times, different Nomad PBA Hosts can be honored to capture USMT data each time. During replace restore, target machine can restore any captured USMT data. Nomad PBA doesn't have a notion of version.	

Issue	Description	Workaround
TS execution fails as Content is not located in Nomad Cache if Nomad Cache was configured on Custom Drive.	If Nomad Cache is configured on the Custom drive then TS execution will fail as content will be searched in the default Nomad location.	
WSA Wizard might requests USB drive even when there is enough disk space.	Even though there is enough disk space on users workstation WSA Wizard might request for USB drive.	
PBA POLL / FIND fails during WSA TS execution.	If potential PBA host found during WSA prepareness, goes offline during Task Sequence execution, the TS can fail. Enabling HA can reduce the chances of such failures.	

9.5.6 Basic Nomad behavior in a simple environment

In order to understand how Nomad behaves in a simple environment, we have provided some examples. All the scenarios use the illustrated network setup, likely scenarios are:

Normal use

Master switched-off during upload

Common uplink broken

Distribution Point modified after initial advert download.

These scenarios are presented in a tabular format where time is represented going down the column and each row in the table marks a significant event. The columns in the table show the events that have taken place for each device.

9.5.6.1 Normal use

This illustration shows Nomad working as expected with no errors encountered during the transmission of a package. It shows a new **ADV00001** advertisement, being sent containing the **PKG00001** package:

Step	Device A	Device B	Device C
1	Start state ON	Start state ON	Start state OFF

Step	Device A	Device B	Device C
2	Receives new ADV00001 advert		
3	Starts Nomad		
4	Initiates election for PKG00001		
5	No replies so starts downloading from DP		
6		Receives new ADV00001 advert	
7		Starts Nomad	
8		Initiates election for PKG00001	
9	Reply to PKG00001 20% complete		
10		A wins election	
11		Updates local cache from A Copies blocks from A until caught up then back off (P2PbackoffSecs) before catching up again.	C is switched on
12	Each 5 minute period, A initiates an election and is re-elected as master		
13			Receives new ADV00001 advert
14			Starts Nomad
15			Initiates election for PKG00001

Step	Device A	Device B	Device C
16			Starts update local cache from A
17	A completes download and broadcasts **Done**		
18	Waits for peers to finish caching	Signals to A that cache is being copied	Signal to A that cache is being copied
19		Loads package	
20	Broadcast **Done**	Returns status for ADV00001	
21	Wait for peers to finish caching		
22			Signals to A that cache is being copied
23			Loads package
24			Returns status for ADV00001 advert
25	Loads package		
26	Returns status for ADV00001 advert		

9.5.6.2 Master switched-off during upload

This illustration shows how three devices running **Nomad** interact to elect a new master when the existing one becomes unavailable. It starts when a new advertisement, ADV00001, is sent containing package, PKG00001.

Step	Device A	Device B	Device C
1	Start state ON	Start state ON	Start state OFF
2	Receives new ADV00001 advert		
3	Starts Nomad		
4	Initiates election for PKG00001		
5	No replies so starts downloading from DP		
6		Receives new Advert ADV00001	
7		Starts Nomad	
8		Initiates election for PKG00001	
9	Replies to PKG00001 20% complete		
10		A wins election	
11		Updates local cache from A Copies blocks from A until caught up then back off (P2PbackoffSecs) before catching up again.	C is switched on
12	Each 5 minute period, A initiates an election and is re-elected as master		
13			Receives new ADV00001 advert
14			Starts Nomad

Step	Device A	Device B	Device C
15			Initiates election for PKG00001
16			Starts update local cache from A
17	A Switched Off		
18		B is partway through copying a block of data and returns an error	C is in a wait state and notices nothing yet
19		B initiates an election (loss of connection)	
20		B wins election and now takes over copying from the DP	C now caches from B
21	A Switched On		
22	Configuration Manager restarts package and Nomad		
23	A initiates an election (start up)		
24		B wins Election (% complete)	
25	A now caching from B		
26		B completes download and broadcasts **Done**	
27	Signals to B that cache is being copied	Wait for peers to finish caching	Signals to B that cache is being copied
28	Loads package		Loads package

Step	Device A	Device B	Device C
29	Returns status for ADV00001 advert		Returns status for ADV00001 advert
30		Loads package	
31		Returns status to for ADV00001 advert	

9.5.6.3 Common uplink broken

This illustration shows how **Nomad** deals with the situation where the WAN to the DP becomes unavailable and is later restored. It starts when a new ADV00001 advertisement has been sent containing the PKG00001 package.

Step	Device A	Device B	Device C
1	Start state ON	Start state ON	Start state ON
2	Receives new ADV00001 advert	Receives new ADV00001 advert	Receives new ADV00001 advert
3	Starts Nomad	Starts Nomad	Starts Nomad
4	Initiates election for PKG00001	Initiates election for PKG00001	Initiates election for PKG00001
5	A wins election and starts downloading from DP		
6		Updates local cache from A	Updates local cache from A
7	Each 5 minute period, A initiates an election and is re-elected as master		
WAN link broken			
8	Error detected – causing election to take place	Catch up with A	Catch up with A

Step	Device A	Device B	Device C
		After 3 periods of no progress, reverts to looking at DP link.	After 3 periods of no progress, reverts to looking at DP link.
9	A switched off		
WAN link restored			
10		B notices that WAN is restored and forces an election	
11		B is elected master	
12			Starts caching from B

9.5.6.4 Distribution Point modified after initial advert download

This illustration shows how the **Nomad** executable and service deals with the situation where the DP is modified after a master device has added the package to its cache. It starts with a new advertisement, ADV00001, is sent containing package, PKG00001 and the administrator then modifies the DP share.

Step	Device A	Device B	Device C
1	A has already cached package		
Admin Modifies the DP Shares			
2		Receives new ADV00001 advert	
3		Starts Nomad	
4		Initiates election for PKG00001	
5	Replies to PKG00001 100% complete		

Step	Device A	Device B	Device C
6		A wins election	
7		Whole package is loaded from A using original file list	
8		B notices that file list from A is older than DP last write time. B creates file list direct from DP and elects itself master	
9		B is now master and wins elections due to later file list	
10		Any file which does not exist or has been modified is now deleted and reloaded from the DP	
11			C caches from B as it has a more up-to-date file list
12	A is still running the old software and will continue to do so until it receives a new advert causing it to update		

9.5.7 Resolving common issues

The most common issues are listed below.

9.5.7.1 Communication issues

Nomad provides two types of encryption. By default, standard encryption uses a 40-bit RC2 algorithm, or you can enable advanced encryption which is compliant with FIPS. The advanced encryption is available for use in high-security environments where restrictions on encrypted algorithm types are enforced. These two methods are incompatible, so you must ensure that all installations of 1E Client are using the same encryption method.

9.5.7.2 Nomad firewall settings

By default, Nomad uses port 1779 to communicate during the election process for determining the master on a subnet. This port is opened during the 1E Client installation, however further action may be required in environments which use alternative firewalls, other than the native Windows Firewall.

> **Note**
>
> If you change the default port, ensure all Nomad clients are communicating on the same port.

9.5.7.2.1 P2P HTTP(S) firewall settings

If you're using HTTP or HTTPS as the protocol for P2P content transfer, then you'll also have to ensure there are firewall exceptions for TCP port(s) specified in settings P2PHttpPort or P2PHttpsPort.

> **Note**
>
> Please note that Nomad service automatically tries to add required firewall exceptions on startup. So if you experience firewall problems, most times it may be enough to simply restart Nomad service, and it'll add the missing exceptions.

9.5.7.3 File and print sharing

HTTP/S is the recommended protocol for peer sharing as well as download from servers. If this is not suitable then clients can use the default SMB, which requires the Windows **File and Printer Sharing Services** to be enabled.

If **File and Printer Sharing Services** is not available then Nomad can be configured to use HTTP or HTTPS.

For more detail about these and other access methods, please refer to Nomad cache.

9.5.7.4 Package version changes

Nomad has significant built-in logic to ensure that package version updates are handled and recoverable. However in complex environments with many package version changes happening whilst software distributions are in progress, unexpected behavior may occur. To increase software distribution success, ensure the following:

Minimize unnecessary package version updates

Avoid package version updates when active advertisements are running for that package

Wait until all distribution points have been updated prior to advertising

If failures occur, update the distribution points and re-advertise.

9.5.7.5 Cannot enable Nomad for a Configuration Manager client package (in the Configuration Manager Console)

The built-in Configuration Manager client package in Configuration Manager is locked, and therefore does not allow any modifications to be made to the package. In this instance, it is good practice to duplicate the existing client package for use with Nomad (for example, in OSD task sequences).

9.5.7.6 Verifying the speed or bandwidth utilization of a recent Nomad download

If you have the Nomad Download GUI already installed on the computer, you can use it to monitor the current download job in Nomad.

To review the download speeds of a recent Nomad download, open the NomadBranch.log file and locate the log entries related to the download job, taking specific interest of the *blk/s* values, as shown in the log extract below:

```
Remote_http   0100007F 9000 "Content_fe7d375d-c77c-4776-88e7-232b9d2ee65d_Cache
\Command_Monitor_x64.msi" blk=85 (blk/s=6)
Remote_http   0100007F 9000 "Content_fe7d375d-c77c-4776-88e7-232b9d2ee65d_Cache
\Command_Monitor_x64.msi" blk=88 (blk/s=3)
Remote_http   0100007F 9000 "Content_fe7d375d-c77c-4776-88e7-232b9d2ee65d_Cache
\Command_Monitor_x64.msi" blk=95 (blk/s=7)
PkgCacheStatusSet Content_fe7d375d-c77c-4776-88e7-232b9d2ee65d(1) Format:0 12.5
53%
Remote_http   0100007F 9000 "Content_fe7d375d-c77c-4776-88e7-232b9d2ee65d_Cache
\Command_Monitor_x64.msi" blk=99 (blk/s=4)
Remote_http   0100007F 9000 "Content_fe7d375d-c77c-4776-88e7-232b9d2ee65d_Cache
\Command_Monitor_x64.msi" blk=105 (blk/s=6)
Remote_http   0100007F 9000 "Content_fe7d375d-c77c-4776-88e7-232b9d2ee65d_Cache
\Command_Monitor_x64.msi" blk=108 (blk/s=3)
```

The *blk/s* refers to the number of blocks downloaded per second. The default block size is 131072 bytes (128KB), so *blk/s=6* equates to 786,432 bytes per second (or 768 KB/s). The block size can be changed by modifying the registry BlockSize.

9.5.8 Resolving content integrity (hash checks) issues

When an LSZ request is made and the request contains a hash, Nomad on DP computes a corresponding hash for the content on its disk. If the computed hash does not match the hash sent by the client, the content is considered corrupted and if it matches, the content is considered good, (see the example N*omadBranch.Log*below).

9.5.8.1 Download process

The process for the download is:

Clients retrieve this LSZ and check it for any errors.

If they evaluate an error (N*omadBranch.Log*shown opposite), they quit the download immediately.

If not, the download proceeds normally.

9.5.8.2 Set CompatibilityFlags on the DP and client

We also need to make sure that we have CompatibilityFlags set correctly on the DP and client respectively as follows:

Bit	Description
0x80000	The bit is enabled by default. Setting this bit enables full hash generation for SIS content when an LsZ file is generated on a DP. If this is not enabled, SIS content is trusted, and corrupted content may be downloaded.
0x100000	The bit is enabled by default. Setting this bit would abort download on a Nomad client if an LsZ hash mismatch is detected. If this is not set, when a Nomad client detects a hash mismatch it will re-request LsZ generation on the DP then try again, and get stuck in a loop if the SIS content is corrupt.

9.5.9 Reducing election notifications in Nomad log

By default, when an election occurs, all Nomad clients log the responses from every other client on the same subnet. In large subnets, this can result in the NomadBranch.log filling up and rolling over. This causes important entries getting missed and makes troubleshooting difficult.

9.5.9.1 Using MaxElectionResponseLogging to manage election notifications

You can turn off election response logging, or limit the number of responses logged for each election using theMaxElectionResponseLogging registry value. By default, the registry value will not be present and so all the election repliesare logged. If it's created (as a REG_DWORD value) and set to zero then no election replies willare logged. When using this option it may be useful to log some election responses to confirm the election process works.To do this, create theMaxElectionResponseLoggingregistry value and set it to themaximumnumber of responses you want logged for each election.

9.5.9.1.1 MaxElectionResponseLogging example

For example, you can create the MaxElectionResponseLogging REG_DWORD value and set it to 10.When there's an election request for package ABC0012D, there may be 350 responses received and processed, but only 10 of those responses will get logged on each client.Doing this, will keep logging to a reasonable amount and keep the logs helpful for troubleshooting.

Note

The value of MaxElectionResponseLogging specifies the number of election replies to be logged per election request.

As an example, if MaxElectionResponseLogging = 5 and there are two election requests for the same package at different times, a maximum of 5 election responses will be logged for each election (up to 10 election replies in total). If there are two concurrent election requests for the same package, the number of maximum election replies logged may vary from 5 to 10.

In general, if MaxElectionResponseLogging = *n* and if there are *m* concurrent election requests for the same package, the number of maximum election replies logged may vary from *n* to *m***n*.

Note

This option can be defined during installation of the 1E Client using the installer property MODULE.NOMAD.MAXELECTIONRESPONSELOGGING.

9.5.10 Resolving hard link issues

A hard link is the file system representation of a file by which more than one path references a single file in the same volume.

9.5.10.1 Using hard links

To create a hard link, use the *CreateHardLink* function. Any changes to that file are instantly visible to applications that access it through the hard links that reference it. However, the directory entry size and attribute information is updated only for the link through which the change was made.

Note

The attributes on the file are reflected in every hard link to that file, and changes to that file's attributes propagate to all the hard links.

If you reset the *READONLY* attribute on a hard link to delete that particular hard link, and there are multiple hard links to the actual file, you will need to reset the *READONLY* bit on the file from one of the remaining hard links to bring the file and all remaining hard links back to the *READONLY* state.

For example, in a system where C: and D: are local drives and Z: is a network drive mapped to *\\fred\share*, the following references are permitted as a hard link:

C:\dira\ethel.txt linked to C:\dirb\dirc\lucy.txt

D:\dir1\tinker.txt to D:\dir2\dirx\bell.txt

C:\diry\bob.bak linked to C:\dir2\mina.txt

However, these are not:

C:\dira linked to C:\dirb

C:\dira\ethel.txt linked to D:\dirb\lucy.txt

C:\dira\ethel.txt linked to Z:\dirb\lucy.txt

9.5.10.2 Deleting hard links

To delete a hard link, use the *DeleteFile* function. You can delete hard links in any order regardless of the order in which they are created.

9.5.10.3 Further considerations

When troubleshooting hard link problems, consider the following:

Consideration	Notes
Antivirus software	Security software and antivirus can block access to the file when you create a hard link so make sure it is not blocked by them.
Security policy	Your security policy should not be blocking hard links.
Insufficient Disk space	Make sure the drive has sufficient space to download the content.
Permissions	Check the permissions on the drive and folder of the source and target.
Configuration Manager	Configuration Manager did not create the folder for the hard link or it deleted it after the hard link failure – you can verify that in the *CAS.Log* and *NomadBranch.Log* Configuration Manager CAS created the folder (such as 2f) in the *ccmcache* folder but deleted for whatever reason, i.e. content was not hashed successfully by Configuration Manager client.

9.5.11 Resolving Nomad peer election issues

There can be multiple reasons why an elected master is disqualified from elections and therefore unable to provide content to a requesting client, for example different Nomad registry settings on client and master, or network issues (such as the client firewall not being configured correctly).

9.5.11.1 Things to check

As part of your troubleshooting process, you can:

Ensure the version of Nomad running is same on all peers.

Ensure the Nomad client settings are correctly matched – for example if you have configured the registry SpecialNetShare to hide the Nomad Share, make sure other clients use the same settings, otherwise the clients won't be able to do a P2P download successfully. Ensure your OSD Task Sequences have the same settings, such as the Install and Configure Nomad in WinPE step.

Ensure client firewalls are configured correctly. Even though Nomad self-configures the Windows Firewall, you may have Group Policy settings that override the local settings. If you have another firewall installed, such as McAfee HIPS or Symantec Endpoint Protection, you will need to configure those settings for Nomad.Check network access, refer to the relevant online help for further information.

Review the following KB article for a scenario where User Rights have prevented Nomad from working correctly, and the suggested solution:https://1eportal.force.com/articles/Info/KB000001596

Check if the peer downloading content from an elected master has disqualified the master because there is no download progress after multiple retries.

9.5.11.2 Remediation

A master that is disqualified for a package remains in the disqualified state for an hour and does not respond to election requests for that package. If any peer holds an election after an hour, the disqualified master participates in the election.

If an elected master is disqualified 6 times, then it enters into a **too many disqualifies** mode and stops responding to election requests for that package. P2PEnabled and SpecialNetShare registry settings should be checked on the disqualified master, to see if they are different from the peer that has disqualified the master. The **1E Nomad Branch** service must be restarted on the master if we want it to act as a peer and participate in the elections.

9.5.12 Resolving Peer Backup Assistant (PBA) issues

Considerations to resolve Peer Backup Assistant (PBA) issues.

9.5.12.1 The state of the Nomad log when PBA is working

The following examples illustrate the state of the Nomad log when PBA is working.

9.5.12.1.1 Peer Backup Assistant: Provision Nomad PBA Data Store

PBA process typically starts with provisioning the Nomad data store to find the OSDStateStorePath variable to let the task sequence know where to store and retrieve user state data. This step is initiated for an election within the subnet or query through AE(SSD PBA) for the site. The task sequence executes:

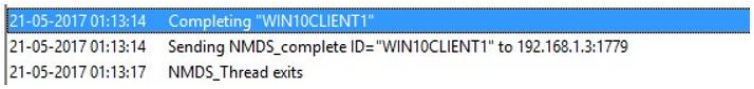
```
NomadPackageLocator.exe -NMDS_POLL,%ComputerName%,100
```

The snippet below from *Nomadbranch.Log* shows the process of NMDS polling and accepting the offer from machine SCCM-PRI.

9.5.12.1.2 Peer Backup Assistant: Close Nomad PBA Data Store

This step closes any existing connections it establishes with its peers to store content. The command it executes for the task sequence to complete the NMDS process is:

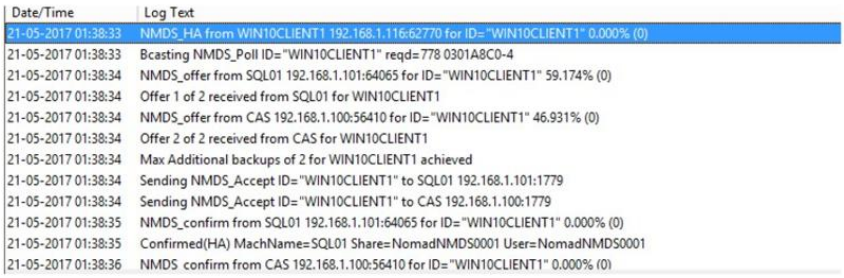
```
NomadPackageLocator.exe -NMDS_COMPLETE,%PBAComputerName%
```



9.5.12.1.3 Peer Backup Assistant: Nomad PBA Data Store High Availability

This step is used to replicate multiple copies in other data stores for high availability. This is helpful to prevent any data loss should the primary data store becomes unavailable or gets corrupted. The command it executes from the task sequence is:

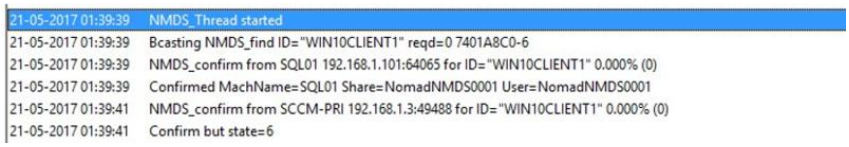
```
NomadPackageLocator.exe -NMDS_HA,1,2,1
```



9.5.12.1.4 Peer Backup Assistant: Locate Existing Nomad PBA Data Store

This step locates an existing data store to restore content. The command it executes from the task sequence is:

```
NomadPackageLocator.exe -NMDS_FIND,%PBAComputerName%
```



9.5.12.1.5 Peer Backup Assistant: Release Nomad PBA Data Store

Finally, this step releases and deletes any existing data store it uses. The command it executes from the task sequence is:

```
NomadPackageLocator.exe -NMDS_DELETE,%PBAComputerName%
```

Once all the data has been successfully copied back and is no longer required, it can be removed from the host. If this step is not used, the data is automatically deleted after a prescribed time.

9.5.12.2 Further considerations

If you see this error in the smsts.log:

```
Failed to run the action: Peer Backup Assistant: Locate Existing Nomad PB
A Data Store.
Incorrect function. (Error: 00000001; Source: Windows)
```

– it is a generic error message with no further information available. The PBA Step, Peer Backup Assistant: Locate Existing Nomad PBA Data Store is used to find Nomad data store to host PBA data.

If you see this error in the Nomadbranch log on PBA peer machines:

```
06-12-2017 12:14:00 NMDS_Thread started NMDS_PC532488 13560 (0x34F8)
06-12-2017 12:14:00 WARNING: latency>10 =15 - NMDS_Poll CommsRx 7828 (0x1
E94)
06-12-2017 12:14:00 Protocol requested: HTTP OR SMB NMDS_PC532488 13560 (
0x34F8)
06-12-2017 12:14:00 Insufficient allocation - Requested=1000 AlreadyAlloc
ated=0 MaxNMDSMega=5120 MaxAllocRequest=200 NMDS_PC532488 13560 (0x34F8)
06-12-2017 12:14:00 NMDS_Thread exits NMDS_PC532488 13560 (0x34F8)
```

In background, this command runs when this step is initiated:

```
NomadPackageLocator.exe -NMDS_POLL,%ComputerName%,100
```

Once the command is initiated, PBA clients broadcast in the subnet to find a suitable PBA store. PBA peers get these broadcast messages in their subnet and respond. However, in some cases where the PBA client finds no peers, it is likely a result of one of these:

Peers are NOT enabled to host PBA store

PBA is enabled but insufficient disk allocated

Allocated space is NOT sufficient to host data store.

If any task sequence steps fails on a PBA step:, check the following:

Is PBA enabled on peer machines? To verify it, you would need to ensure that value of registry value MaximumMegaByte at location Software\1E\NomadBranch\NMDS\ is **not** zero. If it is 0, it means that the machine is not allowed to host any data and will reject all PBA requests.

If PBA is enabled, ensure that the maximum allocation request by each client is configured with optimum space to host PBA data. To configure it, you will need to modify the registry value MaxAllocRequest at location Software\1E\NomadBranch\NMDS\.

For example, if original value is set at 200MB but the space requested by the client to store user state data is 250MB, it will fail. Typically, you can set MaxAllocRequest to be less than or equal to

MaximumMegaByte value. The difference between two is that with MaximumMegaByte, the client is configured to host Maximum data for all PBA clients, whereas with MaxAllocRequest, it is configured to host Maximum data which can be allocated to each client.

For example, if MaximumMegaByte=5120 and MaxAllocRequest=2560, the PBA host can store the user state data of two machines simultaneously where each client can store data up to 2560MB and total space allocated is 5120MB.

9.5.13 Resolving peer copy over HTTP or HTTPS issues

Nomad peer-to-peer content transfer uses SMB by default, which requires File and Print services to be enabled in order for it to share the content. For better security Nomad can be configured to use HTTP or HTTPS for peer-to-peer content transfer, removing the requirement for file shares. When Nomad is configured to use HTTP/S, if Peer Backup Assistant is enabled it will also use HTTP/S.

9.5.13.1 How it works

On start up, the Nomad service starts, the HTTP server logs a list of URLs it listens to, see the picture opposite.

```
1/25/2017 7:45:05 PM    Starting Http(P2P) Server
1/25/2017 7:45:05 PM    Http Initialized
1/25/2017 7:45:05 PM    Http Create Request Queue: 'Nomad'
1/25/2017 7:45:05 PM    listening for http requests on 'Http://*:5080/Nomad/Cache'
1/25/2017 7:45:05 PM    listening for http requests on 'Https://*:5443/Nomad/Cache'
1/25/2017 7:45:05 PM    listening for http requests on 'Http://*:5080/Nomad/Store'
1/25/2017 7:45:05 PM    listening for http requests on 'Https://*:5443/Nomad/Store'
```

When any Nomad client wants to download content, it does an election and identifies a device which has content in its cache (the Master device).

During the elections, the protocols supported by a client are not shared. Based on the local client's configuration, it chooses the protocol to use for downloading content from master. The example opposite illustrates the the connection to PC1 device using HTTPS protocol.

```
1/25/2017 6:24:55 PM    MyElection done - Winner is "PC1"  Best Offer is "" W=50 =0
1/25/2017 6:24:55 PM    Transfer Master has changed - now "PC1"
1/25/2017 6:24:55 PM    Nomad Branch event Evt_MasterChanged : PC1 for S0100015(18)
1/25/2017 6:24:55 PM    Connection::SetDownloadSource = Peer
1/25/2017 6:24:55 PM    RANDOM=558 users=0 delay=558 attempt=1
1/25/2017 6:24:56 PM    AttemptConnection "PC1"
1/25/2017 6:24:56 PM    Standard P2P Https connecting to master Https://PC1:5443/Nomad/Cache as "PC1\SMSNomadP2P&"
1/25/2017 6:25:07 PM    Adding credentials
1/25/2017 6:25:09 PM    Peer Connected OK
```

When a Nomad client is configured to use multiple protocols, the order of preference is HTTPS, HTTP followed by SMB. When files are downloaded, the logging is prefixed **P2P_http** to differentiate it from an SMB download. Both HTTP and HTTPS will use the same prefix.

```
1/25/2017 6:25:09 PM    P2P_http    0100007F A080 "S0100015_Cache\1.txt" blk=1 (blk/s=1) 0(0)
1/25/2017 6:25:09 PM    PkgCacheStatusSet S0100015(18) Format:0 1.431%
1/25/2017 6:25:10 PM    P2P_http    0100007F A000 "S0100015_Cache\NomadBranch.log" blk=309 (blk/s=308) 998000(3AF6C04)
1/25/2017 6:25:11 PM    P2P_http    0100007F A000 "S0100015_Cache\NomadBranch.log" blk=759 (blk/s=450) 17A8000(3AF6C04)
1/25/2017 6:25:12 PM    P2P_http    0100007F A000 "S0100015_Cache\NomadBranch.log" blk=1209 (blk/s=450) 25B8000(3AF6C04)
1/25/2017 6:25:13 PM    P2P_http    0100007F A000 "S0100015_Cache\NomadBranch.log" blk=1699 (blk/s=490) 3508000(3AF6C04)
```

9.5.13.2 Common error conditions

HTTP/HTTPS specific failures are most likely to occur when connecting to master, common errors you may encounter are shown opposite.

Error Code	Reason	Comments
0x00002efd and 0x00004CF	HTTP(S) is **not enabled** on master or HTTP(S) server on master is listening on **different port**	In the below log snippet, HTTP(S) wasn't enabled on PC1. *AttemptConnection "PC1"* *Standard P2P Https connecting to master Https://PC1:5443/Nomad/Cache as "PC1\SMSNomadP2P&"* *Send request failed https://PC1:5443 Nomad/Cache - FormatMessage failed with 0x0000013d for error code 0x00002efd* *Failed to connect to Https://PC1:5443/Nomad/Cache: The network location cannot be reached (0x000004CF)* *Failed to connect: The network location cannot be reached (0x000004CF)* *GetLstFromPeer: Connect ERROR - The network location cannot be reached* *GetLstFromPeer: failed - The network location cannot be reached* *Inside CopyLoopWait CopyError: The network location cannot be reached* *Unexpected Network Error The network location cannot be reached(1231)*
0x00002f8f and 0x000000A	Invalid Certificate on master	Any certificate issue would cause the download to fail with 0x00002f8f(Security Error). And current logging doesn't indicate the root cause of failure. On any security errors, one should check the following on master • Expiry date. • Subjects - should contain hostname (and fqdn). • Issuer should be trusted via the trust chain on the peer machine. • SSL Binding - Refer to above section to verify whether binding is existing for configured HTTPS port. In below log snippet, agent couldn't connect to PC1 because it had certificate issued by unknown CA. *AttemptConnection "PC1"* *Standard P2P Https connecting to master Https://PC1:5443/Nomad/Cache as "PC1\SMSNomadP2P&"* *Send request failed https://PC1:5443 Nomad/Cache - FormatMessage failed with 0x0000013d for error code 0x00002f8f* *Failed to connect to Https://PC1:5443/Nomad/Cache: The environment is incorrect (0x000000A)* *Failed to connect: The environment is incorrect (0x000000A)* *GetLstFromPeer: Connect ERROR - The environment is incorrect* *GetLstFromPeer: failed - The environment is incorrect* *Inside CopyLoopWait CopyError: The environment is incorrect* *Unexpected Network Error The environment is incorrect(10)* *CopyLoopWait: 5000 The environment is incorrect (0x000000A)*

9.5.13.3 Raising a support ticket

When you raise a support case with 1E for P2P HTTP/HTTPS file transfer issues, remember to attach the necessary log files (see below) and identify the Package ID, Deployment date and time for it.

C:\ProgramData\1E\NomadBranch\Logs\NomadBranch.log

C:\Windows\CCM\Logs\CAS.log

C:\Windows\CCM\Logs\CTM.log

9.5.14 Resolving Remote Differential Compression (RDC) issues

Remote Differential Compression (RDC) is sometimes known as binary differential replication or binary deltas but is more commonly known as remote differential compression (RDC) integration, for details refer to https://docs.microsoft.com/en-us/previous-versions/windows/desktop/rdc/about-remote-differential-compression.

For details about how Nomad integrates with RDC refer to Remote differential compression (RDC) integration.

9.5.14.1 Considerations when working with RDC

Considerations when working with Remote Differential Compression (RDC) issues:

Consideration	Notes
Configuration Manager 2012	On Configuration Manager 2012, RDC will not be used for Applications. This is because an Application's content version always remains at 1, only the content revision gets updated with a new content ID and hence RDC for Applications will not occur. This is not a limitation of Nomad, but simply the way the Application model is implemented in Configuration Manager 2012.
LSZ generation	The NomadBranch service skips RDC calculations while generating LSZ of a package for which LSZ of version n-1 has not been generated earlier or if the LSZgen request is for the first version of the package. Nomad only performs binary differential replication (BDR) for packages that are 1 version different (N-1) from the cached version. If the content is at version 3 and the client retrieving content has version 1 in cache, the client will retrieve the entire package. This sounds like a big caveat, but chances are that when Nomad goes to get the content there will be a peer in the local site that has it already, so the package will not be transferred across the WAN link. Also, if the device doesn't have the N-1 version and another device in the site does have the N-1 version, that content will be retrieved from the peer and only the delta content will be retrieved from the DP. In the event that it did have to traverse the WAN, Nomad will never step on your business traffic. For more information refer to http://www.1e.com/blogs/2014/09/01/nomad-and-binary-differential-replication/
Elected master on a subnet	RDC is between the DP and the elected master only in a subnet. The remaining devices or peers in the subnet will copy all the blocks of files modified in the package using normal P2P or local multicast. RDC_alt copy takes place when the elected master does not have the previous version of the package but another device on the subnet has it. The elected master can still do RDC file copy by copying the required blocks using RDC_alt copy from the other device on the subnet.
Packages over 125MB in size	Nomad automatically performs BDR functionality for packages over 125MB in size. Packages smaller than this do not benefit from BDR.

9.5.14.2 The state of the NomadBranch log when things are working

The state of the NomadBranch log when things are working as illustrated by the client and DP logs.

9.5.14.2.1 Client log

The Nomad client has to download version 50 of the package and it has set RDC previous version to 49 which must be present in order for RDC to work:

```
05-12-2016 18:27:24       WARNING: stale ELD P010051E(49)           Copy_P01005
1E(50)        8644 (0x21C4)
05-12-2016 18:27:24       LM16294 caching "http://1ETRAINCMPRI.1ETRAIN.lOCAL/SM
S_DP_SMSPKG$/P010051E" to "C:\ProgramData\1E\NomadBranch\P010051E_Cache"  Copy_
P010051E(50)        8644 (0x21C4)
05-12-2016 18:27:24       CopyLoop started. PackageID: P010051E(50), PackageSou
rce: http://1ETRAINCMPRI.1ETRAIN.lOCAL/SMS_DP_SMSPKG$/P010051E, CachePath: C:\P
rogramData\1E\NomadBranch\P010051E_Cache      Copy_P010051E(50)        8644 (0x
21C4)
05-12-2016 18:27:24       Setting RDC prev Version=49      Copy_P010051E(50)
8644 (0x21C4)
05-12-2016 18:27:24       PkgCacheStatusExtra P010051E(50) was 49           Cop
y_P010051E(50)        8644 (0x21C4)
05-12-2016 18:27:24       PkgCacheStatusExtra2 P010051E(50) was 49        Copy_
P010051E(50)        8644 (0x21C4)
05-12-2016 18:27:24       WARNING: CalcPercent version changed local=49 require
d=50    Copy_P010051E(50)        8644 (0x21C4)
05-12-2016 18:27:24       RequestElection "P010051E"(50) - Startup            C
opy_P010051E(50)        8644 (0x21C4)
```

9.5.14.2.2 DP log

Nomad logging events while it is generating LSZ file for version 50 with CRC and RDC. And it could find that RDC for LSZ version 49 was already processed:

```
05-12-2016 18:27:27       Generating "P010051E_50.LsZ" from SIS location D:\SCC
MContentLib\P010051E with hash 800C8C13CC3DBE5EEDF5C6625E99B5BCE9F2825C7057CB9F
E82E6394A462DBB9               LSZwork_P010051E(50)               15084 (0x3A
EC)
05-12-2016 18:27:27       Generating List LSZFILES\P010051E_50.LsZ with CRCs an
d with RDCdata from P010051E.50               LSZwork_P010051E(50) 15084 (0x3A
EC)
05-12-2016 18:27:27       RDC: Processed previous version LSZ (P010051E_49.LsZ)
- OK       LSZwork_P010051E(50)               15084 (0x3AEC)
05-12-2016 18:27:27       Comparing \\?\C:\ProgramData\1E\NomadBranch\LSZfiles\
TarFiles\P010051E.49.tar \\?\C:\ProgramData\1E\NomadBranch\LSZfiles\TarFiles\P0
10051E.50.tar for "install - Original.xml" to "\\?\C:\ProgramData\1E\NomadBranc
h\LSZFILES\RDCdata\P010051E_49_50\install - Original.xml.needs.bin"
LSZwork_P010051E(50) 15084 (0x3AEC)
05-12-2016 18:27:27       Comparing \\?\C:\ProgramData\1E\NomadBranch\LSZfiles\
TarFiles\P010051E.49.tar \\?\C:\ProgramData\1E\NomadBranch\LSZfiles\TarFiles\P0
10051E.50.tar for "Install.bat" to "\\?\C:\ProgramData\1E\NomadBranch\LSZFILES\
RDCdata\P010051E_49_50\Install.bat.needs.bin"               LSZwork_P010051E(5
0) 15084 (0x3AEC)
05-12-2016 18:27:27       Comparing \\?\C:\ProgramData\1E\NomadBranch\LSZfiles\
TarFiles\P010051E.49.tar \\?\C:\ProgramData\1E\NomadBranch\LSZfiles\TarFiles\P0
10051E.50.tar for "install.xml" to "\\?\C:\ProgramData\1E\NomadBranch\LSZFILES\
RDCdata\P010051E_49_50\install.xml.needs.bin"               LSZwork_P010051E(5
0) 15084 (0x3AEC)
05-12-2016 18:27:27       Comparing \\?\C:\ProgramData\1E\NomadBranch\LSZfiles\
TarFiles\P010051E.49.tar \\?\C:\ProgramData\1E\NomadBranch\LSZfiles\TarFiles\P0
```

```
10051E.50.tar for "setup.exe" to "\\?\C:\ProgramData\1E\NomadBranch\LSZFILES\RD
Cdata\P010051E_49_50\setup.exe.needs.bin"                LSZwork_P010051E(50) 1
5084 (0x3AEC)
05-12-2016 18:27:27       Comparing \\?\C:\ProgramData\1E\NomadBranch\LSZfiles\
TarFiles\P010051E.49.tar \\?\C:\ProgramData\1E\NomadBranch\LSZfiles\TarFiles\P0
10051E.50.tar for "uninstall.xml" to "\\?\C:\ProgramData\1E\NomadBranch\LSZFILE
S\RDCdata\P010051E_49_50\uninstall.xml.needs.bin"                LSZwork_P01005
1E(50) 15084 (0x3AEC)
05-12-2016 18:27:27       Comparing \\?\C:\ProgramData\1E\NomadBranch\LSZfiles\
TarFiles\P010051E.49.tar \\?\C:\ProgramData\1E\NomadBranch\LSZfiles\TarFiles\P0
10051E.50.tar for "Office\Data\v32.cab" to "\\?\C:\ProgramData\1E\NomadBranch\L
SZFILES\RDCdata\P010051E_49_50\Office\Data\v32.cab.needs.bin"                LS
Zwork_P010051E(50) 15084 (0x3AEC)
```

9.5.14.3 The state of the NomadBranch log when it cannot find the previous version

The state of the NomadBranch log when it cannot find the previous version as illustrated by the client and DP logs.

9.5.14.3.1 Client log

Client log at 10:00: Client tried to download the content P010051E(42) from DP 1ETRAINCMPRI.1ETRAIN.lOCAL.

```
18-11-2016 10:01:37       Starting TransferFile 0.000% blks=34945 (F=)       Co
py_P010051E(42)        6336 (0x18C0)
18-11-2016 10:01:37       Nomad Branch event Evt_StartedCopy :  HTTP from http:
//1ETRAINCMPRI.1ETRAIN.lOCAL/SMS_DP_SMSPKG$/P010051E for P010051E
Copy_P010051E(42)                6336 (0x18C0)
```

9.5.14.3.2 DP log

DP log: DP also received the LSZ gen request but could not find the previous version because it could not find the previous version 41 of this package, so it downloaded version 42 from the DP.

```
18-11-2016 10:00:55       Generating "P010051E_42.LsZ" from SIS location D:\SCC
MContentLib\P010051E with hash 3A0C6CAD223B5B244D8AF3CAE1C127B916699F91AD4D8D57
B7EE69B2980FE834             LSZwork_P010051E(42)
18-11-2016 10:00:55       Generating List LSZFILES\P010051E_42.LsZ with CRCs an
d with RDCdata from P010051E.42               LSZwork_P010051E(42) 5472 (0x156
0)
18-11-2016 10:00:55       No RDC: Cannot find previous version LSZ (\\?\C:\Prog
ramData\1E\NomadBranch\LSZFILES\P010051E_41.LsZ) - The system cannot find the f
ile specified               LSZwork_P010051E(42) 5472 (0x1560)
```

9.5.14.4 Considerations when resolving RDC issues

When resolving RDC issues, you should:

Ensure that RDC installed on the site server and on any Branch Distribution Points (BDP), the Nomad client does not need RDC on it

Select the Binary Differential Replication checkbox in the properties of any package for which you want to use BDR

Ensure that the RDC content are one version different from the cached version

Ensure that the content size is more than 125 MB, packages smaller than this do not benefit from BDR

Check where the SMSSIG$ folder is on the DP and compare it with the path in the Nomad registry setting HKLM\Softwares\1E\Nomad\SigsFolder. If it is not set, Nomad assumes that signature files location as C:\SMSSIG$, if it exists.

9.5.15 Resolving slow content transfer issues

If you encounter slow content transfers, we recommend you consider the following:

Consideration	Notes
WAN accelerators	WAN accelerators can sometimes interfere with Nomad bandwidth utilization calculations making Nomad to back-off unnecessarily.
Cisco routers	Network devices such as Cisco routers may have HTTP/HTTPS packet inspection rules turned on by default, which may also interfere with Nomad bandwidth utilization calculations and cause Nomad to back-off unnecessarily.
Network optimization or caching devices	Do you have network optimization or caching devices? If so, work with your Network team to determine the configuration.
Local connected network devices	Ensure that all local connected network devices such data switches, network adapters, are using 1Gpbs links.
Network adapter device drivers	We also recommended that network adapter on clients are using the latest device drivers.
Antivirus solutions	Antivirus solutions might be scanning content as it is being transferred through Nomad. It might be necessary to add an exclusion to the SCCMContentLib folders in the Configuration Manager Distribution Points as well as the Nomad and Configuration Manager client cache folders.
Blocksize	The default blocksize for Nomad 7.0 (and later) is 128KB. The default for earlier versions is 32KB. Every block needs to be authenticated, which may

Consideration	Notes
	add to the content transfer time. Please refer to BlockSize page for more information.
Nomad work rate	Ensure that the Nomad work rate (the proportion of available bandwidth) is not set too low. The default Nomad work rate is 80 and this should work fine in most environments.
P2PEnable	Avoiding configuring Nomad P2PEnable registry value to 6 – Connectionless Server and Client expect Nomad enable OSD task sequences. Connectionless is considerably slower than SMB and HTTP/HTTPS therefore it is not a recommended setting except when there is a business requirement that all Nomad peer-to-peer communications must use connectionless.
Outdated hardware	Nomad peers performance bottlenecks such as CPU, Memory and Disk I/O. Outdated hardware might not provide the best transfer performance when large content such as a Windows image file is being transferred to local Nomad peers.

9.5.16 Resolving SoftwareUpdate metadata validation

Updating the contents of an object in Configuration Manager usually results in a version change (or a new object is created). However, with SoftwareUpdates, the contents could be updated without any change in its ID or version (which always remains at 1). Such changes to content without versioning would cause issues in peer-to-peer (P2P) sharing, because peers could serve stale content. To cope with changes like this, an additional validation has been introduced for software updates, ensuring clients download the latest content.

This additional validation ensures Nomad downloads content as the Configuration Manager client expects. With software updates the metadata of its files is available in the Configuration Manager client's WMI, and is compared against the details in LSZ. If there is a mismatch, the client tells the peers to delete the stale content from their cache and the client retries the download. If the client was downloading from a DP, a message is sent to Nomad on that DP and the LSZ is recreated is using the latest content. Once a client has downloaded the LSZ with the expected metadata, the rest of the download logic continues as expected.

9.5.16.1 How it works

File metadata is obtained from the 'DownloadInfoEx2' class in CM's WMI and as a part of the validation process, the name and hash of every file is compared against those in the LSZ. In the following example, the hashes are SHA1.

Note

The file hashes currently in the LSZ are of SHA2. LSZ generation is updated to put in SHA1 hashes for software updates.

Sample metadata in WMI:

```
<Content ContentId="c54879c8-215e-413f-afbf-a701afa2d637" Version="1">
<FileContent Name="18362.30.190401-1528.19h1_release_svc_refresh_CLIENTBUSINESS
_VOL_x86FRE_en-us.esd" Hash="1F01343ACDE39AE567FF520F9FC51DC2F9507305" HashAlgo
rithm="SHA1" Size="2345415546"/> <FileContent Name="WindowsUpdateBox.exe" Hash=
"A215D07C5B28BA2270D9E2F54FB51C1010777762" HashAlgorithm="SHA1" Size="19524440"
/>
</Content>
```

If the metadata in the LSZ does not match, the LSZ is deleted and the download is retried and downloading of stale LSZ is avoided in the next attempt. If the client is downloading from a Distribution Point (DP), an LSZGen request is sent with a force option, so the existing LSZ file on the DP is deleted and generated again using the latest content, this means that any changes to content after the initial LSZ generation is accounted for.

If the client was downloading from a peer, then a "Validate Metadata" message is broadcast to peers. When peers receive the message, clients will validate the LSZ metadata in their cache using the 'MetadataHash' included in the message. If there is no match, clients delete the entire content from their cache. This means that when the original download is retried, any clients with stale content will not take part in elections. If there are any SSD/LocalSSD peers included, they are informed individually with a similar message.

The 'MetadataHash' used for validation is a hash of details of every file in the content. It is an SHA2 hash, calculated using Name&Hash of each file sorted alphabetically using their hashes (there is no specific reason for choosing hashes as the sort criteria, using the name also would work the same way).

9.5.16.2 Configuration

These changes apply when the *0x40000000* flag is enabled in CompatibilityFlags.

Note

This bit must be added to CompatibilityFlags for this to work, it is not set by default.

Before applying the *0x40000000* flag, consider that:

This validation may not work for updates deployed before this fix, because file hashes in LSZ for existing packages would be of SHA2, which is different from CM client's metadata

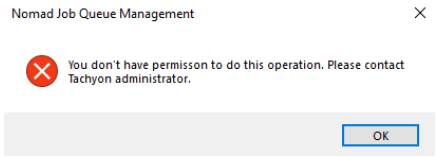
Because older clients will ignore the validation msg, the fix should be deployed on all clients

Clients will not take explicit action (For example, to disqualify) if a peer does not act on the validation msg, (But it may happen automatically, due to the resilience in an existing P2P implementation).

9.5.17 Resolving Configuration Manager Pre-caching and Nomad Pause error

If you have Nomad installed, and you select either **1E Nomad→Pre-caching** or **1E Nomad→Paused Collections** nodes in the **Monitoring** space of the Configuration Manager console, you may see the message opposite.

For a Nomad Administrator to manage Configuration Manager collections, for example to create, view and delete pre-cached and paused collections, the Nomad Administrator role will need to include the appropriate permissions. Refer to Adding Configuration Manager permissions for how to add the required permissions.



9.5.17.1 Adding Configuration Manager permissions

If you have a single AD security group for your Configuration Manager administrators, you should assign it as a member of the **Nomad Administrator** group. This allows them to use the Nomad app, view and delete pre-cache and paused collections, and use Guaranteed State features if installed.

However, if you have decided to use different roles for Nomad app and Guaranteed State features, then you can assign the same or different AD security groups to the **Nomad Administrator** and **Guaranteed State User** roles.

For more information about these features, please refer to Nomad app overview, Nomad Pre-caching, Nomad Download Pause, and the Client Health page.

The example opposite shows a Universal group called CM_Admins of which our Configuration Manager administrator account is a member.

Note

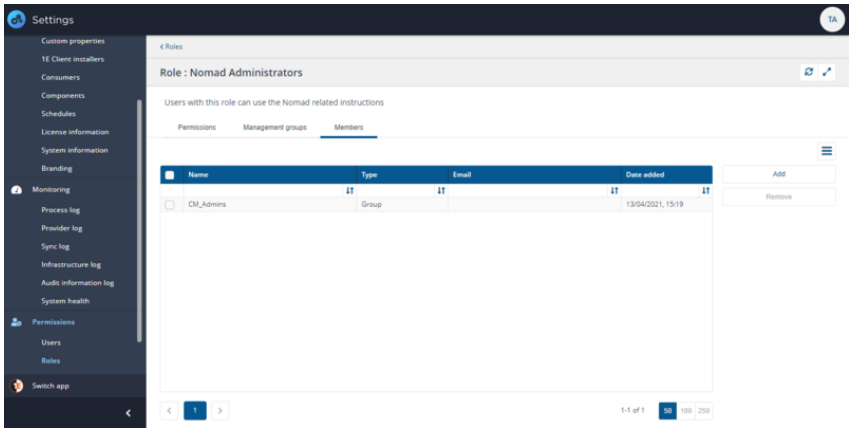
Active Directory security groups are strongly recommended for role-based access control (RBAC) but are not mandatory. AD security groups can be assigned to Tachyon roles after installation, they are not required during installation. They are added as Tachyon users and configured in the same way as AD user accounts.

A Tachyon user can therefore be a domain user account or a security group. Groups are not mandatory because users can be assigned to roles and managed within Tachyon instead of AD, or a combination.

Note

For details about how to use the **Settings** app to configure Tachyon system and application settings, refer to Tachyon Platform 8.0 - Using Settings.

For details about configuring Tachyon users, roles and management groups, refer to Tachyon Platform 8.0 - Permissions Menu.



9.6 Reference

All the Nomad related tables of information, such as supported platforms, communications ports etc.

9.6.1 Content Distribution Web API

Resource representations that are supported by the Content Distribution API for third party use.

9.6.1.1 Example scripts

ContentDistribution currently provides two example scripts:

Script	Description
Active Directory Single Site Script	Fetches site and subnet data from Active Directory and stores it in the ContentDistribution database as device tags using the Web API.
Custom Single Site script	Adds custom site and subnet data to the ContentDistribution database using the ActiveEfficiency Web API.

9.6.1.2 Supported resources

The following resource representations are supported by the Content Distribution Web API for third party use.

9.6.1.2.1 Devices

This is the primary resource representing hardware being discovered for example, desktops, servers or laptops. The following HTTP URI's and methods are supported for this resource:

URI	Method	Description
http://<server>/ActiveEfficiency/discovery/devices	GET	Retrieves a list of devices.
http://<server>/ActiveEfficiency/discovery/devices/{device id}	GET	Retrieves the single device by the id provided in the url.
http://<server>/ActiveEfficiency/discovery/devices	PUT	Adds or updates a single device.

Note

DELETE is not supported.

A device resource has the following properties:

Name	Type	Mandatory	Description
Id	unique identifier	No	A unique identifier that is assigned to the resource by the server. Needed to uniquely identify a device resource.
Identities	IList<DeviceIdentityResource>	No	A list of identities that the device is known by in other systems.
Fqdn	string	Yes	The FQDN of the device.
DomainName	string	No	The NetBIOS name of the domain (or the domain suffix for non Windows devices)

Name	Type	Mandatory	Description
NetbiosName	string	No	The NetBIOS name of the device (or host name for non Windows devices).
Type	int	No	0: Unknown 1: Desktop 2: Laptop 3: Server
CreatedBy	string	No	The name of the client creating the resource. Currently not mandatory, but will change.
CreatedTimestamp	DateTime	No	The time in UTC when the web service created the resource
ModifiedTimestamp	DateTime	No	The last time in UTC when the resource was modified.

A device identity resource has the following properties:

Name	Type	Mandatory	Description
Source	string	Yes	Name of the identity.
Identity	string	Yes	Value of the identity. This is always represented as a string even if the external source represents it as another type (integer, GUID etc.)
AssignedUtc	DateTime	No	The date/time that the external system assigned this identity to the device.

9.6.1.2.2 Device Tags

A device tag represents a name-value pair that defines a certain attribute of the device. These attributes may extend the identity of the device or may be used in defining query based collections of devices. The following HTTP URI's and methods are supported for this resource:

Uri	Method	Description
http://<server>/ActiveEfficiency/discovery/devices/{device id}/tags	GET	Retrieves a list of tags for the device specified
http://<server>/ActiveEfficiency/discovery/devices/{device id}/tags/{category}	GET	Retrieves a list of tags for the device and category specified
http://<server>/ActiveEfficiency/discovery/devices/{device id}/tags/{category}/{name}	GET	Retrieves a list of tags for the device, category and name specified
http://<server>/ActiveEfficiency/discovery/devices/{device id}/tags/{category}/{name}/{index}	GET	Retrieves a single tag for the device, category, name and index specified
http://<server>/ActiveEfficiency/discovery/devices/{device id}/tags	POST	Adds a single device tag to the list of device tags, returning the created resource. Device tags are identified

Uri	Method	Description
		by category, name and index - they do not have an explicit id. If tag with the same category, name and index already exists, the value and the modified date get updated.

DELETE is not supported.

The device tag resource has the following public properties:

Name	Type	Mandatory	Description
Category	string	Yes	The category (namespace) for the tag. The category and name uniquely identify the resource. Category is mandatory. It must not be null, empty or only whitespace.
Name	string	Yes	The tag name. Name is mandatory. It must not be null, empty or only whitespace.
StringValue	string	Yes	The value represented as a string.
Type	int	Yes	Must be 0 (string), or 1 (date/time). If date/time, value must be in universal sortable format (http://msdn.microsoft.com/en-us/library/az4se3k1.aspx)
CreatedBy	string	No	The name of the client creating the resource. Currently not mandatory, but will change.

Name	Type	Mandatory	Description
CreatedTimestamp	string	No	The UTC time when the web service created the resource.
ModifiedTimestamp	string	No	The last UTC time when the resource was modified.

9.6.1.2.3 Location

These location resources are used by Nomad to identify subnets contained within the same site. These are pre-populated by some out-of-band method (e.g. PowerShell script). They are not directly consumed by Nomad (the web service determines which Content Delivery resources to return based on the contents of the location section of its database).

URI	Method	Description
http://<server>/ActiveEfficiency/locations/	POST	Adds a single location resource (returns its unique identifier).
http://<server>/ActiveEfficiency/locations/{id}/	GET	Returns a specific location resource using its unique identifier.
http://<server>/ActiveEfficiency/locations/	GET	Returns a listing of all location resources.
http://<server>/ActiveEfficiency/locations/{id}	DELETE	Removes a single location record using its unique identifier.
http://<server>/ActiveEfficiency/locations/	DELETE	Removes all location records.

Location resources have the following public properties:

Name	Type	Mandatory	Description
Id	GUID	Yes	Unique identifier for this location (auto-generated).
Site	string	Yes	Name of Site that this Location belongs to. Arbitrary and used to find related Subnets.

Name	Type	Mandatory	Description
Subnet	string	Yes	Subnet (for example, "10.0.10.0/24")

9.6.1.2.4 Pre-cached jobs

These content distribution job resources are used to manage pre-cached jobs and retrieve download notifications:

URI	Method	Description
http://<server>/ActiveEfficiency/ContentDistributionJobs/	POST	Creates, view and delete pre-cached jobs.
http://<server>/ActiveEfficiency/ContentDownloadNotifications/{id}/	GET	Retrieves download notifications

Content distribution job resources have the following public properties:

Name	Type	Mandatory	Description
Id	unique identifier	No	Identifier for the resource.
DeviceFqdns	Array of strings	Yes	List of device FQDNs
ContentItems	Array of content items	Yes	List of contents. Must include the ID and version of the content.
UserData	XML	No	Additional details about job.

Content download notifications have the following public properties:

Name	Type	Mandatory	Description
ContentId	string	Yes	Identifier for the content.
Version	string	Yes	Version of the content.

Name	Type	Mandatory	Description
Hash	string	No	SHA-256 hash to verify integrity of files inside content

9.6.1.2.5 Managing large amounts of data

ODATA is an open standard that allows clients to consume data feeds in an open format and was designed for this purpose. The web service supports ODATA so that the clients can ask for pages of data. Assuming that the web service contains 1000 devices, the following are examples of how ODATA helps us:

9.6.1.2.5.1 Without ODATA

Without ODATA, the following url returns 1000 devices in one go; no good if the client limits the buffer size:

```
http://<server>/ActiveEfficiency/devices [GET] ;
```

returns 1000 devices in one go

9.6.1.2.5.2 With ODATA

ODATA supports the keyword **top** and **skip** which allows you to implement the following loop:

```
http://<server>/ActiveEfficiency/devices?$top=100&$skip=0;
```

returns the first 100 devices

```
http://<server>/ActiveEfficiency/devices?$top=100&$skip=100;
```

returns the next 100 devices

```
http://<server>/ActiveEfficiency/devices?$top=100&$skip=200;
```

returns the next 100 devices and so on.

9.6.2 Nomad app

The Nomad app provides visibility of content distribution activity and cache status for content distributed by both Nomad and Delivery Optimization. This includes Configuration Manager content distributed with Nomad and Software Updates content distributed with either Nomad or Delivery Optimization.

The Nomad app **Overview** page gives a high-level view of the current status of content throughout the entire network. By default, the view will show activity and status for both Nomad and Delivery Optimization. These defaults can be modified using the **Technology** filter (to show Nomad or DO activity only) and the **Time period** filter. You can use the Nomad app, powered by the Tachyon Platform, to get a visual snapshot of download activity in your environment.

The Nomad app provides visibility of content distribution activity and cache status for content distributed by both Nomad and Delivery Optimization and consists of the pages listed in this table:

Nomad page	Description
Overview page	Provides a visual snapshot of download activity.
Content page	Lists unique contents synced from MEMCM, including applications, packages and software updates.
Task Sequences page	Lists configured task sequences.
Devices page	Lists every device registered to Nomad.
Nomad Sites page	Primarily designed to show how the network is being used for content distribution in different locations.
Client Health page	Primarily designed to show related data from Using Guaranteed State.

The first version includes Configuration Manager content distributed with Nomad and Software Updates content distributed with either Nomad or Delivery Optimization. Future releases will include Intune and Microsoft Store content distributed with Delivery Optimization as well as other content, such as VMWare Workspace One and 1E Tachyon content distributed with Nomad.

The Nomad app will be available after you install the Tachyon Platform and can be accessed using the Tachyon DNS Alias FQDN. For example:

https://tachyon.acme.local/Tachyon

Although not a requirement for generally using Nomad, Tachyon Platform must be installed and available before you can use certain Nomad features.

The following Nomad features use Content Distribution and require Tachyon Platform and Tachyon features of 1E Client to be enabled:

Nomad app provides visibility of content distribution activity

Single Site Download (SSD)

Single Site Peer Backup Assistant (SSPBA)

High Availability Peer Backup Assistant (HAPBA)

Get Migration Settings task sequence action used to manage computer associations

Nomad Pre-caching

Nomad Download Pause.

Note

Nomad versions prior to Nomad 7.1 used ActiveEfficiency to support similar features. Tachyon platform previously included ActiveEfficiency.

The following features were provided in versions of Nomad older than Nomad 7.1:

1E Client Health - now provided by the Guaranteed State feature of the Tachyon Platform

Nomad Dashboard - now provided by Nomad app feature of the Tachyon Platform.

These features require the full deployment of the Tachyon Platform infrastructure, including Master and Response Stacks, with an optional DMZ Server for Internet based clients.

Tachyon Platform is installed using Tachyon Setup, which should also be used to install the following components, included in the Tachyon Platform download zip.

Nomad app - this consumer application replaces the legacy Nomad Dashboard

Content Distribution - this web service is required by the Nomad app, and replaces the legacy ActiveEfficiency Server.

Please refer to:

Requirements for prerequisites

Introducing Tachyon for details about the Tachyon Platform and other optional applications and features.

9.6.2.1 Overview page

9.6.2.1.1 Explaining content versions

In Configuration Manager (CM), the content associated with a Package or Application Deployment Type may be updated by an administrator. In the case of Packages, CM increases the Package Version property, and for Application Deployment Types, CM generates a new Content ID for the Deployment Type.

The Nomad Overview page displays summarized distribution data for a selected period. The displayed data shows all downloads and download activity for all versions of content for that period. For example, if a device downloaded Package A version 1 a month ago and later downloaded version 2 of the same Package, the Overview page would reflect both downloads.

In this version it has not been possible to reflect previous versions in the **Content Titles** summary in the top status bar, or in the **Content Titles Count by Content Type** and **Download Volume by Content Type** tiles. These will only represent download activity for the latest version of content. This may result in apparent 'loss' of data (e.g. a reduction in the number of content titles or download volume) when content for an existing Package or Application is updated in CM, as these metrics will only include download activity for the latest version. This will be addressed in a later version of Nomad.

> **Note**
>
> Other pages in the app, such as the Content page, only show the latest version of any given **Content Title**. Those pages concern the current state of things (e.g. where content is available) because only the latest version is usable by CM deployments. As a result, showing older versions would be misleading for users.

The **Overview** page gives a brief snapshot of download activity. The page has multiple tiles showing:

Content Titles by Content type

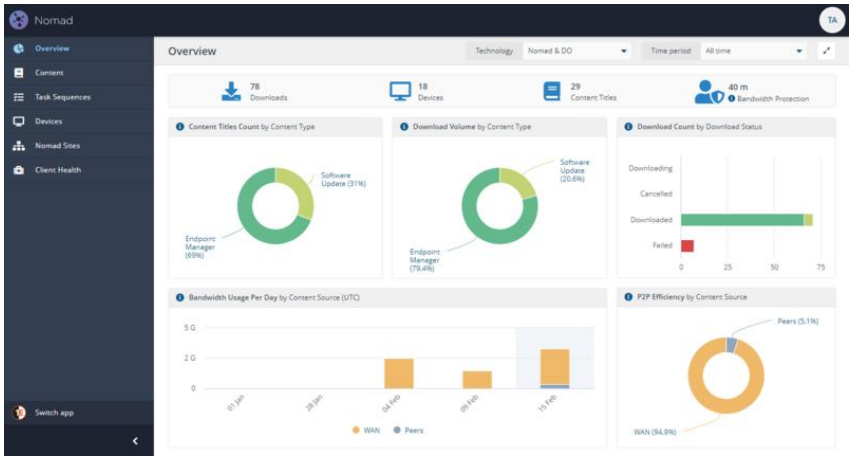
Download Volume by Content Type

Download Count by Download Status

Bandwidth Usage Per Day by Content Source (UTC)

P2P Efficiency by Content Source (Peer to Peer - P2P).

The results can further be narrowed down by using the **Technology** and **Time period** filters on the page.



9.6.2.1.2 Navigation and Filtering

By default, the view shows activity and status for all time and will show activity and status for both Nomad and Delivery Optimization. These defaults can be modified using the **Technology** filter and the **Time period** filter.

> **Note**
>
> Each content tile can be expanded using the **Expand** button on the top right-hand corner of each tile.

9.6.2.1.2.1 Time period filter

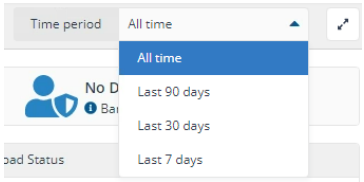
Using the **Time period**filter at the top of the page, you can narrow down the results by date. You can choose from the following options:

Last 90 days

Last 30 days (Default)

Last 7 days.

> **Note**
>
> If these filters are applied to any app page, it is reflected on all other pages in the Nomad App.



9.6.2.1.2.2 *Technology filter*

You can use the **Technology** filter to differentiate between downloads through Nomad or Delivery Optimization (DO).

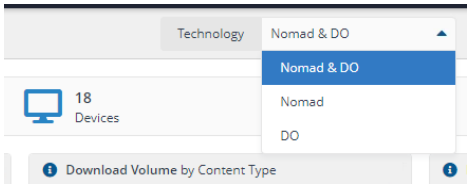
The following options are available:

Nomad & DO (Default)

Nomad

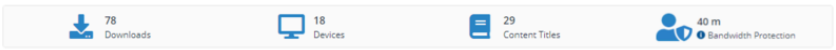
DO.

> **Note**
>
> If this filter is applied to any app page, it is reflected on all other pages in the Nomad App.



9.6.2.1.3 Top status bar

The status bar along the top of the page shows high-level statistics for the currently selected **Technology** (Nomad or DO) and **Time period**. The bar is shown on the Overview page and includes four icons, **Downloads**, **Devices**, **Content Titles** and **Bandwidth Protection**.



Item	Description	Icon
Downloads	Downloads reflect the total number of content downloads. This includes both Delivery Optimization (DO) and Nomad downloads. The results can be filtered on the **Time period** and **Technology** filters and display the total number of downloads of any version of content that occurred in the selected period. A download counts as any download activity for a given Content Title on a given device. For example, if there are 10 content titles downloaded by 50 devices, the total count of download instances would be 500.	

Item	Description	Icon
	For CM Applications, each Application Deployment Type counts as a separate Content Title. Clicking on this icon navigates to the **Content** page filtered to show **Content Titles** reporting download activity within the selected **Time period**.	
Devices	Displays the total number of devices that have reported download activity for any content version in the selected **Time period**, including: Packages Applications Updates from Configuration Manager. Clicking this icon navigates to the **Devices** view, filtered to show devices where download activity was reported within the selected **Time period**.	
Content Titles	Displays the total number of unique **Content Titles** where download activity of the latest version of the content titleis reportedin the selected**Time period.** For CM content, a**Content Title**is a single Application or Package. Clicking on this icon navigates to the Content view filtered to show the **Content Titles** that have reported download activity within the selected**Time period.** **Note** Applications in CM may have many Deployment Types. This summary counts an Application as a single Content Title.When viewing the Content view, Content Titles for CM Applications are further identified with the Deployment Type thatwas downloaded. So, the total number of Content Titles identified on the top status bar may be lower than the corresponding list of Content Titles on the Content page. This is because the Content page reports download activity for individual Deployment Types of CM Applications.	

Item	Description	Icon
Bandwidth Protection	Displays the total time that Nomad backed off when downloading content to protect end-user bandwidth. **Bandwidth Protection** allows Nomad to adjust the speed of ongoing downloads to save bandwidth for other business use. Bandwidth Protection ensures Nomad doesn't consume excess bandwidth and hinder other business activity.It does that by tracking the download time of data packets. If the time increases, it slows itself down (backing off) by sleeping for a few moments before downloading another packet.	

9.6.2.1.4 Content tiles

Content tiles display statistics for content download activity in the following panes:

Content Titles Count by Content Type

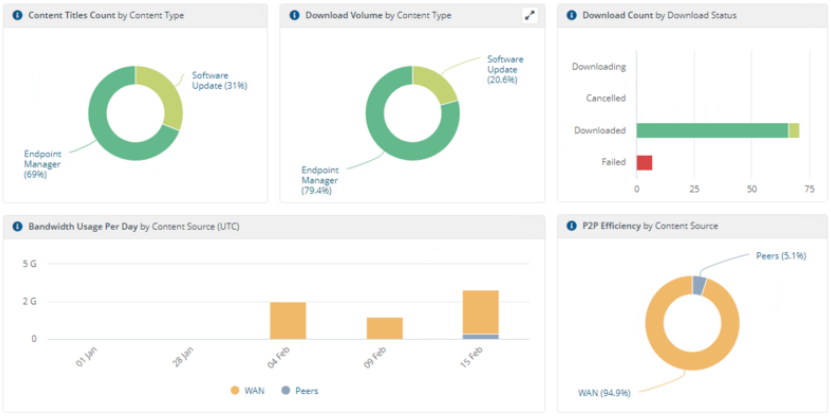
Download Volume by Content Type

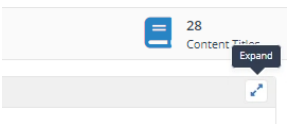
Download Count by Download Status

P2P Efficiency by Content Source

Bandwidth Usage Per Day by Content Source UTC.

> **Note**
>
> Each content tile can be expanded using the **Expand** button on the top right-hand corner of each tile.





9.6.2.1.4.1 Content Titles Count by Content Type

The **Content Title Count by Content Type** tile shows the total number of unique **Content Titles** for where there is download activity reported for the latest version of the content within the selected **Time period**.

The data is grouped by **Content Type** and displayed as a donut chart. The app currently reports on two **Content Types**:

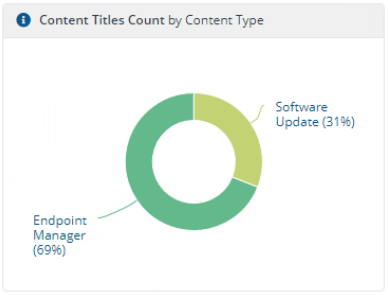
Endpoint Manager - CM applications and packages that are not delivered by DO

Software Update - includes any Microsoft Software Updates deployed through CM or Windows Update.

> **Note**
>
> Applications in CM may have multiple **Deployment Types**. This tile counts an Application as a single **Content Title**. When viewing the **Content view**, **Content Titles** for CM Applications are further identified with the **Deployment Type** that was downloaded.
>
> As a result, the total number of **Content Titles** identified on the top status bar may be lower than the corresponding list of Content Titles on the Content page (which reports download activity for individual **Deployment Types** of CM Applications).

Hovering over a **Content Type** segment of the chart displays the count of **Content Titles** of that type, also represented as a percentage of all **Content Titles**.

Clicking on a **Content Type** segment of the chart will navigate to the **Content** view, filtered to show related **Content Titles**.



9.6.2.1.4.2 Download Volume by Content Type

The **Download Volume by Content Type** tile shows the cumulative volume of content of the latest version of content downloaded by all devices within the selected **Time period**. The data is grouped by **Content Type** and displayed as a donut chart.

The chart enables you to see the effect that different types of content have on your network, in terms of the volume of data associated with them. It shows the percentage of packages and software updates by volume for:

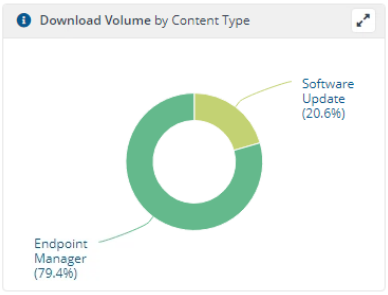
Endpoint Manager - CM applications and packages that are not delivered by DO

Software Update - content that can be delivered by Nomad, or DO if you're using Windows Update directly.

For example, if a single content title is 100MB and it is downloaded by 100 devices, the cumulative **Download Volume** reported for that particular **Content Title** would be 10,000MB. The chart shows the cumulative volume for all **Content Titles** on all devices, grouped by **Content Type**.

Hovering over a **Content Type** segment of the chart displays the total volume of downloaded content of that type. This is also shown as a percentage of total volume of downloaded content.

Clicking on a **Content Type** segment of the chart navigates to the **Content** view, filtered to show **Content Titles** of the selected segment.



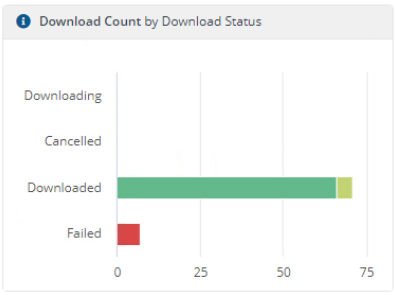
9.6.2.1.4.3 Download Count by Download Status

The **Download Count by Download Status** tile shows the status of download activity within the selected **Time period**, displayed as a bar chart by:

Status	Description
Downloading	Number of downloads currently in progress, where a download has been reported as started but has not yet reported complete, failed or cancelled.
Cancelled	Number of downloads whose last reported status was **Cancelled**, downloads may be cancelled by the user, or by the system, for example if the system is shut down or higher priority downloads are queued.
Downloaded	Number of successful downloads, if the downloaded content is still cached on a given device, it's represented by the dark green part of the Downloaded bar labelled **(Downloaded (Cached)** when you hover over it. If the downloaded content was subsequently deleted from the cache on a given device, it's represented in the light green part of the **Downloaded** bar labelled **(Downloaded (Deleted)** when you hover over it.
Failed	Number of downloads whose last reported status was **Failed**.

Hovering over any of the bars displays the number of downloads in the selected download state.

Clicking on any of the bars navigates to the **Content** view, filtered to include **Content Titles** where one or more devices is in the selected download state.



9.6.2.1.4.4 Bandwidth Usage Per Day by Content Source (UTC)

The **Bandwidth Usage Per Day by Content Source (UTC)** tile represents daily download activity throughout the entire network during the selected **Time period**.

A column is displayed for each day when there was download activity. Each column indicates the volume of content downloaded over the WAN (in orange) or from peers (in grey). Hovering over a segment of the column will display the volume of content downloaded on that day.

This view demonstrates the value that Nomad and Delivery Optimization are providing through reduced WAN traffic. If the majority of content is being downloaded over the WAN, it could indicate that peers are simply not available (e.g. users working from home) or it could be an indication that Nomad or Delivery Optimization are not correctly configured to optimize content from peers.

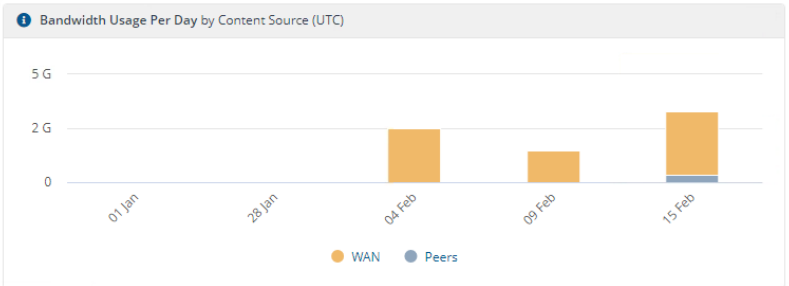
The columns on this chart are not clickable, they are for data visualization only and do not navigate to another view of the data.

> **Tip**
>
> On the Overview page, when you select the **All Time** filter, the **Bandwidth Usage Per Day by Content Source (UTC)** graph displays a maximum 365 days of data.

> **Note**
>
> This chart only displays content that was downloaded over the network either from a peer or from the source (e.g. a CM Distribution Point), if a device:

Requests content that is already in its cache, it will not be represented in this chart

Only has some content in its cache and downloads the remainder of the content from peers or the source, the content that was downloaded will be shown.



9.6.2.1.4.5 P2P Efficiency by Content Source

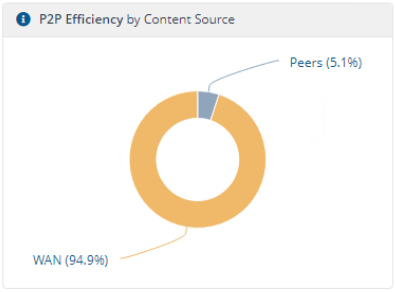
The **P2P Efficiency by Content Source** tile represents the overall peer-to-peer efficiency across the entire network during the selected **Time period**.

The data is grouped by source (Peers and WAN) and displayed as a donut chart showing the volume of content downloaded from peers (in grey) and from the source over the WAN (in orange). This gives an indication of the overall value of Nomad and Delivery Optimization across your organization.

Ideally, more content will be downloaded from peers than from the source over the WAN, which saves network bandwidth. Where this is not the case, it could be due to many users working remotely without any local peers, or it could be due to configuration settings on the client that are not optimized for peer-to-peer caching and availability.

This chart is not clickable, it is summary data visualization only and does not navigate to another view of the data.

> **Note**
>
> In this chart, the volume of content downloaded from peers includes any content requested by a device during the selected **Time period** and was already in the cache at the time (i.e. 'already cached' is represented as content obtained from a peer). If the content was downloaded from a peer or over the WAN during the selected **Time period**, it will be represented accordingly.



9.6.2.2 Content page

The Content page provides a Content-centric view of content distributed throughout your network. It shows all Content Titles where there has been download activity for the latest version of that content within the selected Time period.

> **Note**
>
> The Content page shows you where your content is. As a result, this page does not include downloads of older versions of Configuration Manager (CM) Packages and Application Deployment Types, they are no longer relevant as they can't be used by any CM deployments.
>
> For example, if a device downloads Package A version 1, then Package A gets updated to version 2 but not yet downloaded by the device, the Content Title will not be seen as downloaded on that device. If the device then downloads the latest version then it will be represented against that Content Title.

Software Updates and CM Packages are each represented in a single row. CM Applications are represented as one row per Deployment Type, where the**Content Titles**comprise the Application Name with the Deployment Type name appended.

For example, you can see this with the **1E Client 5.2.3.146** application in the picture opposite, which has three Deployment Types - **1E Client x64 -Server Install**, **1E Client x86** and **1E Client x64**.

On the **Overview** page, a CM Application is counted as a single **Content Title** regardless of how many Deployment Types it contains.

Note

Download activity and Configuration Manager data synchronization

The Nomad client uses Events (a feature of the Tachyon Platform) to update the Nomad app with the latest status of a download. Events are currently not processed and represented in the app unless the **Content Title** is known, except for these tiles:

Bandwidth Usage Per Day by Content Source (UTC)

P2P Efficiency by Content Source.

Events generated for Nomad downloads (i.e. CM Applications, Packages and Software Updates downloaded by Nomad) only identify the content ID, not the content title. The content title is determined through the CM sync that Content Distribution performs periodically. By default, this runs every 30 minutes, and is configured in the following location on your Tachyon Platform server:

C:\Program Files\1E\ContentDistribution\Web\WebService\AppSettings.json

The CM Sync currently synchronizes the following **Content Titles**:

Content for which there have been any download events

Reference content in any Task Sequence

Content for which a pre-cache job has been created.

This means that in many cases, events for new CM deployments will not be represented in the app until the first CM sync after the first events for that content are reported.

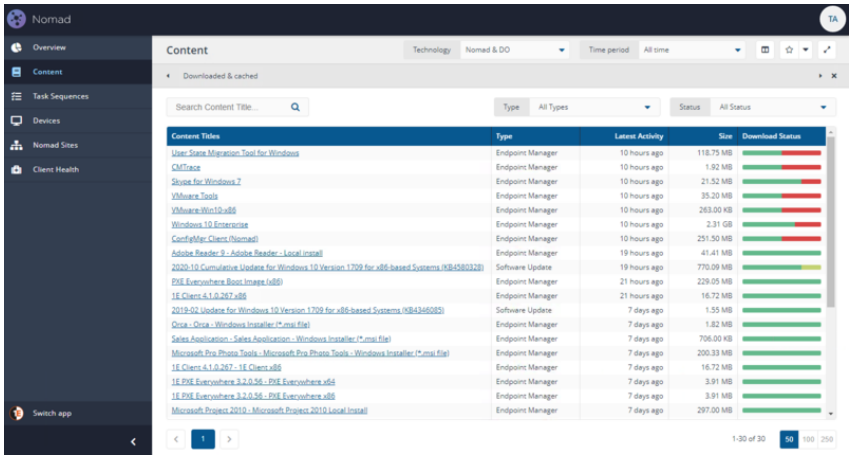
Events generated for software updates downloaded by DO include the **Content Title** in the event as this is determined at the client. These events are represented immediately in the Nomad app.

The table includes the following columns:

Column	Description
Content Title	Content title.

Column	Description
	For CM Packages, this is the Package name For CM Applications, this is a combination of the Application name and Deployment Type name For Software Updates, this is the title of the Software Update as defined in the Microsoft Update catalog (this is collected from the client, not the Microsoft Catalog).
Type	Currently, either **Endpoint Manager** or **Software Update**.
Latest Activity	Date and time of the latest event for the content title.
Size	Size of the CM Package, CM Application Deployment Type or Software Update.
Download Status	Represents the current status of the content across all devices, that have reported events for this Content Title within the selected **Time period**. This can include the following status: **Downloading** **Cancelled** **Downloaded** **Downloaded (Cached)** **Downloaded (Deleted)** **Failed.** Clicking on a **Content Title** navigates to the **Content Detail** page for that **Content Title**. **Note** If a download is **Cancelled** before completing and the partial content is then deleted from the cache on the device, the reported status for that **Content Title** will remain **Cancelled**. **Downloaded (Deleted)** only applies to **Content Titles** that completed download and were subsequently deleted. There is currently no status for Cancelled (Deleted).

Column	Description
	Hovering over the **Download Status** bar displays the count of downloads in each state. The bar is for information only and is not clickable (It will not navigate to a filtered list of devices).



9.6.2.2.1 Navigation and Filtering

You can navigate to the Content page from the Overview page, in which case the Content page will be filtered with the filter selections and the element you clicked on (e.g. a **Content Type** segment in the **Content Titles by Content Type** chart).

If you navigate directly to the Content page from the left-hand navigation menu, the Content page will show all **Content Titles** by default. You can filter **Content Titles** using the filters at the top of the page:

Technology

Time period

Type

Status.

These filters are kept for the current browser session as you navigate your way around the app.

> **Note**
>
> **Content Titles** are sorted by latest activity, so you always see the most recent content activity at the top of the list. You can use the **Search Content Title...** box to search for a specific Content Title.

9.6.2.2.1.1 Technology filter

You can use the **Technology** filter to differentiate between downloads through Nomad or Delivery Optimization (DO).

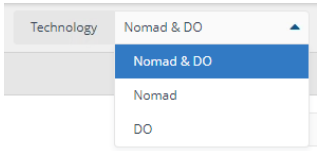
The following options are available:

Nomad & DO (Default)

Nomad

DO.

> **Note**
>
> If this filter is applied to any app page, it is reflected on all other pages in the Nomad App.



9.6.2.2.1.2 Time period filter

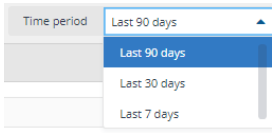
Using the **Time period**filter at the top of the page, you can narrow down the results by date. You can choose from the following options:

Last 90 days

Last 30 days (Default)

Last 7 days.

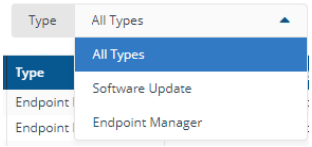
> **Note**
>
> If these filters are applied to any app page, it is reflected on all other pages in the Nomad App.



9.6.2.2.1.3 Type

Using the **Type** filter, you can filter results by either:

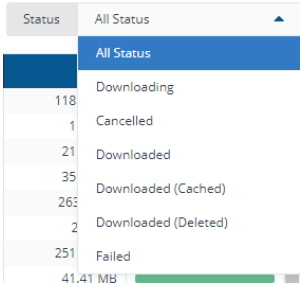
Type	Description
All Types	Default.
Software Update	Content that can be delivered by Nomad, or Delivery Optimization (DO if you're using Windows Update directly.
Endpoint Manager	Configuration Manager applications and packages that are not delivered by DO.



9.6.2.2.1.4 Status

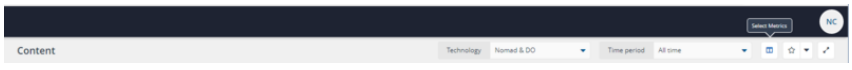
Using the Status filter, you can filter results by download status:

Status	Description
Downloading	Number of downloads currently in progress, where a download has been reported as started but has not yet reported complete, failed or cancelled.
Cancelled	Number of downloads whose last reported status was **Cancelled**, downloads may be cancelled by the user, or by the system, for example if the system is shut down or higher priority downloads are queued.
Downloaded	Number of successful downloads.
Downloaded (Cached)	Downloaded content cached on a given device.
(Downloaded (Deleted)	Downloaded content was subsequently deleted from the cache on a given device.
Failed	Number of downloads whose last reported status was **Failed**.



9.6.2.2.1.5 Select Columns

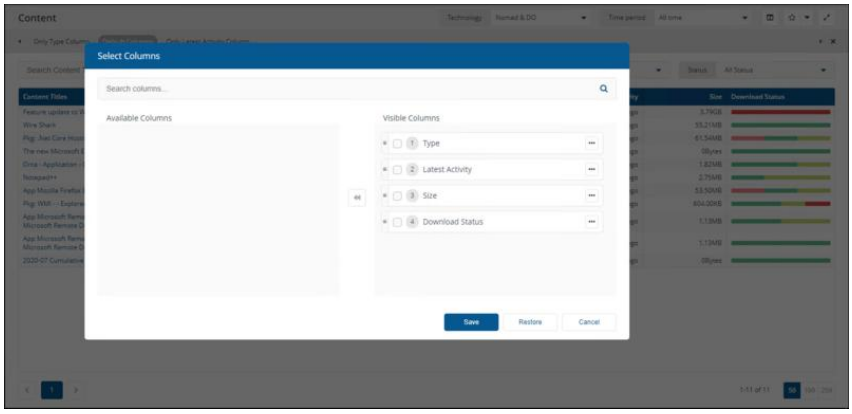
You can select the columns to be displayed by clicking on the **Select Columns** option. You can add, remove or re-order the columns in the **Visible Columns** section.



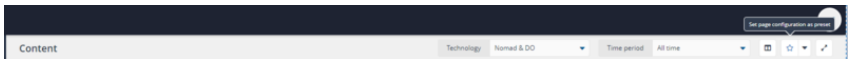
When you click on the **Select columns** control, it opens a pop-up displaying every column on the current screen, the controls are:

Control	Explanation
Available Columns	Columns, which are by default hidden from display on screen. You can still include any of them to display on screen.
Visible Columns	Displays the list of columns displayed on screen.
Arrow buttons	To move up or move down, exclude or include any column, clicking on the ellipsis displays these additional controls.
Drag and drop	You can drag and drop columns to change how they are displayed.
Exclude columns	Exclude column button allows you to select columns to exclude from the current display.

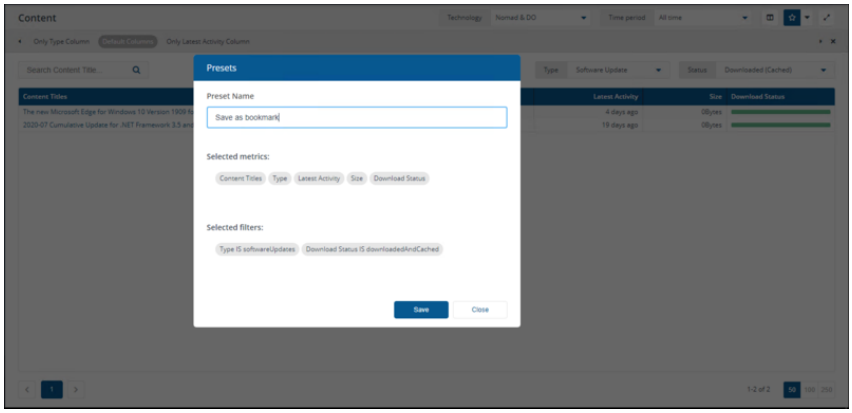
Clicking **Save** on the **Select Columns** screen saves the layout for the current browser session. Clicking **Restore** returns the columns to the default selection.



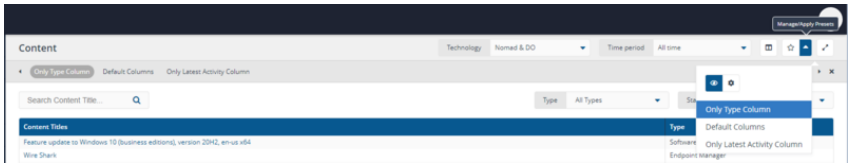
After selecting the columns and any other configurations on the page, you can set them as a preset, so you can select them again after your current browser session.



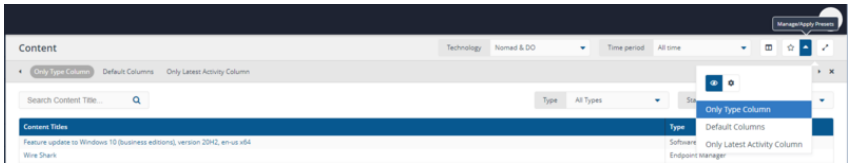
You can save a view as a preset by clicking on the star icon, doing this presents the screen shown opposite. Clicking **Save** adds the view to the list of preset list.



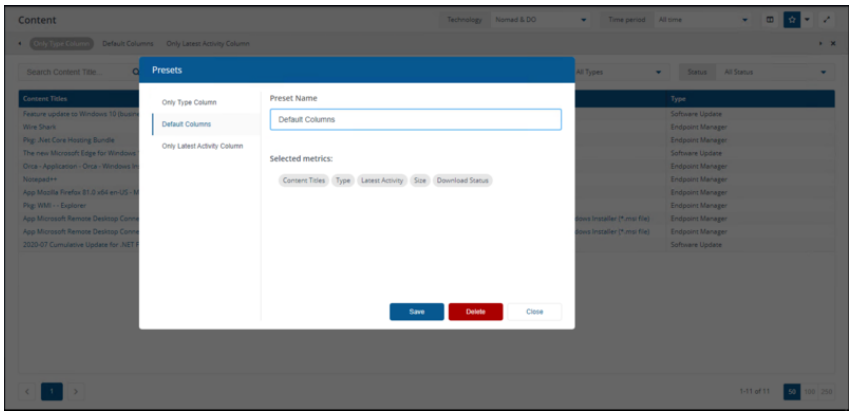
You can apply any saved preset later, either from the list of configured presets or from the bookmark bar of the configured presets when you click **Manage/Apply Presets**.



In this example, the preset **Only Latest Activity Column** is selected.



You can also manage (rename or delete) your saved **Presets**.



9.6.2.2.2 Content details

The Content detail page is displayed when you click on a content title anywhere in the app. It includes a **Summary** tab and a **Devices** tab.

> **Note**
>
> The Content detail page does not 'inherit' the **Time period** filter from other pages. It represents all available data for the selected **Content Title**. As a result, if you have set

the **Time period** filter on the **Content** page to, for example, **Last 7 days**, you may see different results on the content details page.

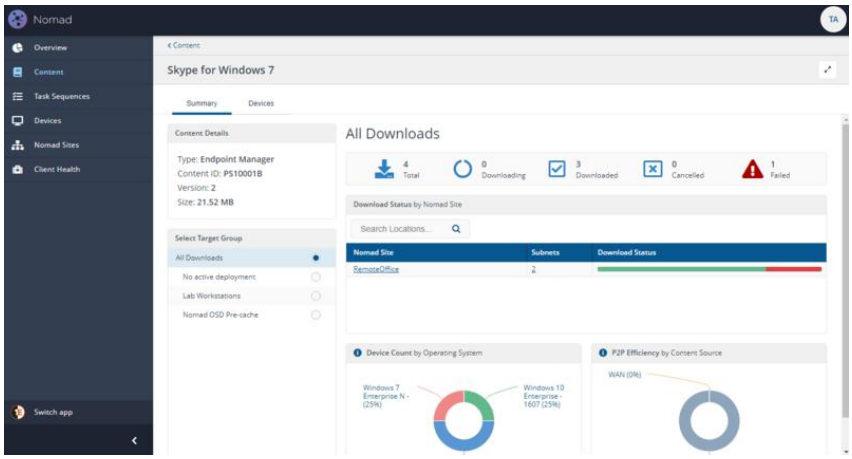
9.6.2.2.2.1 Summary tab

The Summary tab shows summary information about the selected content title.

9.6.2.2.2.1.1 Top status Bar

The top status bar displays the following high-level statistics:

Status	Description
Total	Displays the number of downloads for the latest version of the selected **Content Title**. If the **Content Title** is a CM Application, this number represents the total number of downloads of all of that Application's Deployment Types.
Downloading	Displays the number of devices that are currently downloading the latest version of the **Content Title**.
Downloaded	Displays the number of downloads of the latest version of the **Content Title** that have completed successfully.
Cancelled	Displays the number of downloads of the latest version of the **Content Title** whose latest state was **Cancelled**.
Failed	Displays the number of downloads of the latest version of the **Content Title** whose latest state was **Failed**.



9.6.2.2.2.1.2 Side Panels

On the left side of the page, there are two panels:

Content Details

Select Target Group.

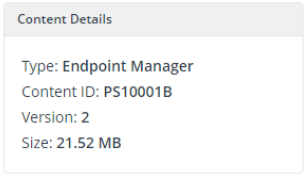
9.6.2.2.2.1.3 Content Details

Displays the content **Type** and the **Size** of the content for:

CM Packages, the size represents the total size of the Package content

CM Applications, the **Size** represents the total size of all Deployment Types

Software Updates, the size represents the total size of the update reported by the update metadata.



9.6.2.2.2.1.4 Select Target Group

Allows the details on the main page to be filtered based on the target group. By default, the main details page shows data for **All Downloads** of the Content Title. In this panel, below**All Downloads**is a list of every Collection in CM that the content has been either deployed or pre-cached to.

You use the **Select Target Group** filter in the following scenarios

To view the status of a specific CM deployment

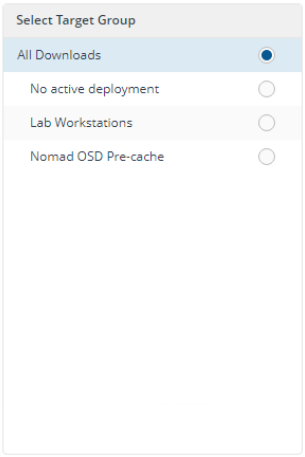
To view the status of a specific Nomad Pre-cache Job.

> **Note**
>
> Although currently this only lists CM Collections, the term Target Group is used in the app as in future the target may be a CM Collection, an Azure AD group (for Intune applications), a Tachyon Management Group or perhaps another type of target group entirely used by other management systems.

There are different options for Endpoint Manager (Configuration Manager) and for the Software Update Content Type:

Content Type	Option	Description
Endpoint Manager (Configuration Manager)	**All Downloads**	(default) shows data for all downloads.
No active deployments	Shows data for downloads that occurred, but no longer have an active deployment (for	

Content Type	Option	Description
	example where a Deployment was deleted).	
Collections	A list of **Collections** that are either the target of an active deployment of the Content Title. Or are the target of a Nomad Pre-cache job.	
Software Update	**All Downloads**	(default) shows data for all downloads
On Demand	Shows downloads initiated through Windows Update on the device.	
No active deployments	Shows data for downloads that occurred, but no longer have an active deployment (for example where a Deployment was deleted).	
Collections	A list of **Collections** that are the target of an active deployment of the Content Title.	



9.6.2.2.2.1.5 Download Status by Nomad Site

Using the **Download Status by Nomad Site** tile you can see in which locations (Nomad Single Site Download (SSD) sites) the content title has been downloaded and is available.

The table shows the status of the selected **Content Title** in each Nomad Site. A Nomad Site corresponds to Nomad Single Site Download site. Customers that have implemented SSD and upgraded ActiveEfficiency to Content Distribution will see their defined SSD locations displayed as Nomad Sites on this tile. Any subnets that are not included in a Nomad SSD Site definition will be represented in a site named **Unknown**. If no SSD sites have been defined, all subnets will be included in the **Unknown** site.

The table displays the following columns:

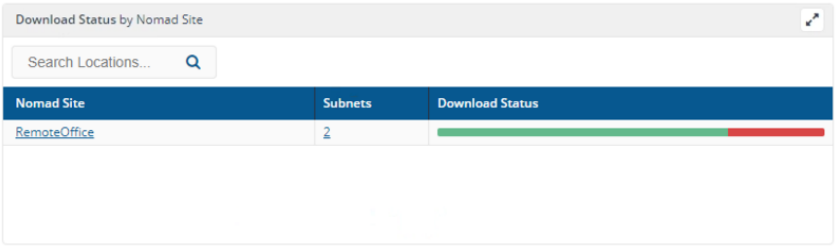
Column	Description
Nomad Site	The Nomad (SSD) site name.
Subnets	The count of subnets included in the Nomad site. Clicking on the number opens a 'drawer' that shows the download status for each subnet in the site. You can click on the subnet in this drawer to view the devices in that subnet that have reported download activity for the Content Title.
Download Status	A bar representing the current status of the content across all devices in the Nomad Site. This can include the following statuses: Downloading Downloaded (Cached) Downloaded (Deleted) Cancelled Failed Unknown. **Note** The **Unknown** status is only displayed if a Target Group has been selected. It indicates the members of the Target Group for which no status for the selected Content Title has been reported.

Hovering over the **Download Status** bar displays the count of downloads in each state. The bar is for information only and is not clickable (i.e. it will not navigate to a filtered list of devices in the various states).

Clicking on a **Nomad Site** navigates to the **Devices** tab, filtered to display devices in the selected **Nomad Site**.

Note

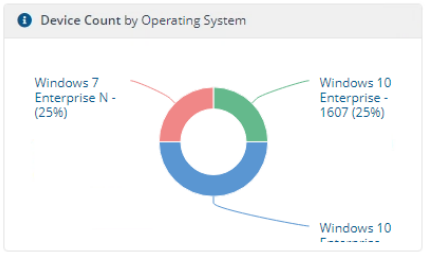
You can use the **Search Locations...** box to search for a specific Nomad Sites.



9.6.2.2.2.1.6 Device Count by Operating system

The **Device Count by Operating System** represents the devices that have downloaded the selected Content Title grouped by Operating System and version and displayed as a donut chart. Delivery Optimization is a Windows 10 feature, but the feature continues to develop with new features and configuration options available in different versions. This data point can help to identify differences across Windows 10 versions.

Clicking on any segment of the chart navigates to the **Devices** tab, filtered to show the devices running the selected OS version.

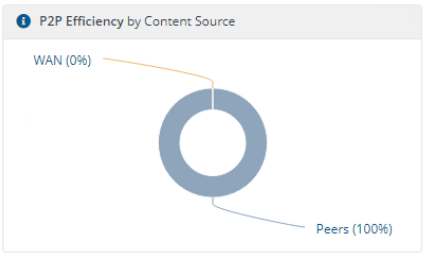


9.6.2.2.2.1.7 P2P Efficiency by Content Source

The **P2P Efficiency by Content Source** tile represents the overall peer-to-peer efficiency across the entire network for the selected Content Title. The data is grouped by source (**Peers** and **WAN**) and displayed as a donut chart showing the volume of content downloaded from peers (in grey) and from the source over the WAN (in orange).

Ideally, more content will be downloaded from peers than from the source over the WAN, thereby saving network bandwidth. Where this is not the case, it could be due to many users working remotely without any local peers, or it could be due to configuration settings on the client that are not optimized for peer-to-peer caching and availability. It may also be worth considering pre-caching the Content Title in more locations to improve the availability of the content on peers in each location.

Clicking either segment in this chart will navigate to the **Devices** tab filtered to show the devices that downloaded the selected Content Title from **Peers** or **WAN**, according to the segment that you clicked on.



9.6.2.2.2.2 Devices tab

The **Devices** tab in the Content detail page lists the devices that have reported download activity or cache status for the selected Content Title.

This tab is displayed when you click a Nomad Site or a segment on the**Device Count by Operating system**or**P2P Efficiency by Content Source**charts on the**Content Detail** summary tab, filtered according to the item clicked on.

Alternatively you can select the tab to view all devices that have reported download activity for the content title. Use the**Search Devices...**box to search for a specific device.

> **Note**
>
> The list can be further organized using the filters:

Source - (Peers or WAN)

Status:

Downloading

Downloaded (Cached)

Downloaded (Deleted)

Cancelled

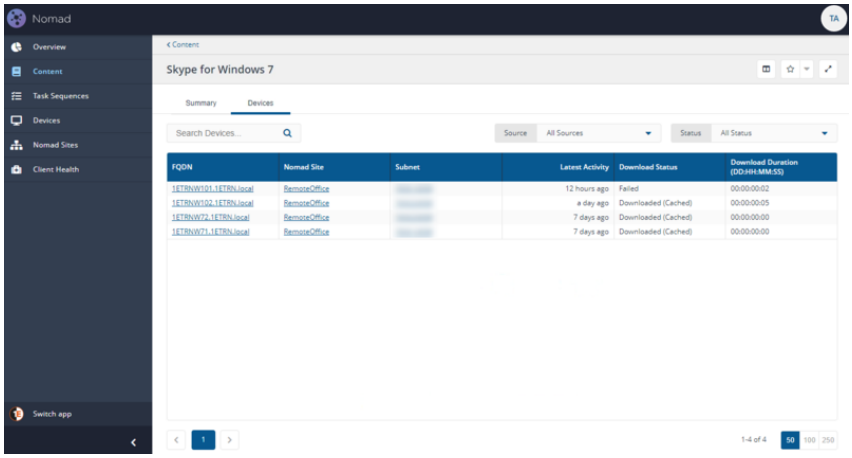
Failed

Unknown.

The table of Devices displays the following columns and from this list, you can click on an FQDN to view details of the specific device on the Devices page.

Column	Description
FQDN	Fully Qualified Domain Name.
Nomad Site	The Nomad SSD Site that the device is currently in, based on the device's latest device registration.
Subnet	The subnet the device is currently in, based on the device's latest device registration.

Column	Description
Latest Activity	Indication of how long ago the latest download activity for the selected Content Title occurred on this device.
Download Status	Status of the selected Content Title on this device, one of: Downloading Downloaded (Cached) Downloaded (Deleted) Cancelled Failed.
Download Duration (DD:HH:MM:SS)	The amount of time it took to download the content.



9.6.2.3 Task Sequences page

Configuration Manager (CM) Task Sequences typically use multiple Packages and Applications, called Reference Content. Those packages and applications may be distributed in their own right, or may be distributed through one or more Task Sequence. As an administrator, you want to know where the content that the Task Sequence requires has been cached.

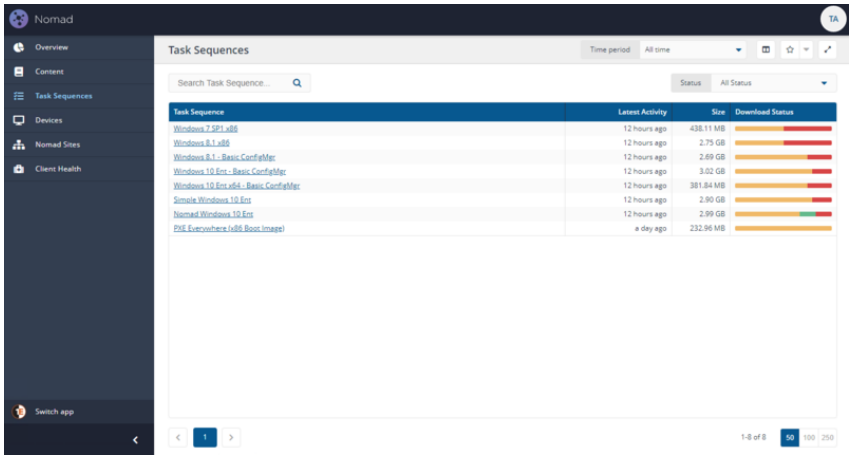
For example, you might pre-cache a Task Sequence (which will pre-cache all reference content) ahead of deploying it to devices, and you want to confirm that pre-caching has been successful before starting the deployment. The Task Sequences page provides that visibility by grouping the reference content for each Task Sequence into a single view, so you can see which content is cached and which is not. The Task Sequences table shows all Task Sequences that were defined in CM when the last CM sync ran.

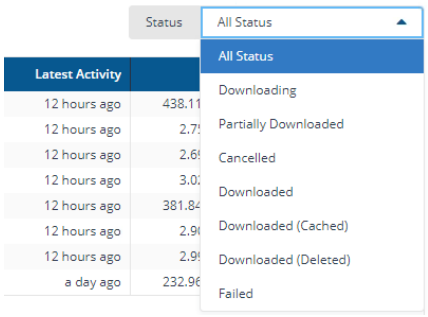
The**Task Sequences**list has the following columns:

Column	Description
Task Sequence	The name of the Task Sequence.
Latest Activity	How long ago the most recent download activity occurred for any reference content in the Task Sequence.
Size	The total size of all reference content in the Task Sequence.
Download Status	A bar representing the overall status of the Task Sequence content across devices. The status of the overall Task Sequence (all referenced content) on a device will be reported as follows, in order of priority.

Status	Description
Downloading	Represents devices that are currently downloading one referenced content.
Partially Downloaded	Represents devices that have completed download one or more referenced content.
Cancelled	Represents devices that cancelled the download of any of the referenced content. When viewing a Task Sequence as a whole, **Cancelled** status is prioritised over **Partially Downloaded**. For example if a device has successfully downloaded some content but one or more reference contents were cancelled, the overall status of the Task Sequence will be **Cancelled**.
Downloaded	Represents devices that have completed download of all referenced content.
Downloaded (Cached)	Represents devices that have completed download of all referenced content.
Downloaded (Deleted)	Represents devices that had previously downloaded all referenced content, which has subsequently all been deleted from the cache.
Failed	Represents devices that failed to download any of the referenced content. When viewing a Task

Column	Description
	Sequence as a whole, **Failed** status is prioritised over **Cancelled** and **Partially Downloaded**. For example, if a device has successfully downloaded some content, cancelled other content and failed to download one content, the overall status for the Task Sequence will be Failed.





9.6.2.3.1 Navigation and filtering

You can use the **Search Task Sequence...** box to filter the list to show Task Sequences based on your chosen criteria. Clicking on a Task Sequence name takes you to the Task Sequence**Details**page.

9.6.2.3.1.1 Time period filter

You can use the **Time period** filter to filter out older activity. For example, selecting Last 30 days will only show Task Sequences for which there has been download activity for any of its reference content in the last 30 days.

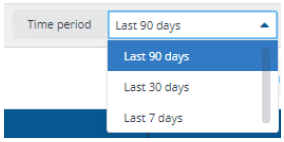
Using the **Time period**filter at the top of the page, you can narrow down the results by date. You can choose from the following options:

Last 90 days

Last 30 days (Default)

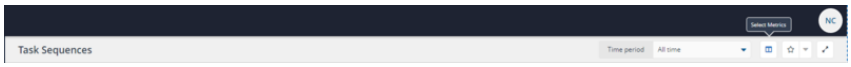
Last 7 days.

> **Note**
>
> If these filters are applied to any app page, it is reflected on all other pages in the Nomad App.



9.6.2.3.1.2 Select Columns

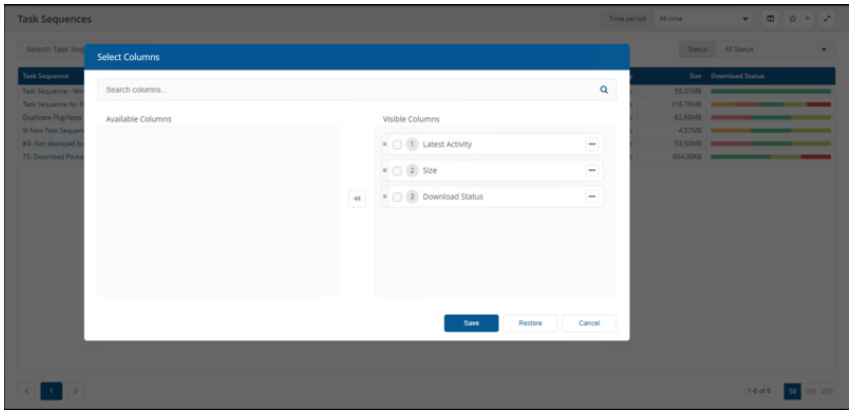
You can select the columns you want displayed by clicking on the **Select Columns** option. From the **Available Columns** and **Visible Columns**, you can add, remove or re-order the columns.



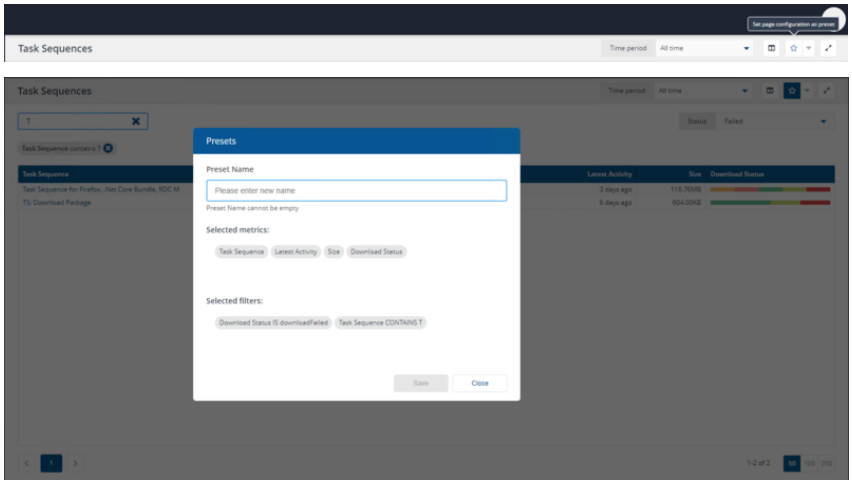
When you click on the **Select columns** control it opens a popup displaying every column on the current screen, the controls are:

Control	Explanation
Available Columns	Columns which are by default hidden from display on screen. You can still include any of them to display on screen.
Visible Columns	Displays the list of columns displayed on screen.
Arrow buttons	To move up or move down, exclude or include any column, clicking on the ellipsis displays these additional controls. <image detail goes here>
Drag and drop	You can drag and drop columns to change how they are displayed.
Exclude columns	Exclude column button allows you to select columns to exclude from the current display.

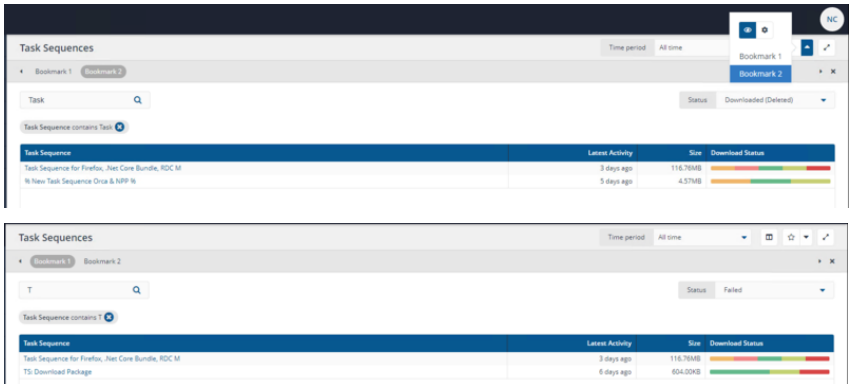
Clicking **Save** on the **Select Columns** screen saves the layout for the current browser session.



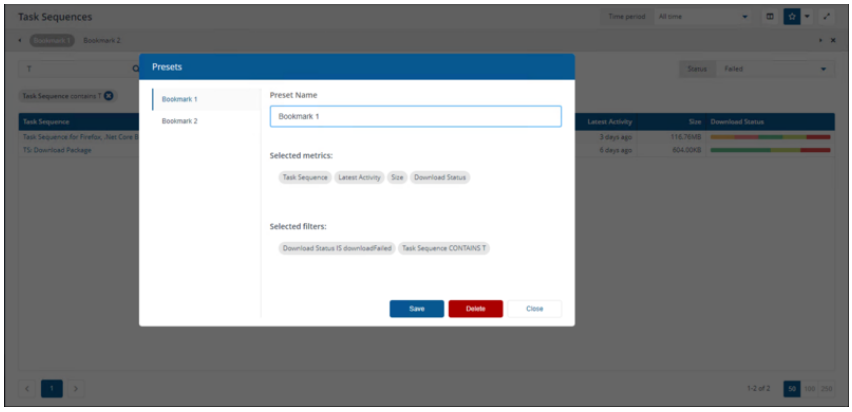
After selecting the columns and other configurations done on the page, you can set it as a preset to be selected further.



You can apply any preset later either from the list of configured presets or from the bookmark bar of the configured presets.



You can also manage (rename or delete) your saved **Presets**.



9.6.2.3.2 Task Sequence details page

The Task Sequence detail page is displayed when you click on a task sequence title on the **Task Sequence** page. It includes a **Summary** tab and a **Devices** tab.

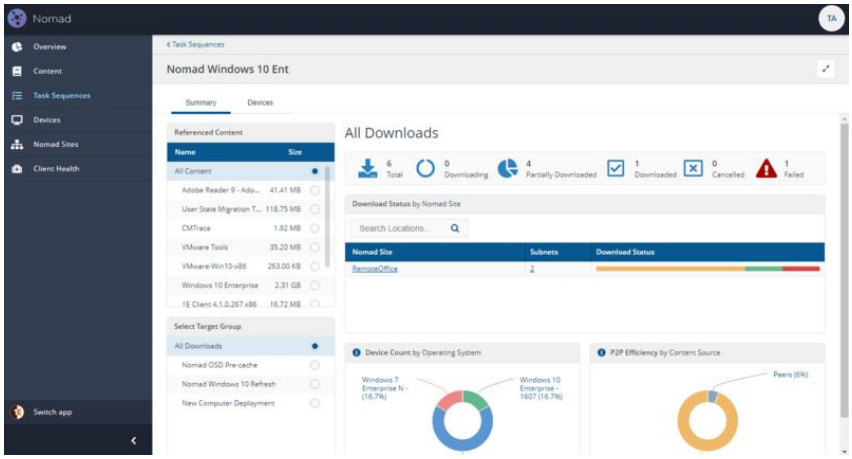
9.6.2.3.2.1 Summary tab

The Summary tab shows summary information about the selected task sequence.

9.6.2.3.2.1.1 Top status Bar

The top status bar displays the following statistics of the selected Task Sequence:

Status	Description
Total	Displays the number of downloads for the latest version of the selected **Content Title**. If the **Content Title** is a CM Application, this number represents the total number of downloads of all of that Application's Deployment Types.
Downloading	Displays the number of devices that are currently downloading the latest version of the **Content Title**.
Partially Downloaded	Displays the number of downloads of the latest version of the **Content Title** that have partially completed.
Downloaded	Displays the number of downloads of the latest version of the **Content Title** that have completed successfully.
Cancelled	
Failed	Displays the number of downloads of the latest version of the **Content Title** whose latest state was **Failed**.



9.6.2.3.2.1.2 Side Panels

On the left side of the page, there are two panels:

Referenced Contents

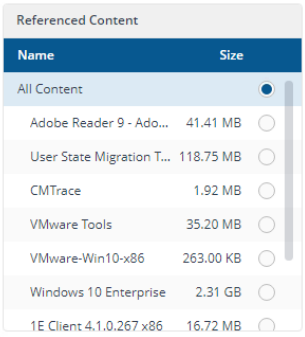
Select Target Group.

9.6.2.3.2.1.2.1 Referenced Contents

Displays the Application or Package **Name** and the **Size** of the content for:

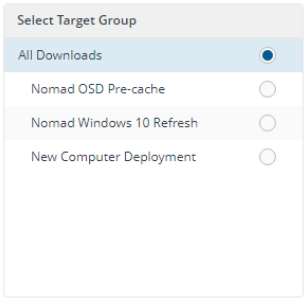
CM Packages, the size represents the total size of the Package content

CM Applications, the **Size** represents the total size of all Deployment Types.



9.6.2.3.2.1.2.2 Select Target Group

Allows the details on the main page to be filtered based on the target group. By default, the main details page shows data for **All Downloads** of the Content Title.



9.6.2.3.2.1.3 Download Status by Nomad Site

Using the **Download Status by Nomad Site** tile you can see in which locations (Nomad Single Site Download (SSD) sites) the content title has been downloaded and is available.

The table shows the status of the selected **Content Title** in each Nomad Site. A Nomad Site corresponds to Nomad Single Site Download site. Customers that have implemented SSD and upgraded ActiveEfficiency to Content Distribution will see their defined SSD locations displayed as Nomad Sites on this tile. Any subnets that are not included in a Nomad SSD Site definition will be represented in a site named **Unknown**. If no SSD sites have been defined, all subnets will be included in the **Unknown** site.

The table displays the following columns:

Column	Description
Nomad Site	The Nomad (SSD) site name.
Subnets	The count of subnets included in the Nomad site. Clicking on the number opens a 'drawer' that shows the download status for each subnet in the site. You can click on the subnet in this drawer to view the devices in that subnet that have reported download activity for the Content Title.
Download Status	A bar representing the current status of the content across all devices in the Nomad Site. This can include the following statuses: Downloading Downloaded (Cached) Downloaded (Deleted) Cancelled Failed Unknown.

Note

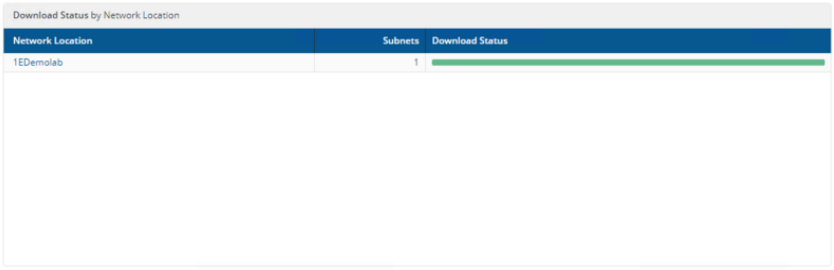
Column	Description
	The **Unknown** status is only displayed if a Target Group has been selected. It indicates the members of the Target Group for which no status for the selected Content Title has been reported.

Hovering over the **Download Status** bar displays the count of downloads in each state. The bar is for information only and is not clickable (i.e. it will not navigate to a filtered list of devices in the various states).

Clicking on a **Nomad Site** navigates to the **Devices** tab, filtered to display devices in the selected **Nomad Site**.

Note

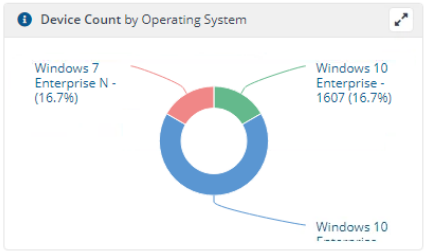
You can use the **Search Locations...** box to search for a specific Nomad Sites.



9.6.2.3.2.1.4 Device Count by Operating system

The **Device Count by Operating System** represents the devices that have downloaded the selected Content Title grouped by Operating System and version and displayed as a donut chart. Delivery Optimization is a Windows 10 feature, but the feature continues to develop with new features and configuration options available in different versions. This data point can help to identify differences across Windows 10 versions.

Clicking on any segment of the chart navigates to the **Devices** tab, filtered to show the devices running the selected OS version.

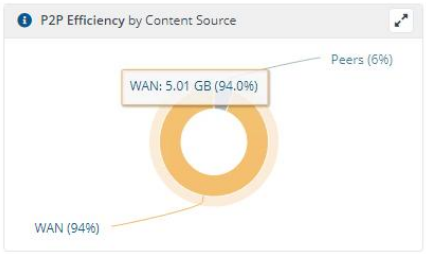


9.6.2.3.2.1.5 P2P Efficiency by Content Source

The **P2P Efficiency by Content Source** tile represents the overall peer-to-peer efficiency across the entire network for the selected Content Title. The data is grouped by source (**Peers** and **WAN**) and displayed as a donut chart showing the volume of content downloaded from peers (in grey) and from the source over the WAN (in orange).

Ideally, more content will be downloaded from peers than from the source over the WAN, thereby saving network bandwidth. Where this is not the case, it could be due to many users working remotely without any local peers, or it could be due to configuration settings on the client that are not optimized for peer-to-peer caching and availability. It may also be worth considering pre-caching the Content Title in more locations to improve the availability of the content on peers in each location.

Clicking either segment in this chart will navigate to the **Devices** tab filtered to show the devices that downloaded the selected Content Title from **Peers** or **WAN**, according to the segment that you clicked on.



9.6.2.3.2.2 Devices tab

The **Devices** tab in the Task Sequence detail page lists the devices that have reported download activity or cache status for content referenced in the selected Task Sequence.

This tab is displayed when you click a **Nomad Site** or a segment on the **Device Count by Operating system** or **P2P Efficiency by Content Source** charts on the Task Sequence summary tab, filtered according to the item clicked.

Alternatively, you can select the tab to view all devices that have reported download activity for content referenced in the Task Sequence.

Alternatively you can select the tab to view all devices that have reported download activity for the content title. Use the**Search Devices...**box to search for a specific device.

> **Note**
>
> The list can be further organized using the filters:

Source - (Peers or WAN)

Status:

Downloading

Downloaded (Cached)

Downloaded (Deleted)

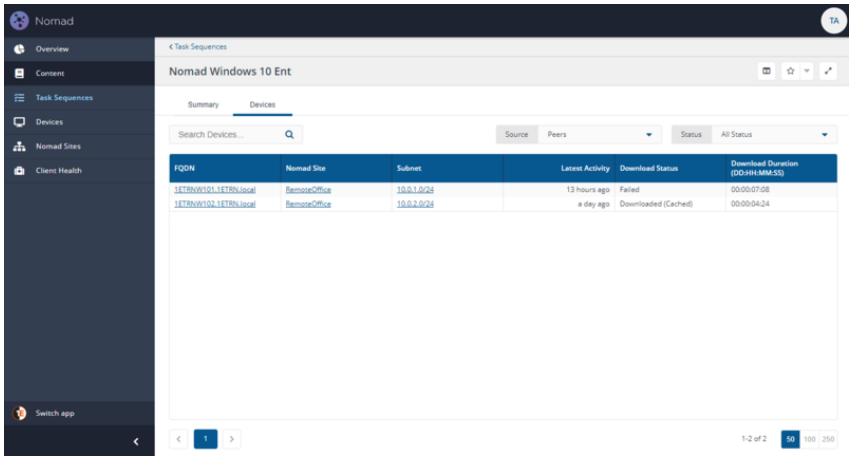
Cancelled

Failed

Unknown.

The table of Devices displays the following columns and from this list, you can click on an FQDN to view details of the specific device on the Devices page.

Column	Description
FQDN	Fully Qualified Domain Name.
Nomad Site	The Nomad SSD Site that the device is currently in, based on the device's latest device registration.
Subnet	The subnet the device is currently in, based on the device's latest device registration.
Latest Activity	Indication of how long ago the latest download activity for the selected Content Title occurred on this device.
Download Status	Status of the selected Content Title on this device, one of: Downloading Downloaded (Cached) Downloaded (Deleted) Cancelled Failed.
Download Duration (DD:HH:MM:SS)	The amount of time it took to download the content.



9.6.2.4 Devices page

The **Devices** page lists all Devices that have sent Nomad device registration events and have sent download events within the selected **Time period**.

9.6.2.4.1 Navigation and filtering

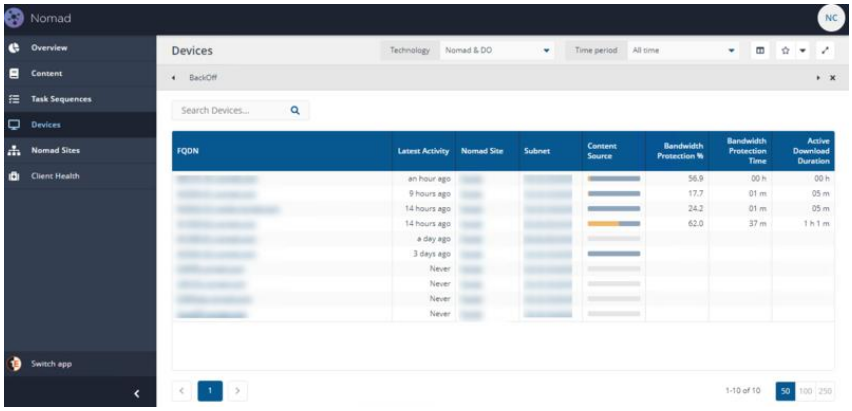
Devices are listed in order of **Latest Activity**, devices with the most recent activity are at the top of the list. The **Time period** filter is 'inherited' if it has been previously set on another page in the same browser session. If the **Time period** is set to **All time**, devices that have registered (i.e. they are running Nomad) but have not sent any download activity will appear at the bottom of the list and **Latest Activity** will show **Never** in the **Latest Activity** column.

In addition to the **Time period** filter, you can use the **Technology** filter to show devices that have download activity from Nomad, Delivery Optimization (DO) or both (default).

The **Devices** list has the following columns:

Column	Description
FQDN	Fully Qualified Domain Name.
Latest Activity	Indication of how long ago the latest download activity occurred on this device.
Nomad Site	The Nomad SSD Site that the device is currently in based on the last adapter registration event.
Subnet	The subnet that the device is currently in based on the last adapter registration event.
Content Source	A bar representing the volume of content this device has downloaded from a peer (in grey) vs from a source over the WAN (in orange).
Bandwidth Protection %	Bandwidth Protection shown as a percentage of downloads This is the result of the **Bandwidth Protection Time** column dived by the **Active Download Duration** and multiplied by 100.
Bandwidth Protection Time	Duration the client backed off from downloading to save download bandwidth. **Note** This metric is not visible by default, you can select it using **Select Columns**
Active Download Duration	Duration for which client actively downloaded the content, this excludes interruptions while downloading, for example because of network issues.

Column	Description
	Note This metric is not visible by default, you can select it using **Select Columns**.

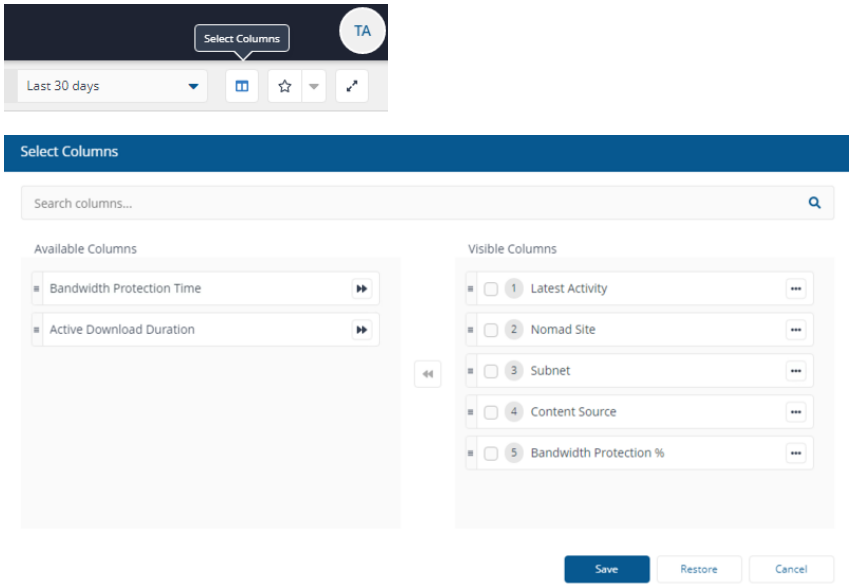


9.6.2.4.1.1 Select Columns

On the pages where you can pick the displayed columns, you'll see the following **Select Columns** control.

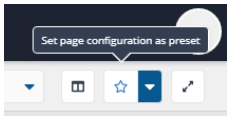
When you click on the **Select columns**control it opens a popup displaying the columns shown on the current screen and any additional columns you can select, the controls are:

Control	Explanation
Available Columns	Columns, which are by default hidden from display on screen. You can still include any of them to display on screen.
Visible Columns	Displays the list of columns displayed on screen. Mandatory Columns cannot be excluded, the selection controls for these items are disabled. They can still be moved up or down.
Arrow buttons	To move up or move down, exclude or include any column, clicking on the ellipsis displays these additional controls.
Drag and drop	You can drag and drop columns to change how they are displayed.
Exclude columns	Exclude column button allows you to select columns to exclude from the current display.

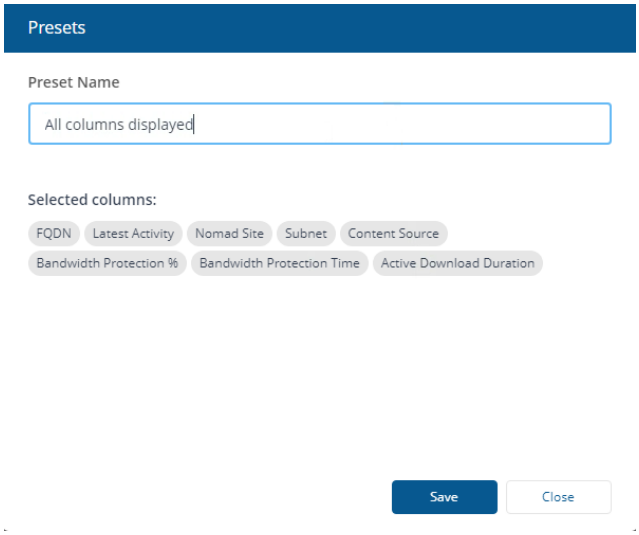


9.6.2.4.1.2 Set page configuration as preset

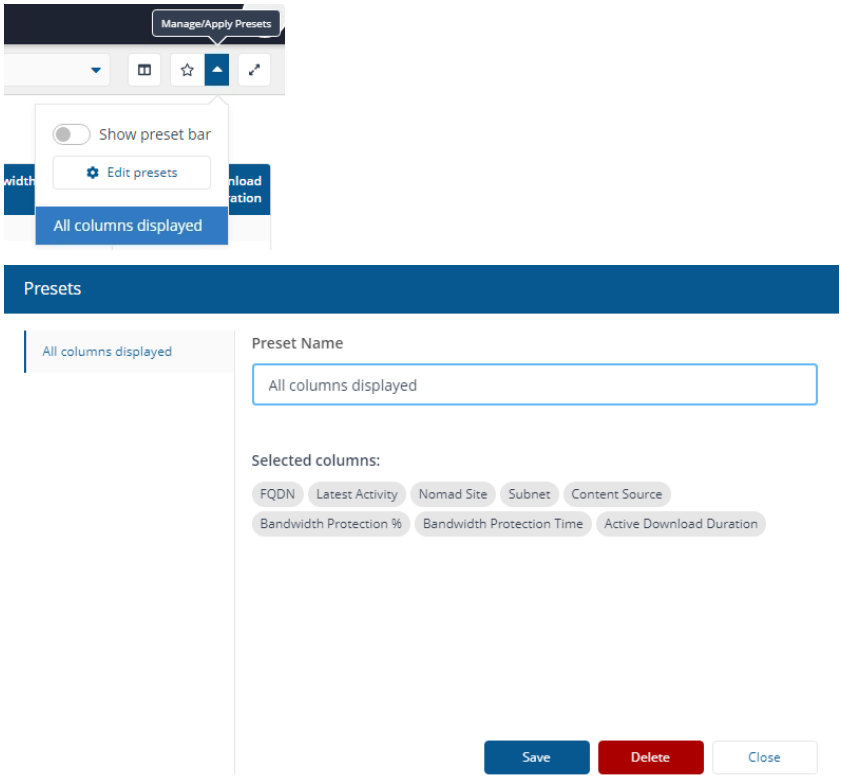
If you have amended the displayed columns using the **Choose columns** control, you can then save the view as a preset which will be available later.



Clicking **Set page configuration as preset** displays the **Presets** popup. Here, you can give the view a name, in the shown example this is called **All columns displayed** as we have chosen to display every available column.



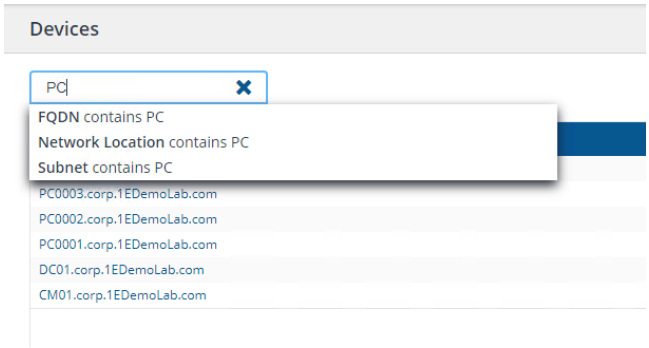
Once saved, you can select your saved views using the **Manage/Apply Presets** control or edit them by clicking **Edit presets**.



9.6.2.4.1.3 Search

You can use the **Search Devices...** box to search for a specific device by **FQDN**, **Network Site** or **Subnet**.

When you start typing into the search box, a list will appear as indicated below, allowing you to select which column (**FQDN**, **Network Site** or **Subnet**) that the search term should be applied to.



9.6.2.4.1.4 Time period filter

Using the **Time period**filter at the top of the page, you can narrow down the results by date. You can choose from the following options:

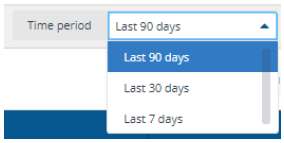
Last 90 days

Last 30 days (Default)

Last 7 days.

Note

If these filters are applied to any app page, it is reflected on all other pages in the Nomad App.



9.6.2.4.1.5 Technology filter

You can use the **Technology** filter to differentiate between downloads through Nomad or Delivery Optimization (DO).

The following options are available:

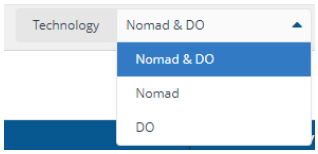
Nomad & DO (Default)

Nomad

DO.

Note

If this filter is applied to any app page, it is reflected on all other pages in the Nomad App.



9.6.2.4.2 The Device view Downloads tab

The **Device view** is a common view used throughout Tachyon to present details of a device from multiple Tachyon Platform applications.

The default view in the Nomad devices view is **Downloads**. The remaining tabs display information corresponding to an app, feature or data set implemented in Tachyon, other tabs are visible if an app has been installed and licensed, and the user has permissions to use the app, refer to Additional Device View Tabs for detail. Clicking on one of the links in the **FQDN** column of the **Devices** page displays the Device view for the selected device. The aim of the Device view is to provide a combined overview of all the information known about a device, along with the ability to retrieve information about the device in real-time. When displaying the Device view from a Nomad page, the view defaults to the **Downloads** tab. The **Downloads** tab contains information derived from and useful for using Nomad.

In addition, the Summary banner displays a quick summary of the information provided in the various tabs displayed in the Device View. It can be viewed by toggling the **Summary banner** switch to on, refer to Summary banner for details.

Note

The **Time period** filter does not apply to detail pages. As a result, if you have set the**Time period**filter on the**Devices** page to, for example,**Last 7 days**, you may see different results on the detail page for a device.

Note

The details shown on the Downloads and other tabs rely on access to the associated app, but also Instruction Sets used by the Tachyon Platform. >To view details in the Downloads tab for the Nomad app you'll need to load the 1E Nomad product pack. For more details, refer to Installing the Nomad app - 1E Nomad product pack.

9.6.2.4.2.1 Downloads tab

The**Downloads**tab has three items:

Summary

Content

Nomad Configuration.

The Downloads tab presents download activity and status for the device. Whenever you click on an FQDN on any of the Nomad dashboard pages, the Device details page will be displayed with the **Downloads** tab selected.

9.6.2.4.2.1.1 Summary

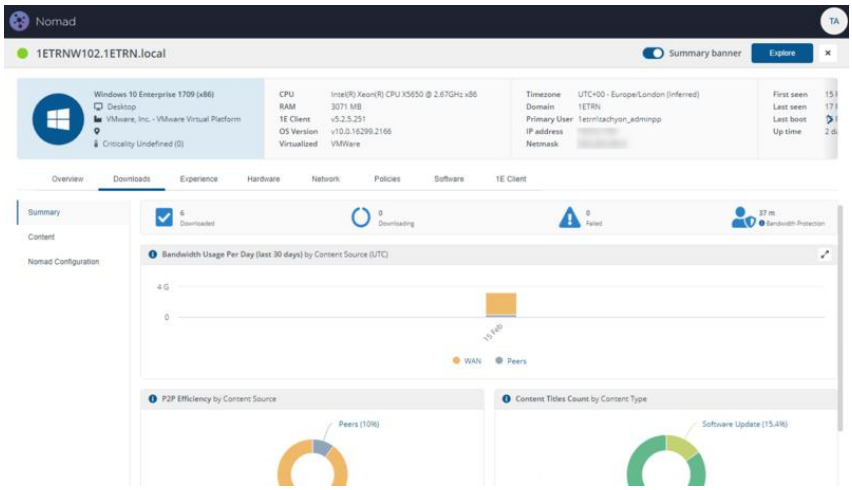
Summary has four panels:

Status bar

Bandwidth Usage Per Day by Content Source (UTC)

P2P Efficiency by Content Source

Content Titles Count by Content Type.

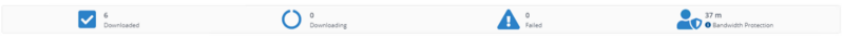


9.6.2.4.2.1.1.1 Status bar

The status bar along the top shows high-level download statistics for this device:

Column	Description
Downloaded	Number of completed downloads on this device.
Downloading	Number of downloads that are actively in progress on this device.
Failed	Number of downloads on devices that are currently in the site, whose latest status is failed.
Bandwidth Protection	Bandwidth Protection allows Nomad to adjust the speed of ongoing downloads to save bandwidth for other business use. Bandwidth Protection ensures Nomad doesn't consume excess bandwidth and hinder other business activity.

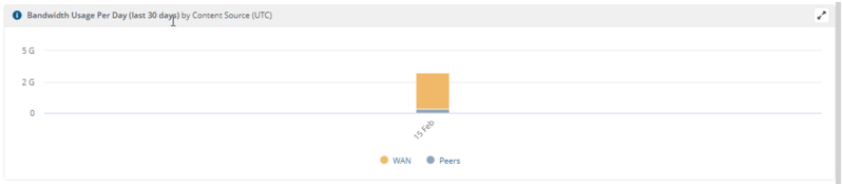
Clicking on any of these icons will navigate to the**Content**view of the**Device detail**tab, filtered according to the clicked icon.



9.6.2.4.2.1.1.2 Bandwidth Usage Per Day by Content Source (UTC)

The **Bandwidth Usage Per Day by Content Source (UTC)** tile represents daily download activity on this device for the last 30 days. A column is displayed for each day when there was download activity. Each column indicates the volume of content that was downloaded over the WAN (in orange) or from peers (in grey).

Hovering over a segment of the column displays the volume of content downloaded on that day, demonstrating the value that Nomad and Delivery Optimization are providing through reduced WAN traffic. If the majority of content is being downloaded over the WAN, it could indicate that peers are simply not available (e.g. this device is being used from home) or it could be an indication that Nomad or Delivery Optimization are not correctly configured to optimize content from peers.

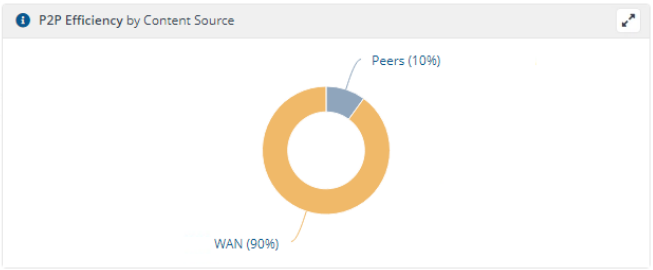


9.6.2.4.2.1.1.3 P2P Efficiency by Content Source

The **P2P Efficiency by Content Source** tile represents the overall peer-to-peer efficiency on this device. The data is grouped by source (**Peers** and **WAN**) and displayed as a donut chart showing the volume of content downloaded from peers (in grey) and from the source over the WAN (in orange).

The chart gives an indication of the overall value of Nomad and Delivery Optimization on this device. Ideally, more content will be downloaded from peers than from the source over the WAN, thereby saving network bandwidth. Where this is not the case, it could be due to remote working (where there are no peers available), or it could be due to configuration settings on the client that are not optimized for peer-to-peer caching and availability.

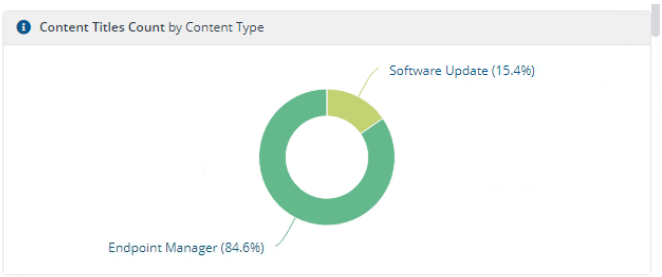
Clicking on a segment in this chart will navigate to the **Content** view for this device, filtered to show content that was downloaded from the selected source (Peer or WAN).



9.6.2.4.2.1.1.4 Content Titles Count by Content Type

The **Content Titles Count by Content Type** chart gives an indication of the number of **Endpoint Manager** applications and **Software Update** this device has downloaded.

Clicking on a segment in this chart will navigate to the **Content** view for this device, filtered by the selected Content Type.



9.6.2.4.2.1.2 Content

The **Content** panel shows the status of content downloaded on the device:

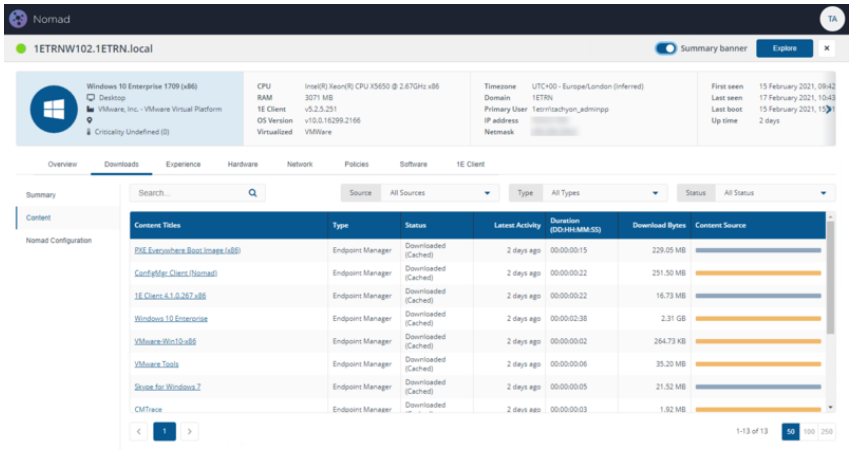
Column	Description
Content Titles	Content title, for: CM Packages, this is the Package name CM Applications, this is a combination of the Application name and Deployment Type name Software Updates, this is the title of the Software Update as defined in the Microsoft Update catalog (this is collected from the client, not the Microsoft Catalog).

Column	Description
Type	Currently, either Endpoint Manager or Software Update.
Status	Current status of the content on this device. This can include the following statuses. **Downloading** **Downloaded (Cached)** - downloaded and has not subsequently reported deletion **Downloaded (Deleted)** - downloaded but has subsequently been deleted from the cache **Cancelled** **Failed.**
Latest Activity	Date and time of the latest event for the content title on this device.
Duration	The time taken to download the content.
Download Bytes	Amount of bytes of the content actually downloaded by the device. In some cases, especially with Software Updates, only deltas or byte ranges will be downloaded rather than the entire source content.
Content Source	A bar indicating the proportion of the content that was downloaded over the WAN or from peers.

Note

The **Time period** filter does not apply to detail pages.

As a result, if you have set the **Time period** filter on the **Devices** page to, for example, **Last 7 days**, you may see different results on the detail page for a device.



9.6.2.4.2.1.3 Navigation and filtering

There are four ways you can filter viewable content:

Search...

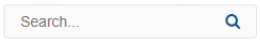
Sources

Types

Status.

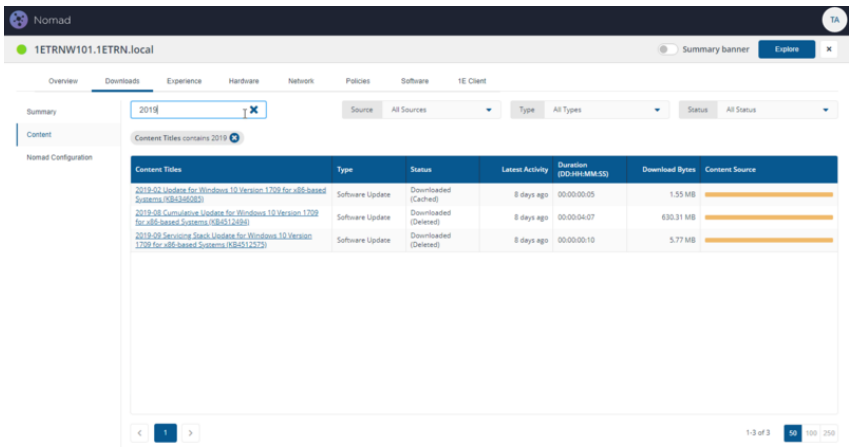
9.6.2.4.2.1.3.1 Search...

Use the search box at the top left of the page to filter by specific criteria, for example in the picture opposite the default view has been filtered by Content Titles containing 2019 in their title.



Note

Navigating away from this view resets the table to its default view.



9.6.2.4.2.1.3.2 Filters

Filter the table using these options:

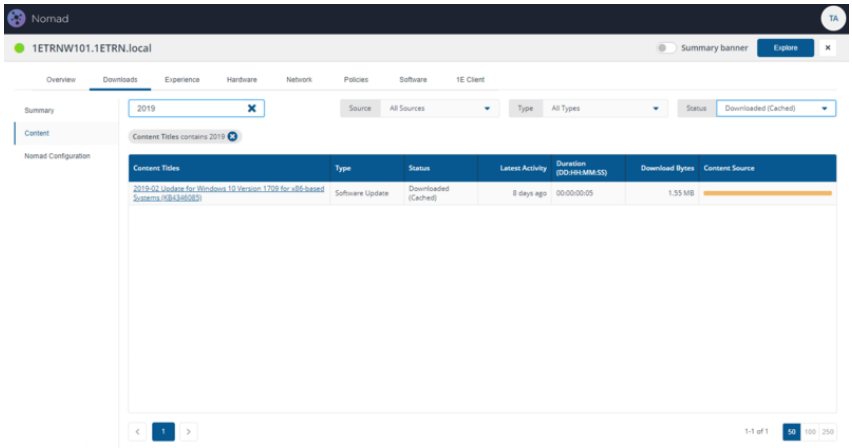
Source

Type

Status.

Filter	Options	Description
Source	**All Sources** (default)	Shows content that was downloaded from either the WAN or peers.
WAN	Shows content that was partially or fully downloaded over the WAN.	
Peers	Shows content that was partially or fully downloaded from peers.	
Type	**All Types** (default)	Shows Endpoint Manager and Software Update content.
Software Update	Shows only Software Update content.	
Endpoint Manager	Shows only Endpoint Manager content.	
Status	**All Status** (default)	Shows all content for which any download activity has been reported.
Downloading	Shows all content for which the latest reported status was downloading.	
Cancelled	Shows all content for which the latest reported status was cancelled.	
Downloaded (Cached)	Shows all content for which the latest reported status was Downloaded and has not subsequently reported deletion.	

Filter	Options	Description
Downloaded (Deleted)	Shows all content which completed downloading but has subsequently been deleted from the cache.	
Failed	Shows all content for which the latest reported status was Failed.	
Downloaded	Shows all content that has been downloaded (either still cached or deleted).	



9.6.2.4.2.1.4 Nomad Configuration

Shows the **1E Nomad Branch Settings** for the selected device. You can use this to check a device's Nomad registry entries if the device is not behaving as expected.

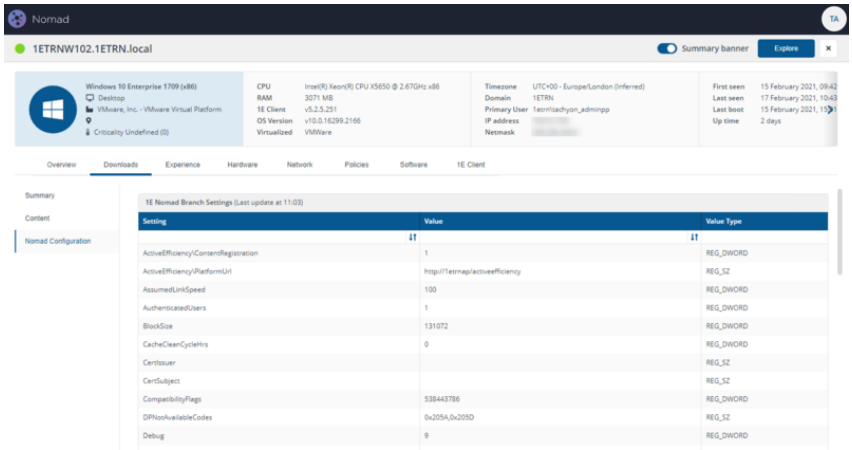
The registry details presented are gathered by the **1E-Nomad-NomadBranchSettings** instruction of the 1E Nomad product pack.

Classic product pack used to create the **1E Nomad** instruction set in Tachyon, required by the following Nomad features:

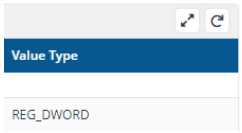
Downloads tab on Device views - instructions used to populate details about Content download and other Nomad features

Nomad Download Pause - instructions used by the CM Admin Console extensions

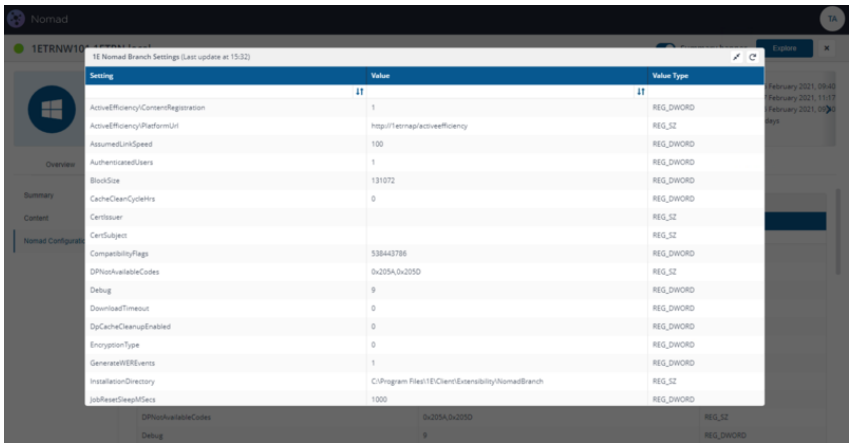
Instructions to help with the following Nomad features: Nomad cache, CacheCleaner, Single Site Download, Nomad jobs, NomadBranch service.



The **1E Nomad Branch Settings** panel is expandable. Moving your mouse over the panel reveals an **Expand** button on the top left of the panel and a refresh button. Clicking the refresh button, re-runs the **1E-Nomad-NomadBranchSettings** instruction.



A full list of Nomad registry values by feature are available on the Nomad registry values page. Registry values for NomadBranch are located in: *HKLM\Software\1E\NomadBranch*



9.6.2.4.3 Summary banner

The Summary banner displays a quick summary of the information provided in the various tabs displayed in the Device View. It can be viewed by toggling the **Summary banner** switch to on.

The following picture shows the Summary banner displayed for a particular device.

The following table describes the information provided in the Summary banner.

<table>
<tr><th>Panel</th><th>Description</th><th>Data source</th></tr>
<tr><td></td><td>Shows details equivalent to the following tiles:
<table>
<tr><th>Tab</th><th>Panel</th><th>Column</th><th>Tile</th><th>Description</th><th>Example</th></tr>
<tr><td>Overview</td><td>Details</td><td>Hardware and Operating System</td><td>Operating System</td><td>Version</td><td>Windows 10 Pro 20H2 (x86)</td></tr>
<tr><td>Hardware and Operating System</td><td>Hardware</td><td>Device Type</td><td>Desktop</td><td></td><td></td></tr>
<tr><td>Hardware and Operating System</td><td>Hardware</td><td>Manufacturer</td><td>VMware, Inc</td><td></td><td></td></tr>
<tr><td>Hardware and Operating System</td><td>Hardware</td><td>Model</td><td>VMWare Virtual Platform</td><td></td><td></td></tr>
<tr><td>Identification</td><td>Location</td><td>Location</td><td></td><td></td><td></td></tr>
<tr><td>Identification</td><td>Identification</td><td>Criticality</td><td>Undefined (0)</td><td></td><td></td></tr>
</table>
Shows details equivalent to the following tiles:
<table>
<tr><th>Tab</th><th>Panel</th><th>Column</th><th>Tile</th><th>Description</th><th>Example</th></tr>
<tr><td>Overview</td><td>Details</td><td>Hardware and</td><td>Hardware</td><td>CPU Type</td><td>Intel(R) Xeon(R) CPU X5650</td></tr>
</table></td><td>Data from Tachyon Master (the latest online status message)</td></tr>
</table>

Panel	Description				Data source
		Operating System		@2.67GHz x86	
Hardware and Operating System	Hardware	RAM	3071 MB		
Identification	Identification	1E Client	v5.2.5.251		
Hardware and Operating System	Operating System	Version	v10.0.19042.746		
Hardware and Operating System	Operating System	Virtual/Physical	VMWare		

Shows details equivalent to the following tiles:

Tab	Panel	Column	Tile	Description	Example
Overview	Details	Identification	Location	Timezone	UTC+00 - Europe/London (Inferred)
Identification	Identification	Domain	1ETRN		
Connectivity and Activity	Activity	User	1ETRN\Administrator		

Panel	Description					Data source
	Connectivity and Activity	Connectivity	Local IP Address	10.0.1.3/24		
					Netmask	255.255.255.0

Shows details equivalent to the following tiles:

Tab	Panel	Column	Tile	Description	Example
Overview	Details	Connectivity and Activity	Connectivity	First Connected	22 March 2021, 12:17 UTC
Connectivity and Activity	Connectivity	Last Connected	27 April 2021, 09:23 UTC		
Connectivity and Activity	Activity	Last Boot	18 March 2021, 12:24 UTC		
				Up time	a month

Shows details equivalent to the following tiles:

Tab	Panel	Column	Tile	Description	Example
Overview	Details	Identification	Grouping	Mgmt. Groups	All Devices All Win10 Workstations Servers.

9.6.2.4.4 Additional Device View tabs

In addition to the **Downloads** tab, there are a series of tabs, each corresponding to an app, feature or data set implemented in Tachyon.

The **Overview** and **1E Client** tabs are always present in the **Device View**. Other tabs are visible if an app has been installed and is licensed.

Each tab has one or more panels with tiles populated with data from various sources, some by instructions that are run instantly, with results cached for 3 minutes. An appropriate error message is displayed instead of a tile in the following circumstances:

If the device is offline, as indicated by the color of the icon in the top left

The user does not have at least Viewer permission to view use the license the tab or panel

The user does not have questioner permission to run the instruction

An instruction has not been uploaded.

The The Device View tabs and panels page lists the names of tabs and their panels, and a description of each tile indicating how the tile is populated.

9.6.2.4.5 Navigation and filtering

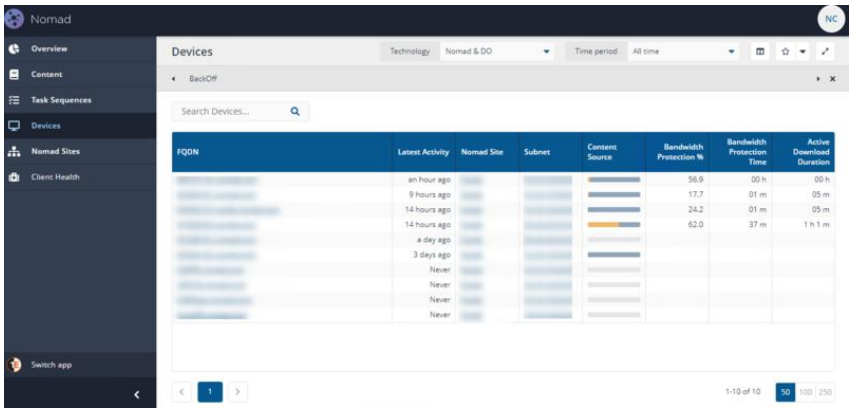
Devices are listed in order of **Latest Activity**, devices with the most recent activity are at the top of the list. The **Time period** filter is 'inherited' if it has been previously set on another page in the same browser session. If the **Time period** is set to **All time**, devices that have registered (i.e. they are running Nomad) but have not sent any download activity will appear at the bottom of the list and **Latest Activity** will show **Never** in the **Latest Activity** column.

In addition to the **Time period** filter, you can use the **Technology** filter to show devices that have download activity from Nomad, Delivery Optimization (DO) or both (default).

The**Devices**list has the following columns:

Column	Description
FQDN	Fully Qualified Domain Name.
Latest Activity	Indication of how long ago the latest download activity occurred on this device.
Nomad Site	The Nomad SSD Site that the device is currently in based on the last adapter registration event.
Subnet	The subnet that the device is currently in based on the last adapter registration event.

Column	Description
Content Source	A bar representing the volume of content this device has downloaded from a peer (in grey) vs from a source over the WAN (in orange).
Bandwidth Protection %	Bandwidth Protection shown as a percentage of downloads This is the result of the **Bandwidth Protection Time** column dived by the **Active Download Duration** and multiplied by 100.
Bandwidth Protection Time	Duration the client backed off from downloading to save download bandwidth. **Note** This metric is not visible by default, you can select it using**Select Columns**
Active Download Duration	Duration for which client actively downloaded the content, this excludes interruptions while downloading, for example because of network issues. **Note** This metric is not visible by default, you can select it using **Select Columns**.

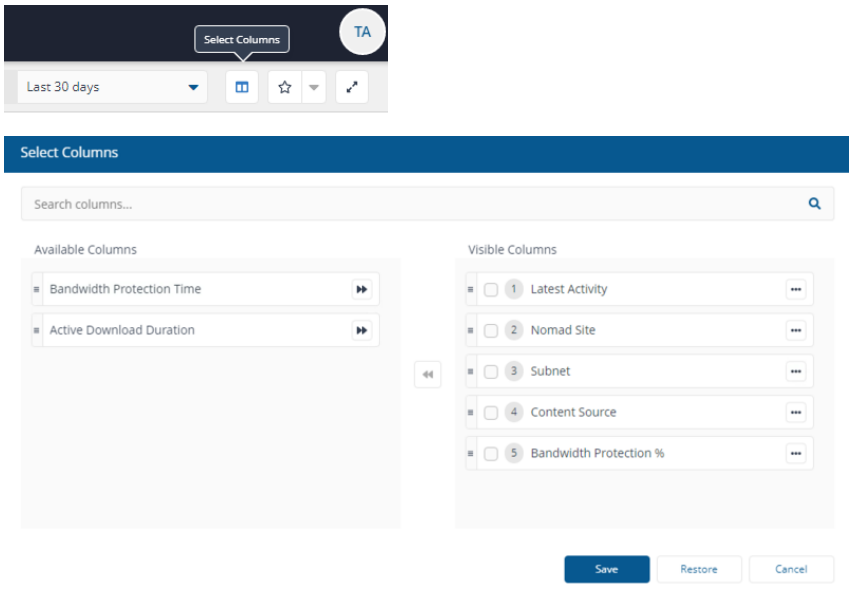


9.6.2.4.5.1 Select Columns

On the pages where you can pick the displayed columns, you'll see the following **Select Columns** control.

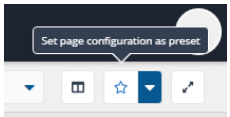
When you click on the **Select columns**control it opens a popup displaying the columns shown on the current screen and any additional columns you can select, the controls are:

Control	Explanation
Available Columns	Columns, which are by default hidden from display on screen. You can still include any of them to display on screen.
Visible Columns	Displays the list of columns displayed on screen. Mandatory Columns cannot be excluded, the selection controls for these items are disabled. They can still be moved up or down.
Arrow buttons	To move up or move down, exclude or include any column, clicking on the ellipsis displays these additional controls.
Drag and drop	You can drag and drop columns to change how they are displayed.
Exclude columns	Exclude column button allows you to select columns to exclude from the current display.

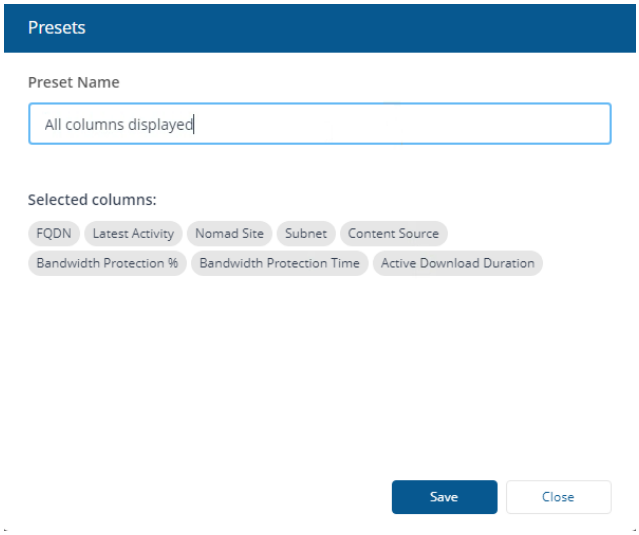


9.6.2.4.5.2 Set page configuration as preset

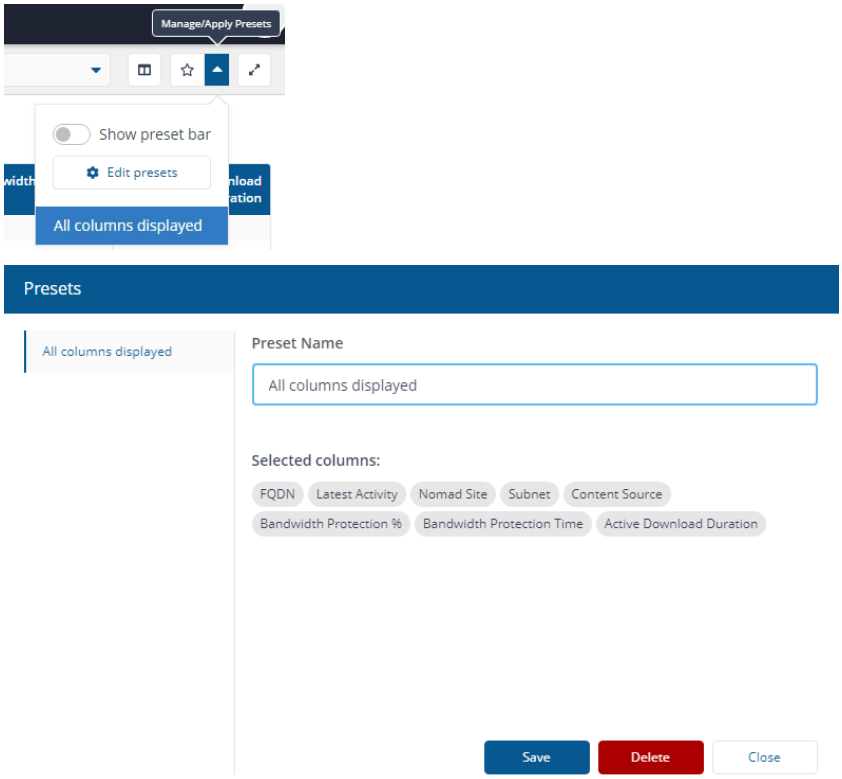
If you have amended the displayed columns using the **Choose columns** control, you can then save the view as a preset which will be available later.



Clicking **Set page configuration as preset** displays the **Presets** popup. Here, you can give the view a name, in the shown example this is called **All columns displayed** as we have chosen to display every available column.



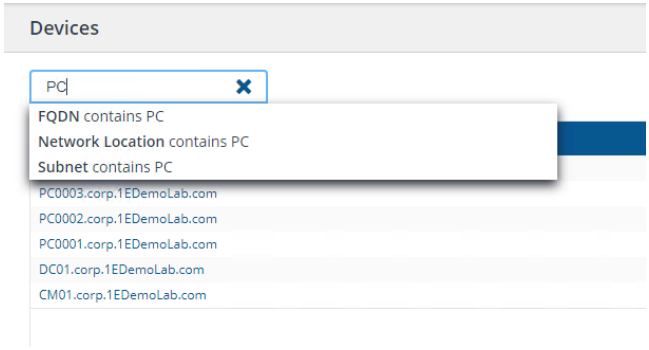
Once saved, you can select your saved views using the **Manage/Apply Presets** control or edit them by clicking **Edit presets**.



9.6.2.4.5.3 Search

You can use the **Search Devices...** box to search for a specific device by **FQDN**, **Network Site** or **Subnet**.

When you start typing into the search box, a list will appear as indicated below, allowing you to select which column (**FQDN**, **Network Site** or **Subnet**) that the search term should be applied to.



9.6.2.4.5.4 Time period filter

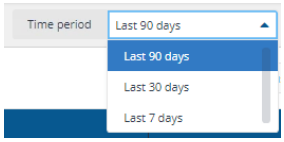
Using the **Time period**filter at the top of the page, you can narrow down the results by date. You can choose from the following options:

Last 90 days

Last 30 days (Default)

Last 7 days.

> **Note**
>
> If these filters are applied to any app page, it is reflected on all other pages in the Nomad App.



9.6.2.4.5.5 Technology filter

You can use the **Technology** filter to differentiate between downloads through Nomad or Delivery Optimization (DO).

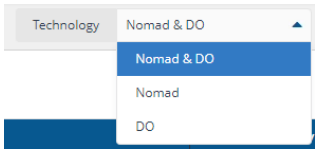
The following options are available:

Nomad & DO (Default)

Nomad

DO.

> **Note**
>
> If this filter is applied to any app page, it is reflected on all other pages in the Nomad App.



9.6.2.4.6 The Device view Downloads tab

The **Device view** is a common view used throughout Tachyon to present details of a device from multiple Tachyon Platform applications.

The default view in the Nomad devices view is **Downloads**. The remaining tabs display information corresponding to an app, feature or data set implemented in Tachyon, other tabs are visible if an app has been installed and licensed, and the user has permissions to use the app, refer to Additional Device View Tabs for detail. Clicking on one of the links in the **FQDN** column of the **Devices** page displays the Device view for the selected device. The aim of the Device view is to provide a combined overview of all the information known about a device, along with the ability to retrieve information about the device in real-time. When displaying the Device view from a Nomad page, the view defaults to the **Downloads** tab. The **Downloads** tab contains information derived from and useful for using Nomad.

In addition, the Summary banner displays a quick summary of the information provided in the various tabs displayed in the Device View. It can be viewed by toggling the **Summary banner** switch to on, refer to Summary banner for details.

> **Note**
>
> The **Time period** filter does not apply to detail pages. As a result, if you have set the**Time period**filter on the**Devices** page to, for example,**Last 7 days**, you may see different results on the detail page for a device.

> **Note**
>
> The details shown on the Downloads and other tabs rely on access to the associated app, but also Instruction Sets used by the Tachyon Platform. >To view details in the Downloads tab for the Nomad app you'll need to load the 1E Nomad product pack. For more details, refer to Installing the Nomad app - 1E Nomad product pack.

9.6.2.4.6.1 Downloads tab

The**Downloads**tab has three items:

Summary

Content

Nomad Configuration.

The Downloads tab presents download activity and status for the device. Whenever you click on an FQDN on any of the Nomad dashboard pages, the Device details page will be displayed with the **Downloads** tab selected.

9.6.2.4.6.1.1 Summary

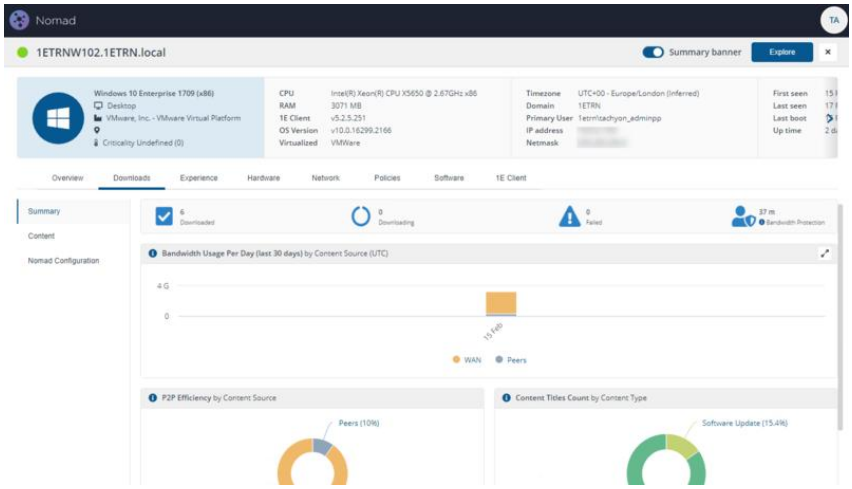
Summary has four panels:

Status bar

Bandwidth Usage Per Day by Content Source (UTC)

P2P Efficiency by Content Source

Content Titles Count by Content Type.



9.6.2.4.6.1.1.1 Status bar

The status bar along the top shows high-level download statistics for this device:

Column	Description
Downloaded	Number of completed downloads on this device.
Downloading	Number of downloads that are actively in progress on this device.
Failed	Number of downloads on devices that are currently in the site, whose latest status is failed.
Bandwidth Protection	Bandwidth Protection allows Nomad to adjust the speed of ongoing downloads to save bandwidth for other business use. Bandwidth Protection ensures Nomad doesn't consume excess bandwidth and hinder other business activity.

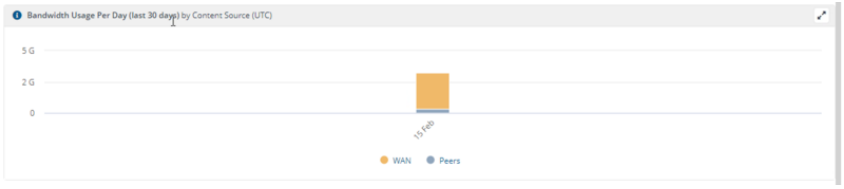
Clicking on any of these icons will navigate to the**Content**view of the**Device detail**tab, filtered according to the clicked icon.

9.6.2.4.6.1.1.2 Bandwidth Usage Per Day by Content Source (UTC)

The **Bandwidth Usage Per Day by Content Source (UTC)** tile represents daily download activity on this device for the last 30 days. A column is displayed for each day when there was download activity. Each column indicates the volume of content that was downloaded over the WAN (in orange) or from peers (in grey).

Hovering over a segment of the column displays the volume of content downloaded on that day, demonstrating the value that Nomad and Delivery Optimization are providing through reduced WAN traffic. If the majority of

content is being downloaded over the WAN, it could indicate that peers are simply not available (e.g. this device is being used from home) or it could be an indication that Nomad or Delivery Optimization are not correctly configured to optimize content from peers.

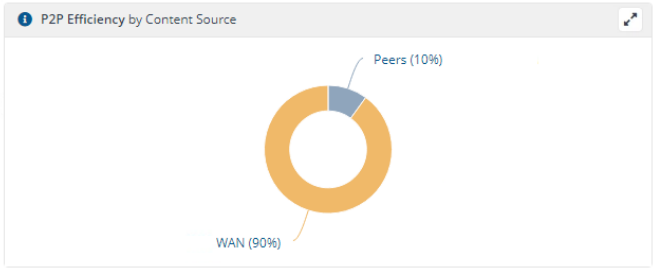


9.6.2.4.6.1.1.3 P2P Efficiency by Content Source

The **P2P Efficiency by Content Source** tile represents the overall peer-to-peer efficiency on this device. The data is grouped by source (**Peers** and **WAN**) and displayed as a donut chart showing the volume of content downloaded from peers (in grey) and from the source over the WAN (in orange).

The chart gives an indication of the overall value of Nomad and Delivery Optimization on this device. Ideally, more content will be downloaded from peers than from the source over the WAN, thereby saving network bandwidth. Where this is not the case, it could be due to remote working (where there are no peers available), or it could be due to configuration settings on the client that are not optimized for peer-to-peer caching and availability.

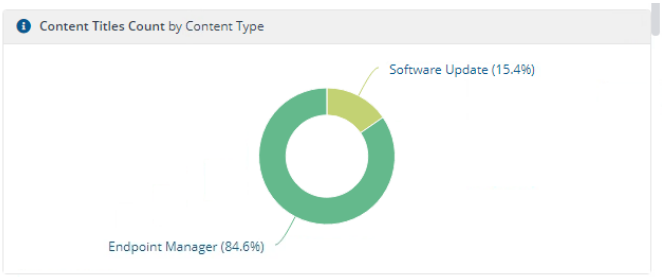
Clicking on a segment in this chart will navigate to the **Content** view for this device, filtered to show content that was downloaded from the selected source (Peer or WAN).



9.6.2.4.6.1.1.4 Content Titles Count by Content Type

The **Content Titles Count by Content Type** chart gives an indication of the number of **Endpoint Manager** applications and **Software Update** this device has downloaded.

Clicking on a segment in this chart will navigate to the **Content** view for this device, filtered by the selected Content Type.



9.6.2.4.6.1.2 Content

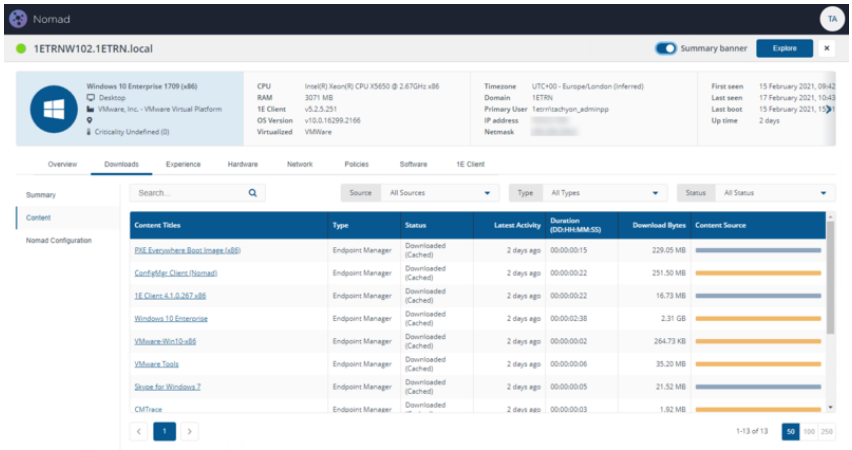
The **Content** panel shows the status of content downloaded on the device:

Column	Description
Content Titles	Content title, for: CM Packages, this is the Package name CM Applications, this is a combination of the Application name and Deployment Type name Software Updates, this is the title of the Software Update as defined in the Microsoft Update catalog (this is collected from the client, not the Microsoft Catalog).
Type	Currently, either Endpoint Manager or Software Update.
Status	Current status of the content on this device. This can include the following statuses. **Downloading** **Downloaded (Cached)** - downloaded and has not subsequently reported deletion **Downloaded (Deleted)** - downloaded but has subsequently been deleted from the cache **Cancelled** **Failed.**
Latest Activity	Date and time of the latest event for the content title on this device.
Duration	The time taken to download the content.
Download Bytes	Amount of bytes of the content actually downloaded by the device. In some cases, especially with Software Updates, only deltas or byte ranges will be downloaded rather than the entire source content.
Content Source	A bar indicating the proportion of the content that was downloaded over the WAN or from peers.

Note

The **Time period** filter does not apply to detail pages.

As a result, if you have set the **Time period** filter on the **Devices** page to, for example, **Last 7 days**, you may see different results on the detail page for a device.



9.6.2.4.6.1.3 Navigation and filtering

There are four ways you can filter viewable content:

Search...

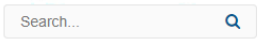
Sources

Types

Status.

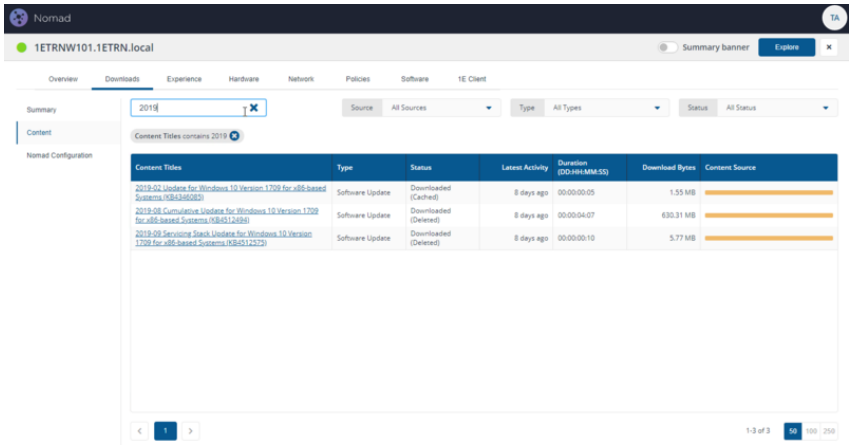
9.6.2.4.6.1.3.1 Search...

Use the search box at the top left of the page to filter by specific criteria, for example in the picture opposite the default view has been filtered by Content Titles containing 2019 in their title.



Note

Navigating away from this view resets the table to its default view.



9.6.2.4.6.1.3.2 Filters

Filter the table using these options:

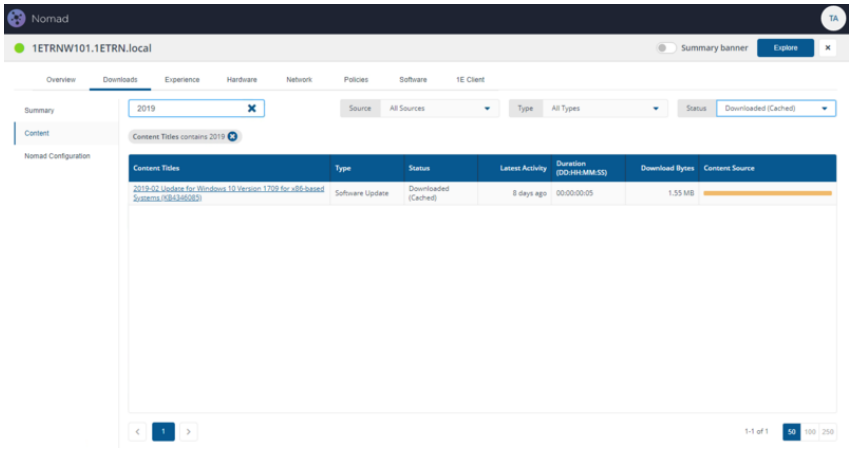
Source

Type

Status.

Filter	Options	Description
Source	**All Sources** (default)	Shows content that was downloaded from either the WAN or peers.
WAN	Shows content that was partially or fully downloaded over the WAN.	
Peers	Shows content that was partially or fully downloaded from peers.	
Type	**All Types** (default)	Shows Endpoint Manager and Software Update content.
Software Update	Shows only Software Update content.	
Endpoint Manager	Shows only Endpoint Manager content.	
Status	**All Status** (default)	Shows all content for which any download

Filter	Options	Description
		activity has been reported.
Downloading	Shows all content for which the latest reported status was downloading.	
Cancelled	Shows all content for which the latest reported status was cancelled.	
Downloaded (Cached)	Shows all content for which the latest reported status was Downloaded and has not subsequently reported deletion.	
Downloaded (Deleted)	Shows all content which completed downloading but has subsequently been deleted from the cache.	
Failed	Shows all content for which the latest reported status was Failed.	
Downloaded	Shows all content that has been downloaded (either still cached or deleted).	



9.6.2.4.6.1.4 Nomad Configuration

Shows the **1E Nomad Branch Settings** for the selected device. You can use this to check a device's Nomad registry entries if the device is not behaving as expected.

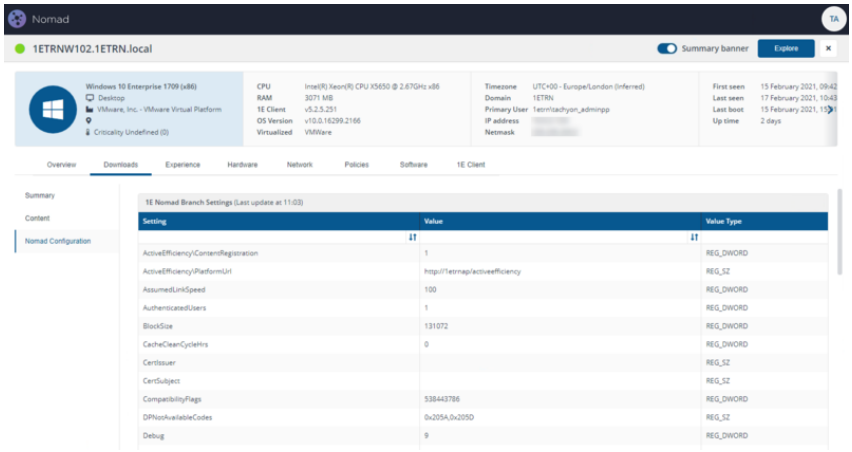
The registry details presented are gathered by the **1E-Nomad-NomadBranchSettings** instruction of the 1E Nomad product pack.

Classic product pack used to create the **1E Nomad** instruction set in Tachyon, required by the following Nomad features:

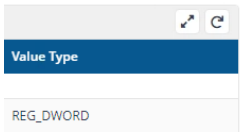
Downloads tab on Device views - instructions used to populate details about Content download and other Nomad features

Nomad Download Pause - instructions used by the CM Admin Console extensions

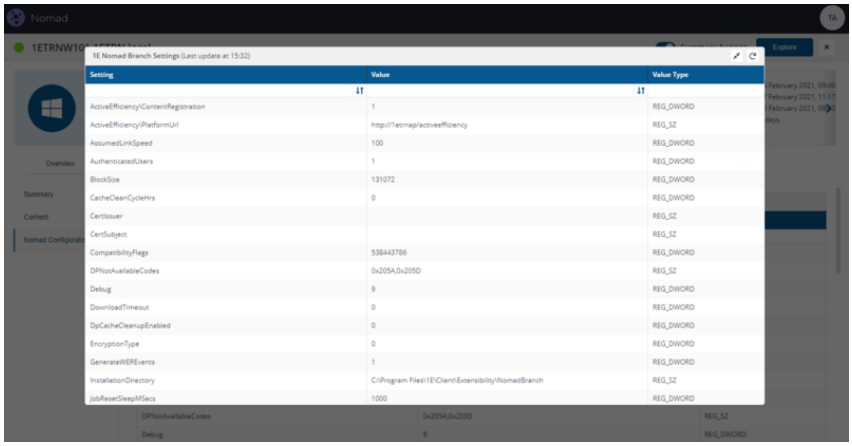
Instructions to help with the following Nomad features: Nomad cache, CacheCleaner, Single Site Download, Nomad jobs, NomadBranch service.



The **1E Nomad Branch Settings** panel is expandable. Moving your mouse over the panel reveals an **Expand** button on the top left of the panel and a refresh button. Clicking the refresh button, re-runs the **1E-Nomad-NomadBranchSettings** instruction.



A full list of Nomad registry values by feature are available on the Nomad registry values page. Registry values for NomadBranch are located in: *HKLM\Software\1E\NomadBranch*



9.6.2.4.7 Summary banner

The Summary banner displays a quick summary of the information provided in the various tabs displayed in the Device View. It can be viewed by toggling the **Summary banner** switch to on.

The following picture shows the Summary banner displayed for a particular device.

The following table describes the information provided in the Summary banner.

<table>
<tr><th>Panel</th><th>Description</th><th>Data source</th></tr>
<tr><td></td><td>Shows details equivalent to the following tiles:
<table>
<tr><th>Tab</th><th>Panel</th><th>Column</th><th>Tile</th><th>Description</th><th>Example</th></tr>
<tr><td>Overview</td><td>Details</td><td>Hardware and Operating System</td><td>Operating System</td><td>Version</td><td>Windows 10 Pro 20H2 (x86)</td></tr>
<tr><td>Hardware and Operating System</td><td>Hardware</td><td>Device Type</td><td>Desktop</td><td></td><td></td></tr>
<tr><td>Hardware and Operating System</td><td>Hardware</td><td>Manufacturer</td><td>VMware, Inc</td><td></td><td></td></tr>
<tr><td>Hardware and Operating System</td><td>Hardware</td><td>Model</td><td>VMWare Virtual Platform</td><td></td><td></td></tr>
<tr><td>Identification</td><td>Location</td><td>Location</td><td></td><td></td><td></td></tr>
<tr><td>Identification</td><td>Identification</td><td>Criticality</td><td>Undefined (0)</td><td></td><td></td></tr>
</table></td><td>Data from Tachyon Master (the latest online status message)</td></tr>
</table>

Panel	Description	Data source

Shows details equivalent to the following tiles:

Tab	Panel	Column	Tile	Description	Example
Overview	Details	Hardware and Operating System	Hardware	CPU Type	Intel(R) Xeon(R) CPU X5650 @2.67GHz x86
Hardware and Operating System	Hardware	RAM	3071 MB		
Identification	Identification	1E Client	v5.2.5.251		
Hardware and Operating System	Operating System	Version	v10.0.19042.746		
Hardware and Operating System	Operating System	Virtual/Physical	VMWare		

Shows details equivalent to the following tiles:

Tab	Panel	Column	Tile	Description	Example
Overview	Details	Identification	Location	Timezone	UTC+00 - Europe/London (Inferred)

Panel	Description					Data source
	Identification	Identification	Domain	1ETRN		
	Connectivity and Activity	Activity	User	1ETRN\Administrator		
	Connectivity and Activity	Connectivity	Local IP Address	10.0.1.3/24		
					Netmask	255.255.255.0

Shows details equivalent to the following tiles:

Tab	Panel	Column	Tile	Description	Example
Overview	Details	Connectivity and Activity	Connectivity	First Connected	22 March 2021, 12:17 UTC
Connectivity and Activity	Connectivity	Last Connected	27 April 2021, 09:23 UTC		
Connectivity and Activity	Activity	Last Boot	18 March 2021, 12:24 UTC		
				Up time	a month

Shows details equivalent to the following tiles:

Panel	Description	Data source

Tab	Panel	Column	Tile	Description	Example
Overview	Details	Identification	Grouping	Mgmt. Groups	All Devices All Win10 Workstations Servers.

9.6.2.4.8 Additional Device View tabs

In addition to the **Downloads** tab, there are a series of tabs, each corresponding to an app, feature or data set implemented in Tachyon.

The **Overview** and **1E Client** tabs are always present in the **Device View**. Other tabs are visible if an app has been installed and is licensed.

Each tab has one or more panels with tiles populated with data from various sources, some by instructions that are run instantly, with results cached for 3 minutes. An appropriate error message is displayed instead of a tile in the following circumstances:

If the device is offline, as indicated by the color of the icon in the top left

The user does not have at least Viewer permission to view use the license the tab or panel

The user does not have questioner permission to run the instruction

An instruction has not been uploaded.

The The Device View tabs and panels page lists the names of tabs and their panels, and a description of each tile indicating how the tile is populated.

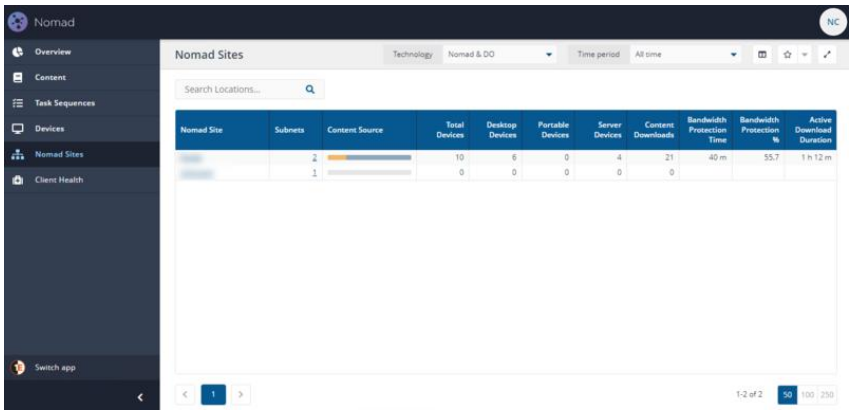
9.6.2.5 Nomad Sites page

The Nomad Sites page is primarily designed to show how the network is being used for content distribution in different locations. It focuses on the volume of content downloaded from peers vs over the WAN, rather than the status of specific Content titles in a given site. You can see what content is available by looking at the Content tab for that site.

> **Note**
>
> A Nomad Site corresponds to Nomad Single Site Download (SSD) site. Customers that have implemented SSD and upgraded ActiveEfficiency to the Nomad app and Content Distribution will see their defined SSD locations displayed as **Nomad Sites** in the app.
>
> Any subnets that are not included in a Nomad SSD Site definition will be represented in a site named **Unknown**. If no SSD sites have been defined, all subnets will be included in the 'Unknown' site.

9.6.2.5.1 Navigation and filtering

By default, the table lists **Nomad Sites** from which download activity has been reported within the selected **Time period**. These defaults can be modified using the **Technology** filter (to show Nomad or DO activity only) and the **Time period** filter.



The **Network Sites** page has the following columns, displayed by default in the order shown in the table.

Column	Description
Nomad Site	The name of the site as defined in the Content Distribution database. Nomad sites are typically defined using a script that imports site definition from another source, such as Active Directory Sites and Subnets, in which case the site name will be derived from that original source (e.g. AD Site Name).
Subnets	The count of subnets included in the Nomad site. Clicking on the number opens a 'drawer' that shows the peer-to-peer efficiency for each subnet in the site. Clicking on the subnet in this drawer shows the devices in that subnet reporting download activity within the selected **Time period**.
Content Source	A bar representing the volume of content downloaded in that site from **peers** (gray) and from the **WAN** (orange) within the selected **Time period**.
Bandwidth Protection Time	Duration the client backed off from downloading to save download bandwidth.
Bandwidth Protection %	Bandwidth Protection shown as a percentage of downloads.

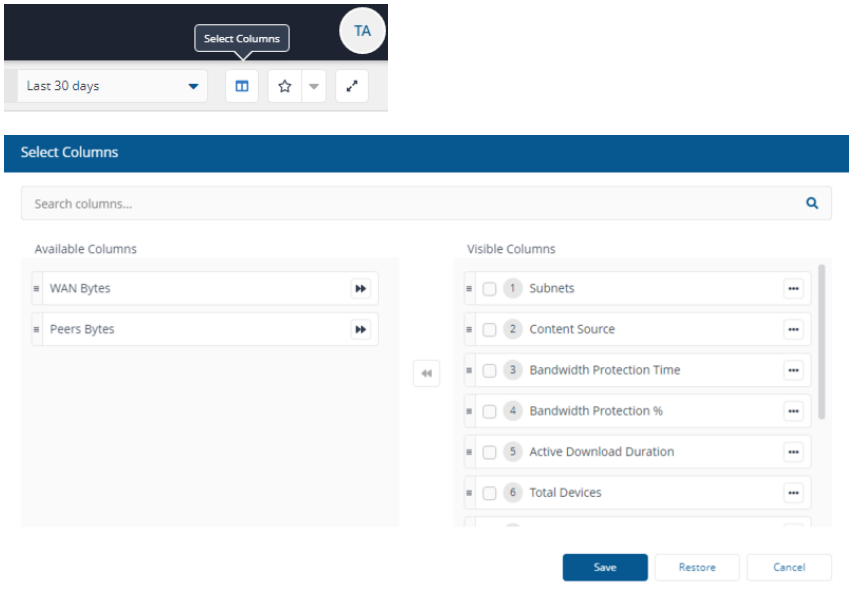
Column	Description
	This is the result of the **Bandwidth Protection Time** column dived by the **Active Download Duration** and multiplied by 100.
Active Download Duration	Duration for which client actively downloaded the content, this excludes any kind of interruption while downloading, for example network issues.
Total Devices	Representing the number of devices in the site that have reported download activity within the selected **Time period**.
Desktop Devices	A subset of Total Devices that are desktop devices (based on chassis type) and therefore most likely 'fixed' to the site.
Portable Devices	A subset of Total Devices that are portable devices (based on chassis type) and therefore may move from site to site.
Server Devices	A subset of Total Devices that are running a Server Operating System and therefore most likely 'fixed' to the site.
Content Downloads	Representing the total number of downloads at the site for which activity has been reported within the selected **Time period**.
WAN Bytes	Representing the total volume of content that has been downloaded by devices in that site from the WAN. The number is represented in units of Bytes, KB, MB or GB as appropriate to fit in the column. **Note** This metric is not visible by default, you can select it using **Select Columns**.
Peers Bytes	Representing the total volume of content that has been downloaded by devices in that site from peers. The number is represented in units of Bytes, KB, MB or GB as appropriate to fit in the column. **Note** This metric is not visible by default, you can select it using **Select Columns**.

9.6.2.5.1.1 Select Columns

On the pages where you can pick the displayed columns, you'll see the following **Select Columns** control.

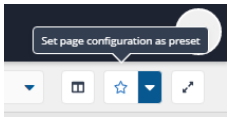
When you click on the **Select columns**control it opens a popup displaying the columns shown on the current screen and any additional columns you can select, the controls are:

Control	Explanation
Available Columns	Columns, which are by default hidden from display on screen. You can still include any of them to display on screen.
Visible Columns	Displays the list of columns displayed on screen. Mandatory Columns cannot be excluded, the selection controls for these items are disabled. They can still be moved up or down.
Arrow buttons	To move up or move down, exclude or include any column, clicking on the ellipsis displays these additional controls.
Drag and drop	You can drag and drop columns to change how they are displayed.
Exclude columns	Exclude column button allows you to select columns to exclude from the current display.

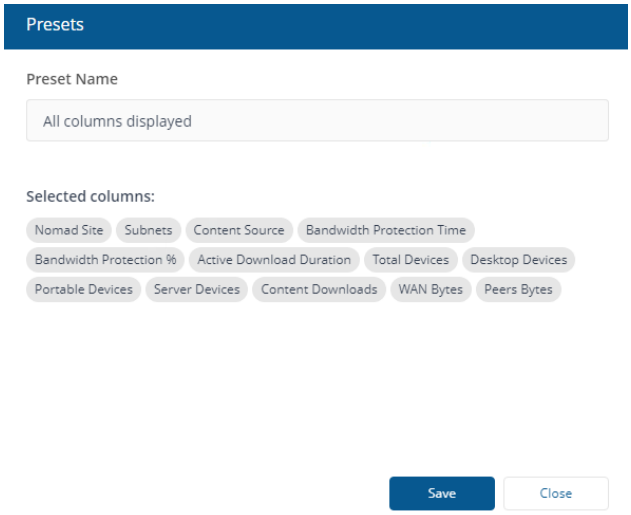


9.6.2.5.1.2 Set page configuration as preset

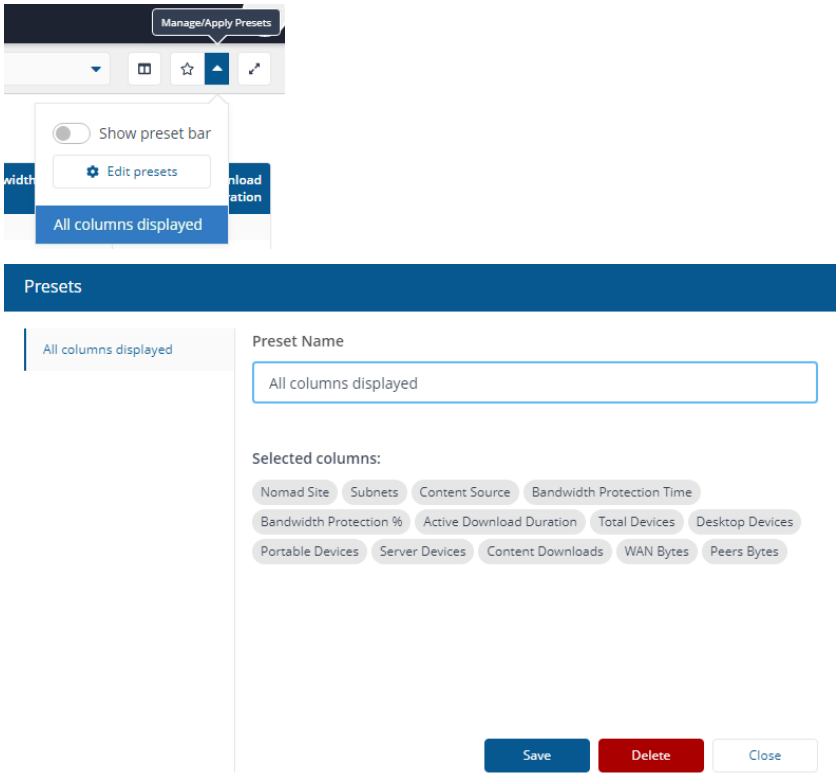
If you have amended the displayed columns using the **Choose columns** control, you can then save the view as a preset which will be available later.



Clicking **Set page configuration as preset** displays the **Presets** popup. Here, you can give the view a name, in the shown example this is called **All columns displayed** as we have chosen to display every available column.



Once saved, you can select your saved views using the **Manage/Apply Presets** control or edit them by clicking **Edit presets**.



9.6.2.5.1.3 Technology filter

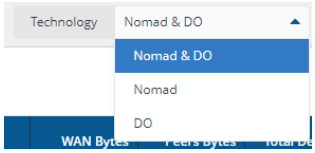
You can use the technology filter to differentiate between downloads through Nomad or Delivery Optimization (DO).

The following options are available:

Nomad & DO (Default)

Nomad

DO.



Note

If this filter is applied to any page, it is reflected on all other pages in the Nomad App.

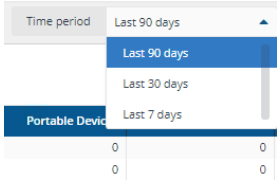
9.6.2.5.1.4 Time period filter

Using the **Time period**filter at the top of the page, you can narrow down the results by date. You can choose from the following options:

Last 90 days

Last 30 days (Default)

Last 7 days.

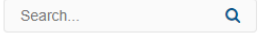


Note

If these filters are applied to any app page, it is reflected on all other pages in the Nomad App.

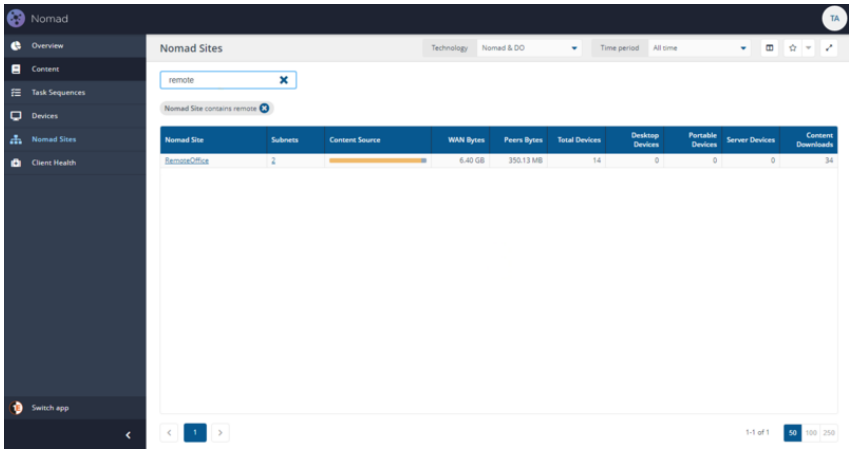
9.6.2.5.1.5 Search...

Use the search box at the top left of the page to filter by specific criteria, for example in the picture opposite the default view has been filtered by Network Sites containing remote in their title.



Note

Navigating away from this view resets the table to its default view.

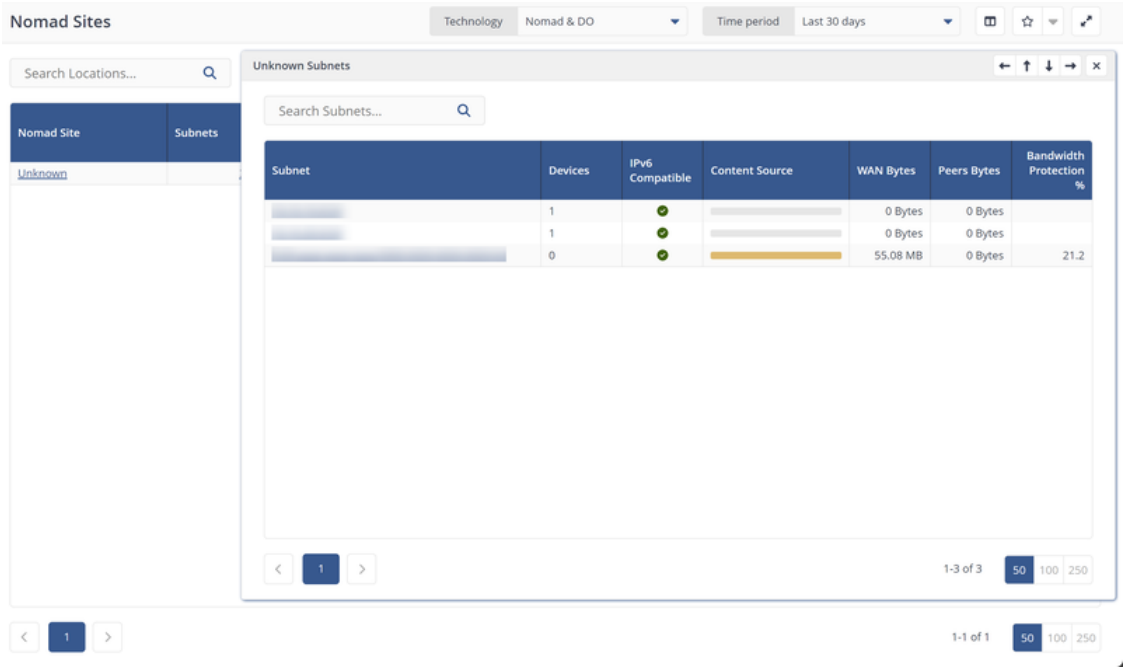


9.6.2.5.1.6 Subnets drawer

A drawer that opens up when you click on **Subnets**, **Content Source**, **WAN Bytes** etc. except **Network Location**. It shows a list of all Subnets falling under that location, with the following purpose:

Column	Description
Subnet	Subnet address (Clicking on this column takes you to the Network Location details page with selection based on this subnet).
Devices	Count of devices under this subnet.
Content Source	Percentage of downloads by WAN or Peers and content size. Hovering your mouse over the Content Source bar shows the percentage and download size per Content Type.
WAN Bytes	Representing the total volume of content that has been downloaded by devices in that site from the WAN. The number is represented in units of Bytes, KB, MB or GB as appropriate to fit in the column.
Peers Bytes	Representing the total volume of content that has been downloaded by devices in that site from the Peers. The number is represented in units of Bytes, KB, MB or GB as appropriate to fit in the column.
Bandwidth Protection %	Bandwidth Protection shown as a percentage of downloads.

Column	Description
	This is the result of the **Bandwidth Protection Time** column dived by the **Active Download Duration** andmultiplied by 100.

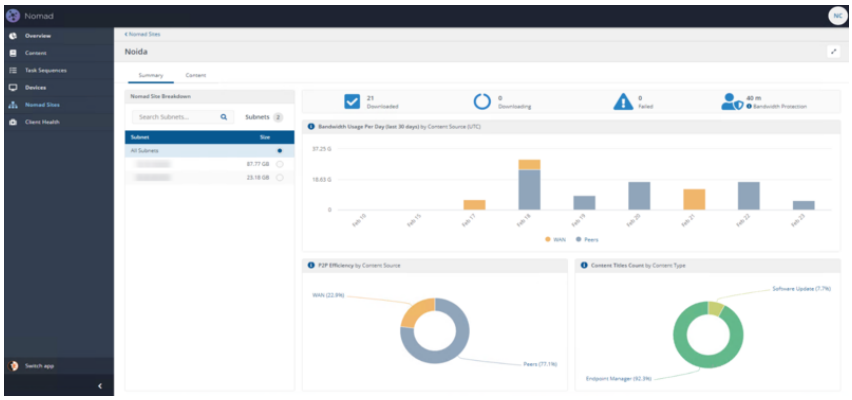


9.6.2.5.2 Nomad Site details

Clicking a **Nomad Site** takes you to the Nomad Site details page and shows information for a specific site. It includes two tabs:

Summary: Summary information about the site.

Content: All content downloaded in a Network Location.



9.6.2.5.2.1 Summary tab

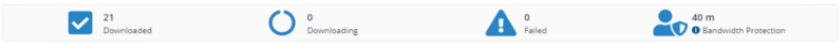
The Summary tab shows summary information about the site.

9.6.2.5.2.1.1 Top Status Bar

The top status bar shows high-level statistics similar to the one on the Overview page:

Status	Description
Total	Number of downloads on devices that are currently in the site.
Downloading	Number of downloads currently in progress in the site.
Downloaded	Number of downloads on devices that are currently in the site that have successfully completed.
Cancelled	Number of downloads on devices that are currently in the site, whose latest status was Cancelled.
Bandwidth Protection	Bandwidth Protection allows Nomad to adjust the speed of ongoing downloads to save bandwidth for other business use. Bandwidth Protection ensures Nomad doesn't consume excess bandwidth and hinder other business activity. **Note** When viewing individual Nomad sites, all data is displayed on the details page, irrespective of any time duration filter you have set on the **Nomad Sites** page. As a result, if you have set the **Time period** filter on the **Nomad Sites** page to, for example, **Last 7 days**, you may see a different result for all data except **Bandwidth Usage Per Day (Last 30 days) by Content Source (UTC)**, which displays data only for the previous 30 days.

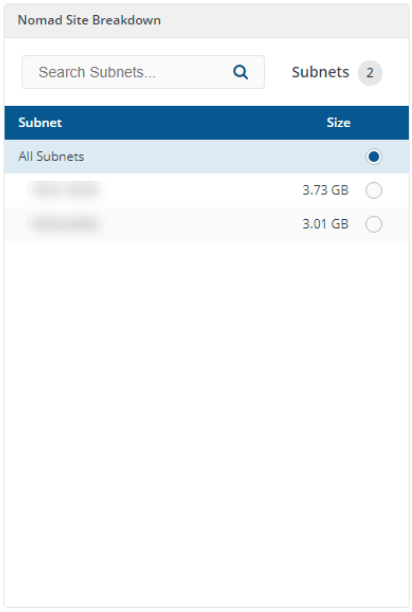
Clicking on any of the icons will take you to the Content tab filtered according to the clicked status icon.



9.6.2.5.2.1.2 Subnet Side Panel

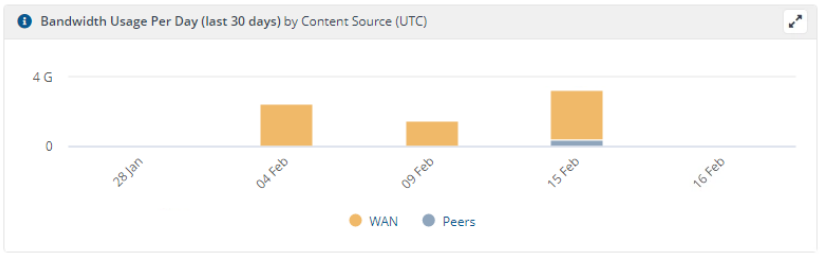
The Subnet list in the left panel shows every subnet in the selected site. By default, the page shows aggregated data for the entire site. You can filter page to examine a specific subnet within the site.

Panel item	Description
Search Subnets...	In large sites you can search for a subnet using the search box.
Subnets	The total number of subnets in the site is shown in the Subnets 'badge'. in our example the total number is **3**.
Subnet	A list of subnet detected for that Network Site.
Size	The **Size** column in this list indicates the total volume of content downloaded in that subnet.



9.6.2.5.2.1.3 Bandwidth Usage Per Day (Last 30 days) by Content Source (UTC)

The **Bandwidth Usage Per Day (Last 30 days) by Content Source (UTC)** tile represents daily download activity in this site over the last 30 days.



A column is displayed for each day where download activity was reported from devices that were in the site on that day. If a device moves into another site, this chart will still show content that it downloaded while it was in this site.

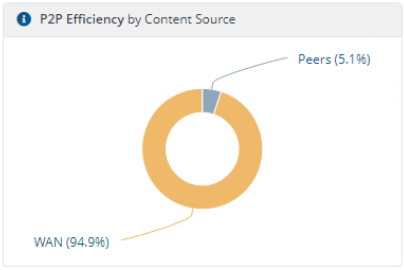
Each column indicates the volume of content that was downloaded over the **WAN** (in orange) or from **Peers** (in grey). Hovering over a segment of the column displays the volume of content downloaded on that day.

This view demonstrates the value that Nomad and Delivery Optimization provide through reduced WAN traffic. If the majority of content is being downloaded over the WAN, it could indicate that peers are simply not available (e.g. users working from home) or it could be an indication that Nomad or Delivery Optimization are not correctly configured to optimize content from peers.

> **Note**
>
> The columns on this chart are not clickable - they are for data visualization only and do not navigate to another view of the data.

9.6.2.5.2.1.4 P2P Efficiency by Content Source

The **P2P Efficiency by Content Source** tile represents the overall peer-to-peer efficiency across the site.



The data is grouped by source (**Peers** and **WAN**) and displayed as a donut chart showing the volume of content downloaded from **Peers** (in grey) and from the source over the **WAN** (in orange).

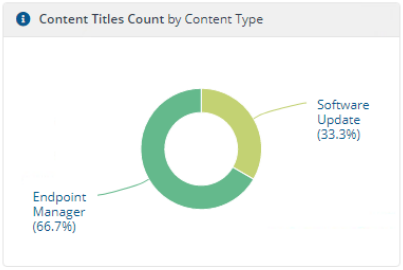
This gives an indication of the overall value of Nomad and Delivery Optimization within the site. Ideally, more content will be downloaded from peers than from the source over the WAN, thereby saving network bandwidth.

Where this is not the case, it could be due to many users working remotely without any local peers, or it could be due to configuration settings on the client that are not optimized for peer-to-peer caching and availability.

> **Note**
>
> Clicking on the chart navigates to the **Content** tab filtered by either **Peers** or **WAN**, for that subnet.

9.6.2.5.2.1.5 Content Titles Count by Content Type

The **Content Title Count by Content Type** tile shows the total number of unique Content Titles where there is download activity reported for the latest version of the content within the site. The data is grouped by **Content Type**.



The app reports on two Content Types:

Endpoint Manager - in this release this includes CM Applications and Packages.

Software Updates - includes any Microsoft Software Updates deployed through CM or Windows Update.

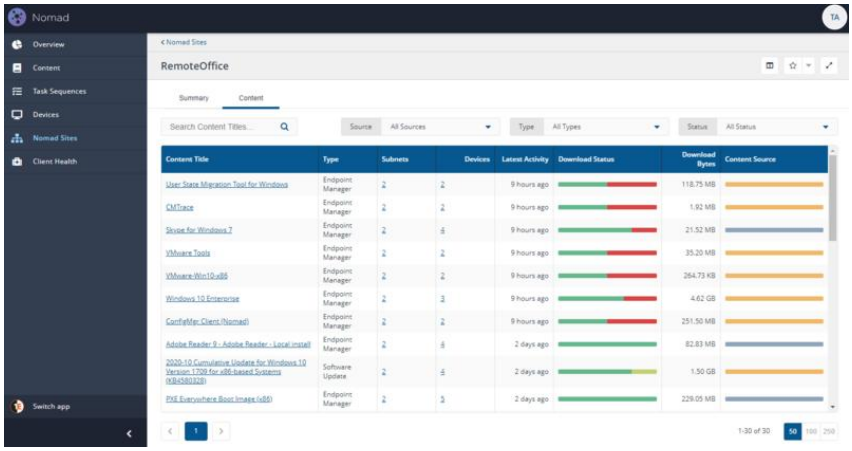
In a future release these will be expanded to include other content types such as Endpoint Manager Intune applications, Microsoft Store apps.

Hovering over a **Content Type** segment of the chart displays the count of Content Titles of that type, also represented as a percentage of all Content Titles.

> **Note**
>
> Clicking on a **Content Type** segment of the chart will navigate to the Content tab, filtered to show Content Titles of the selected segment.

9.6.2.5.2.2 Content tab

A table showing all content downloaded in a Network Location and optionally filtered on the Subnet selected from the **Summary** tab.



Columns	Description
Content Title	Name of the content (Clicking on this column takes you to the details of the content).
Type	Type of content.

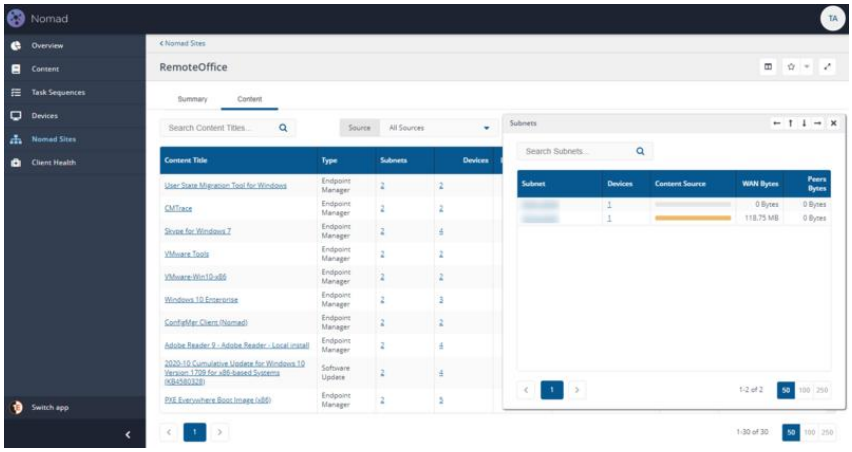
Columns	Description
Subnets	Count of subnets this content is downloaded to (Clicking on this column opens a drawer that expands on the list of subnets).
Devices	Count of devices this content is downloaded to (Clicking on this column opens a drawer that expands on the list of devices).
Latest Activity	Time when most recent activity happened.
Download Status	Flexible chart showing distribution of download statuses.
Download Bytes	Representing the total size of downloads for this content for this Location and Subnet. The number is represented in units of Bytes, KB, MB or GB as appropriate to fit in the column.
Content Source	Same chart as on Main page but for this Content only.

9.6.2.5.2.2.1 Subnet draw

A drawer that opens up when you click on the subnets count. It shows a list of all subnets falling under that location and have downloaded the specified content, with the following functionality:

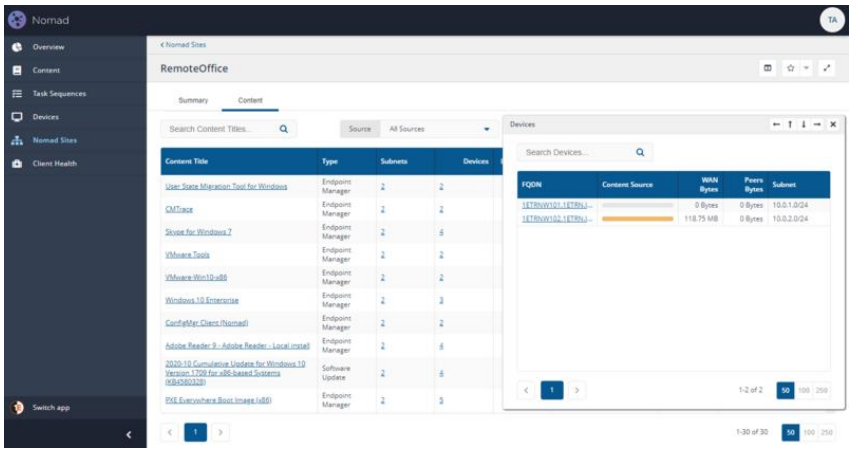
Columns	Description
Subnet	Takes you to Devices drawer with filter on this subnet.
Devices	Number of devices in this subnet, clicking it will take you to Devices drawer with filter on this subnet.
Content Source	A flex bar chart showing distribution across WAN and Peers.
WAN Bytes	Representing the total size of downloads for this content for this Location and Subnet. The number is represented in units of Bytes, KB, MB or GB as appropriate to fit in the column.
Peers Bytes	Representing the total size of downloads for this content for this Location and Subnet.

Columns	Description
	The number is represented in units of Bytes, KB, MB or GB as appropriate to fit in the column.



9.6.2.5.2.2.2 Devices drawer

A drawer that opens up when you click on the device count. It shows a list of all devices falling under that location and have downloaded the specified content.



Columns	Description
FQDN	FQDN of the device (Clicking on it will take you to the device details).
Content Source	A flex bar chart showing distribution across WAN and Peers.
WAN Bytes	Representing the total size of downloads for this content for this Location and Subnet.

Columns	Description
	The number is represented in units of Bytes, KB, MB or GB as appropriate to fit in the column.
Peers Bytes	Representing the total size of downloads for this content for this Location and Subnet. The number is represented in units of Bytes, KB, MB or GB as appropriate to fit in the column.

9.6.2.6 Client Health page

The Client Health page shows information from two Integrated Product Packs provided with the Tachyon Platform:

MEMCM Client Health Policy

Nomad Client Health Policy.

These Integrated Product Packs are represented on the Client Health page by two sets of panels that can be explored in the Rules and Devices pages in Introducing Guaranteed State.

9.6.2.6.1 Introduction to Guaranteed State concepts

Guaranteed State allows you to easily check and enforce device state. Device state can represent just about anything you'd like to be set in a certain way for a collection of devices. Once you have imported an Integrated Product Pack you can configure and deploy policies to manage various device attributes. For example:

Registry keys

Services

Config Manager metrics such as client cache usage

Disk free space

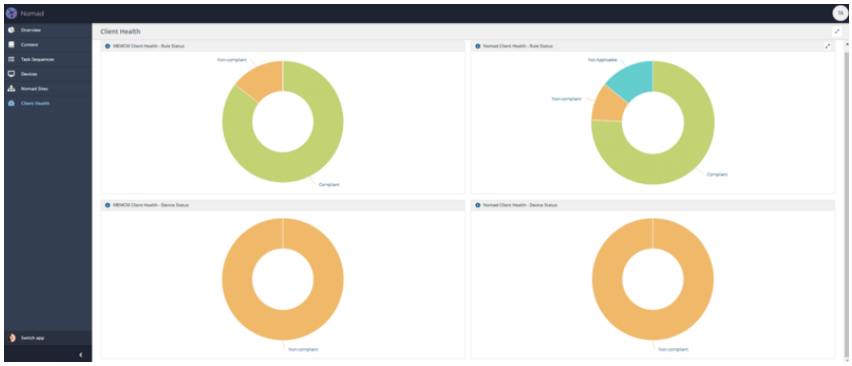
WMI namespaces and classes.

Before using Guaranteed State you need to upload some policies (with their rules, triggers and preconditions). Please refer to Installing the Nomad app and 1E Content Distribution - 1E Nomad product packs for details about Nomad feature-related Product Packs.

Product Packs are required to support various features of Nomad**:**

Classic Product Packs - contain instructions, for use in Explorer and other Tachyon applications

Integrated Product Packs - contain policies, rules and fragments for use by Guaranteed State, and may also include instructions.



The state of devices where Guaranteed State policies have been deployed is represented in this form.

The user has the ability to drill down into the percentage of failures for each group of device states. For example, where the meaning of device states and their precedence is as follows:

State	Description
Unknown	The device has yet to receive, evaluate or report back on its compliance state for at least one rule.
Error	The device has failed to evaluate at least one deployed rule. For example a device may report 97% of deployed rules as **Not Applicable**, but since 3% of the deployed rules reported as Error this means the whole Device State is marked as **Error**.
Not Applicable	At least one rule deployed to the device is not applicable. For example, this would occur if a Windows-specific rule was deployed to a non-Windows device.
Non-compliant	At least one rule deployed to the device failed compliance checks. For example in the example above 86% of policy rules are compliant for the high-lighted device, but since 8% of the rules are Non-compliant the state of the whole device is marked as Non-compliant.
Compliant	The device passed compliance checks for every deployed policy rule.

The drill down navigates to the **Devices** report filtered on the selected **Device State** such as **Noncompliant**.

The Device State panel is shown on the Guaranteed State Overview page.

Refer to Guaranteed State Overview page page for details about other Guaranteed State Dashboard charts.

9.6.2.6.2 MEMCM Client Health Policy

Many businesses rely on Microsoft Endpoint Manager Configuration Manager (MEMCM) to deploy software, patches and updates across their company networks. It is crucial that Configuration Manager is working effectively.

The MEMCM Client Health policy monitors Configuration Manager client health and performance. It checks for cache availability, inventory cycles, service availability and Configuration Manager WMI integrity - common causes of Configuration Manager client problems on devices.

The MEMCM Client Health policy replaces the previous SCCM Client Health policy and covers the following:

Ensure the correct version of the CM client is installed and running and assigned to the correct site

Ensure the CM client is not stuck in provisioning mode

Ensure that heartbeat discovery, inventory and state messages are being sent regularly

Ensures the CM client cache is set to the correct size

Ensure the CM client log settings are correct

Ensure the BITS service exists, configured to start up automatically and is running

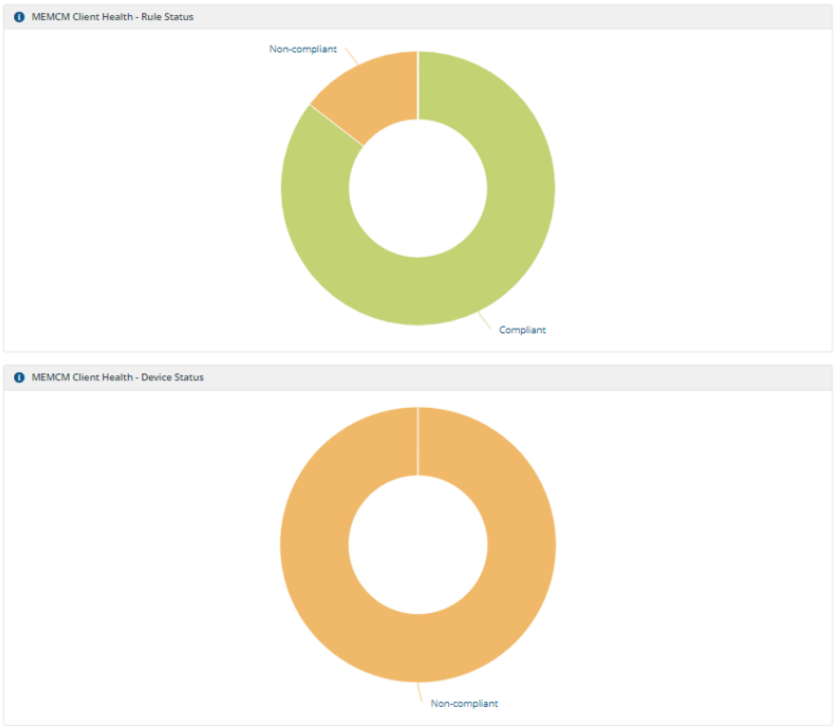
Ensure the Windows Time service exists with correct startup settings

Ensure the Windows Management Instrumentation (WMI) service exists, configured to start automatically and is running

Ensure WMI is healthy, the core CIMv2 and ccm namespaces and classes exist and that the WMI repository is consistent

Ensure the Windows Update service exists with correct startup settings, is configured to use the correct source (CM, WSUS or Microsoft Update) and that the service can connect to the source

> **Note**
>
> This policy is intended for deployment to Windows devices only.



9.6.2.6.2.1 MEMCM Client Health Rule Status example

A user has the ability to drill down into a segment, for example, to examine exactly which policy rules reported failures across all the devices for which it was deployed.

In our example, a member of the Nomad Administrator role wants to investigate why **Policy Rule Status** is showing as **Non-compliant** for 14.5% of the 16 assigned rules.

By clicking on the **Non-compliant** segment they open the Guaranteed State app on the **Rules** page which displays the associated rules, in this case these are:

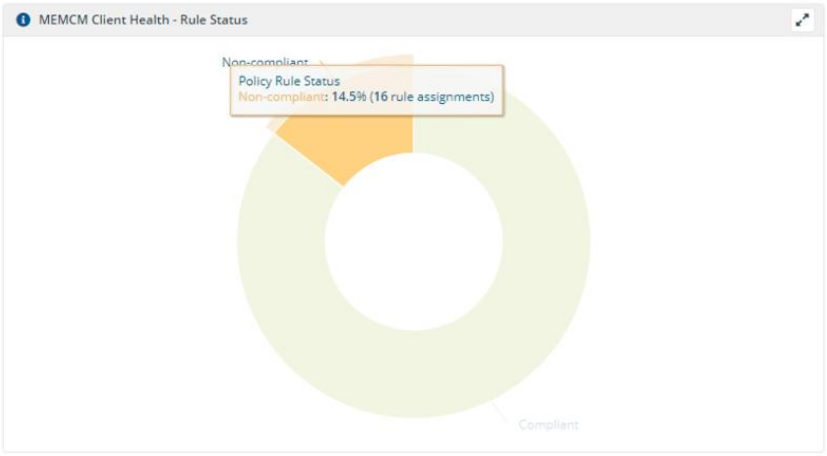
MEMCM Client FileCollectionSent

MEMCM Client IDMIFCollectionSent

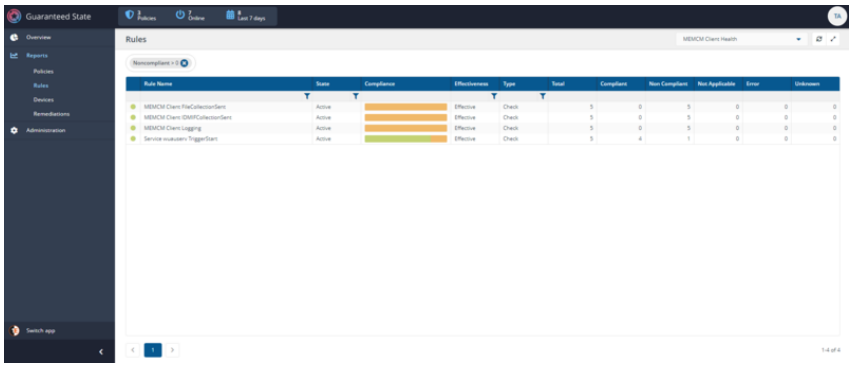
MEMCM Client Logging

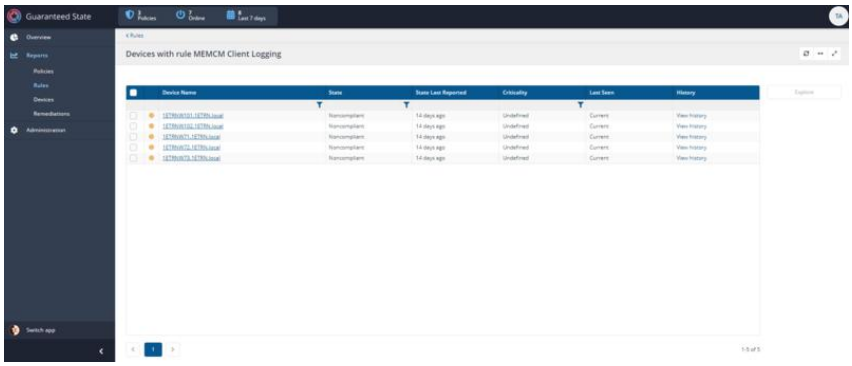
Service wuauserv TriggerStart.

You can reference a table showing the policies included in the **MEMCM Client Health Integrated Product Pack** at /document/preview/761891#UUID-54dc3ca7-e7a9-e8df-752b-d5229270d4a0.



In the Compliance column the Nomad Administrator sees there are no compliant computers for the Configuration Manager Client rules. From this point, they can click on the Compliance color bar for the Configuration Manager Client Logging Rule Name, and expose the individual devices affected.

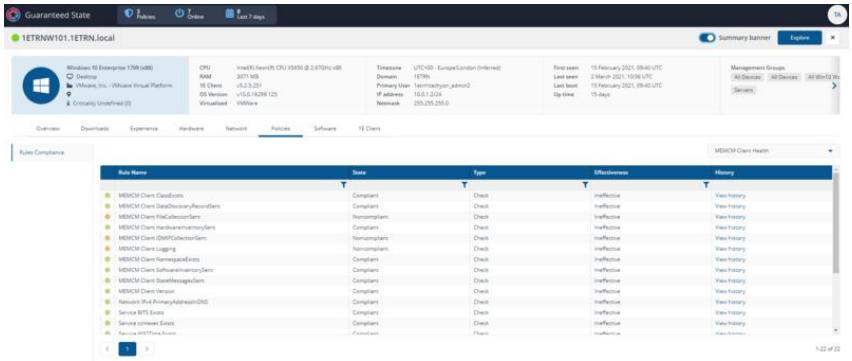




To assist troubleshooting the Nomad Administrator can click on a device name to see its Device View. This is the same view you can see in the Devices Page - Nomad Configuration in the Nomad app, but here it is focused on the Polices tab as the focus is in the Guaranteed State app, filtered on the **Configuration Manager Client Health** policy.

Note

Clicking the Device Status navigates to the **Devices** page in the Guaranteed State app filtered based on the chart segment clicked on. From the filtered **Devices** page, you can then explore an individual Device View as shown in the picture opposite.



9.6.2.6.3 Nomad Client Health Policy

Nomad is included as part of the 1E Client, and as part of that integration, we offer a Nomad client health compliance policy in Guaranteed State. This verifies common Nomad requirements such as ACP registration, disk availability, firewall exceptions, crash notifications and cache monitoring.

The Nomad client health policy replaces the client health tile in the Nomad dashboard plus additional remediation steps:

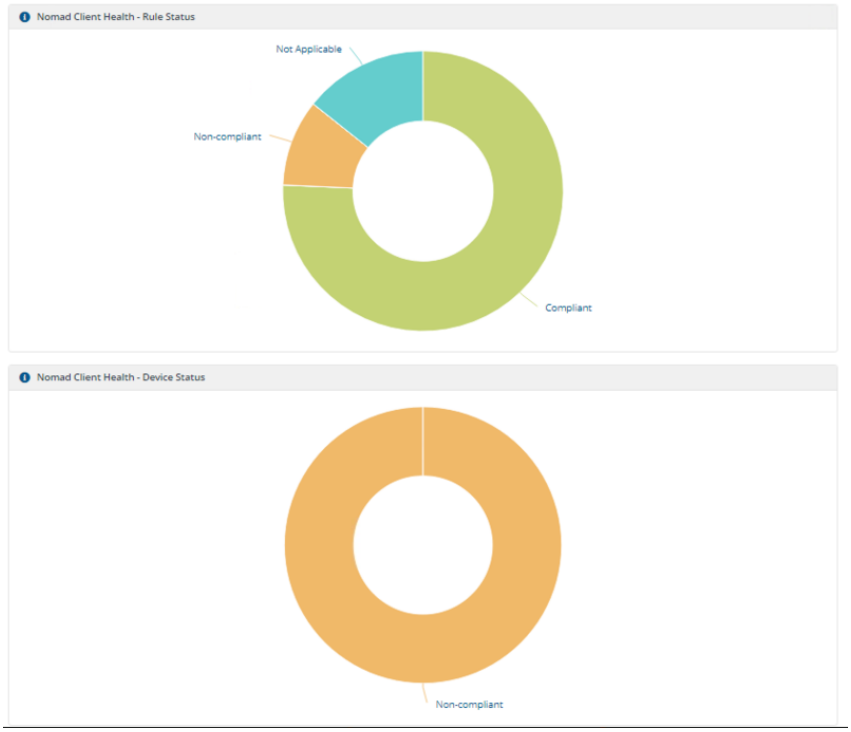
Keeps content distribution services up and running on Nomad clients, so that users are secure and productive

Ensures Alternative Content Provider (ACP) registration configuration is set

Maintains optimal disk availability and monitors cache size for storage capacity planning

Enforces Firewall exceptions.

> **Note**
>
> This policy is intended for deployment to Windows devices only.



9.6.2.6.3.1 Nomad Client Health Rule Status example

A user has the ability to drill down into a segment, for example, to examine exactly which policy rules reported failures across all the devices for which it was deployed.

In our example, a member of the Nomad Administrator role wants to investigate why **Policy Rule Status** is showing as **Not Applicable** for 14.3% of the 10 assigned rules.

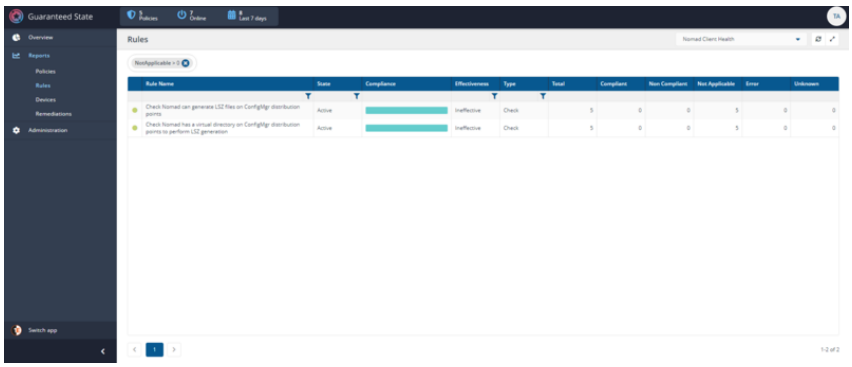
By clicking on the **Not Applicable** segment they open the Guaranteed State app on the **Rules** page which displays the associated rules, in this case these are:

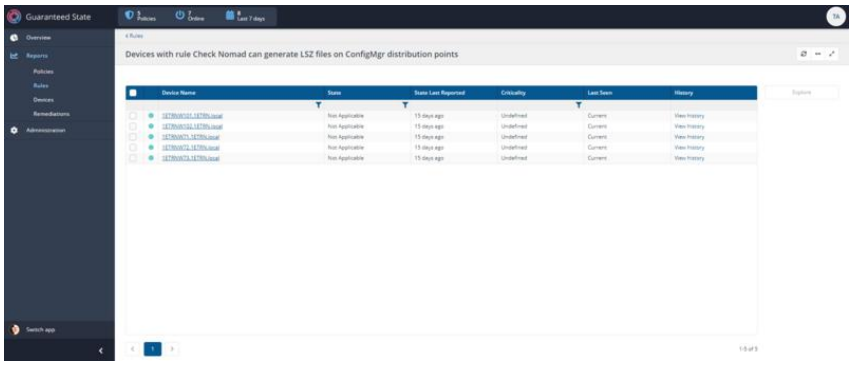
Check Nomad can generate LSZ files on ConfigMgr distribution points

Check Nomad has a virtual directory on ConfigMgr distribution points to perform LSZ generation.

You can reference a table showing the policies included in the **Nomad Client Health Integrated Product Pack** at /document/preview/761891#UUID-54dc3ca7-e7a9-e8df-752b-d5229270d4a0.

In the Compliance column the Nomad Administrator sees there are no compliant computers for the two Check Nomad rules. From this point they can click on the Compliance colour bar for the Check Nomad can generate LSZ files on ConfigMgr distribution points **Rule Name**, and expose the individual devices affected.

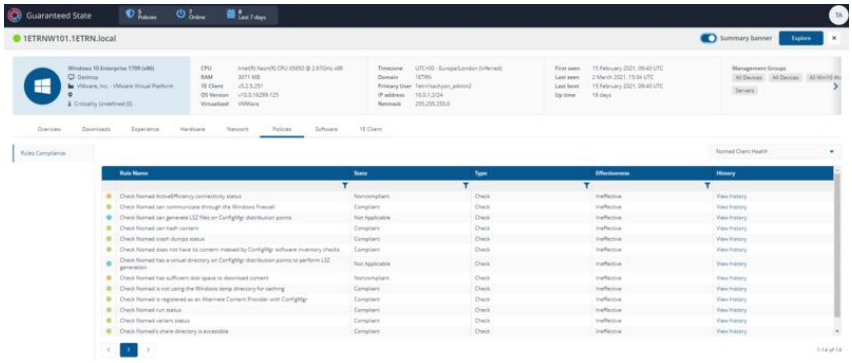




To assist troubleshooting the Nomad Administrator can click on a device name to see its Device View. This is the same view you can see in the Devices Page - Nomad Configuration in the Nomad app, but here it is focused on the Polices tab as the focus is in the Guaranteed State app filtered on the **Nomad Client Health** policy.

Note

Clicking the Device Status navigates to the **Devices** page in the Guaranteed State app filtered based on the chart segment clicked on. From the filtered **Devices** page, you can then explore an individual Device View as shown in the picture opposite.



9.6.2.6.4 Integrated Product Packs overview

Integrated Product Packs are Zip files containing Guaranteed State policies, but can also contain instructions (as an alternative to classic Product Packs which can only contain instructions).

You can upload these Zip files into Tachyon using the Tachyon Product Pack deployment tool, please refer to Uploading Integrated Product Packs for details.

1E provides a number of ready-made policies which are described on the Integrated Product Packs pages:

MEMCM Client Health Policy

Nomad Client Health Policy

Windows Client Health Policy

Tachyon Core Utilities.

These pages include lists of instructions, policies, rules, fragments (preconditions, checks, and fixes), and trigger templates. The lists have links to more detailed information about each pack in the Tachyon Product Packs reference.

You can also create your own policies using rules, fragments, and triggers from other Integrated Product Packs, for example, the Tachyon Core Integrated Product Pack.

9.6.3 Nomad tools

Tools that can help troubleshoot or configure Nomad.

Please also refer to Nomad command-line switches.

For Nomad OSD Tools, please refer to Installing Nomad Branch Tools.

9.6.3.1 Nomad Download Monitor

The Nomad Download Monitor tool (also known as NomadBranchGUI) is useful for administrators for troubleshooting downloads as they view the status of downloads on local and remote Nomad client devices.

Please refer to Installing the Nomad download monitor for details of how to install Download monitor in either **basic** or **advanced** mode.

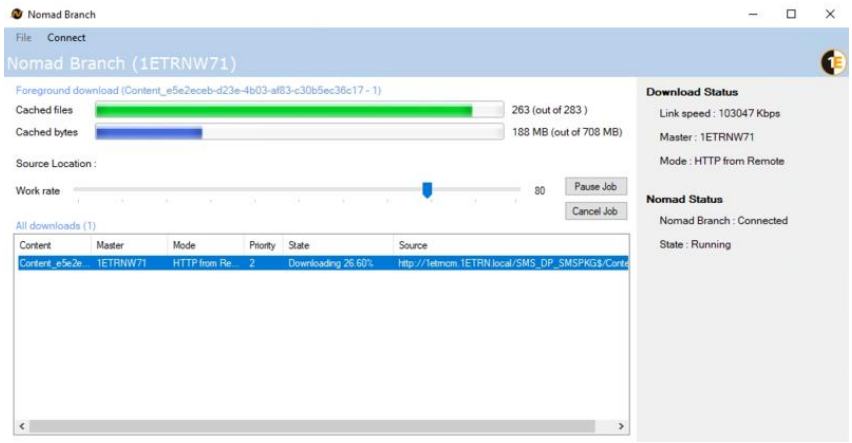
Mode	Description
Basic	You will only see progress bars in the UI. Useful for those who only need to see the status of the downloads.
Advanced	You will see an extended UI – useful for administrators to troubleshooting downloads as they can connect to remote devices to view the status of the downloads, provided they have sufficient Remote Activation DCOM permissions. By default, the Download Monitor connects to the local machine.

During a download, the NomadBranch dialog, provides you with feedback on its activities and lets you manage the impact of the download on the network link by giving you the opportunity to pause, resume or cancel it.

9.6.3.1.1 Feedback and actions

Feedback and actions	Description
Package ID	Name of the download package.
Cached files	The cached files progress bar shows the percentage of the total number of files in the package that have been downloaded. In this example, approximately a 92% of the files in the package have been downloaded. The figures at the end of the progress bar show this is exactly 263 files out of 283.
Cached bytes	The cached bytes progress bar shows the percentage of the total number of bytes in the package that have been downloaded. In this example, approximately a 26% of the total package has been downloaded. The figures at the end of the progress bar show this is exactly 188 MB out of 708 MB.
Source location	This field identifies the source of the download. In this example, the package is being downloaded using HTTP from the share, SMS_DP_SMSPKG$ For more details, refer to Peer copy over HTTP or HTTPS and PermittedLSZShares.
Work rate	The work rate slider determines the percentage of available bandwidth to use for the download. The default work rate is 80%.

Feedback and actions	Description
	For example, if you drag the slider all the way to the left (1%), it improves network availability as Nomad uses only 1% of the available bandwidth, but the drawback is that it increases the duration of the download. You can configure intra-day work rates (using MaxWorkRates) for the client to maximize the use of available bandwidth over the course of a day. Work rates only apply to transfers from a DP not to P2P transfers within a LAN, hence, it does not apply to Single Site Download (SSD) downloads.
Pause Job	Pauses a download in the queue or resumes it.
Cancel Job	Cancels a download in the queue.



9.6.3.1.2 Identifying the download to be monitored

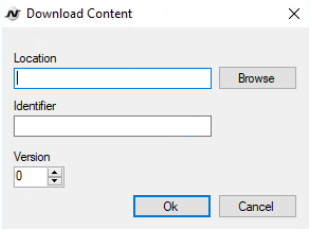
It is possible to kick off a standalone download from the **File→Download** menu. You must specify the parameters listed below in the dialog.

> **Note**
>
> We do not recommend this feature being used in any scenario other than by an Administrator during software evaluation or for troubleshooting purposes.

Download Content UI:

Parameter	Description
Location	The directory where the file is to be downloaded to. Click the **Browse** button to choose a location.

Parameter	Description
Identifier	The unique package ID for the download.
Version	The version for the package to be downloaded.

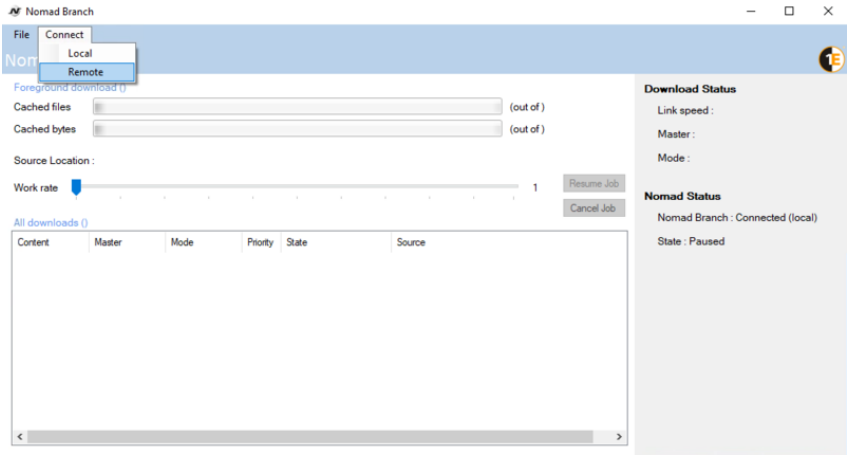


9.6.3.1.3 Connecting to a remote machine

You can only connect to a remote device if the **Download Monitor** on the client you are using has been installed in **Advanced** mode if it was installed in **Basic** mode, you can alter its behavior, for details refer to Installing the Nomad download monitor - Changing the behavior of the monitor.

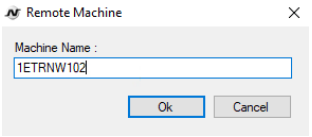
To connect to a remote device, on the system tray, double-click the **Download monitor** icon.

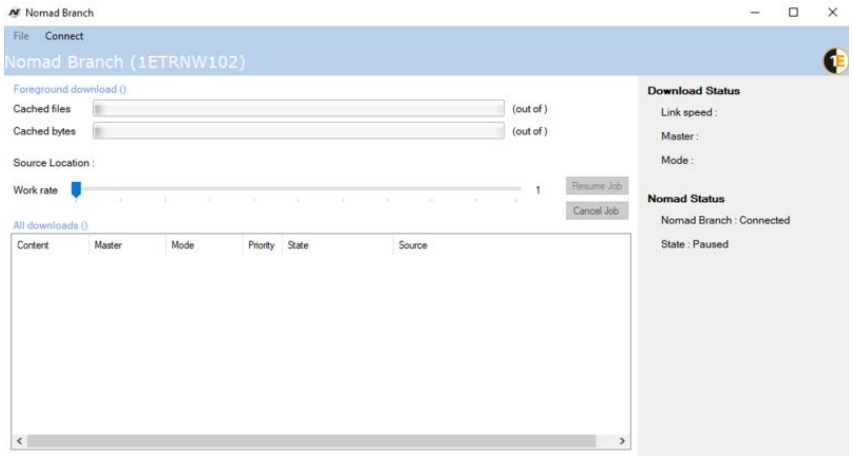
In the NomadBranch dialog, click **Connect** and choose **Remote**.



In the **Remote Machine** dialog, type the name of the machine you want to connect to, in our example this is **1ETRNW102**, alternatively, you can use its IP address. Click **OK**.

To disconnect from the remote device, click **Connect** and choose **Local**.





9.6.3.2 Nomad Baseline wizard

The Nomad Baseline wizard is used to create a Configuration Manager (CM) Baseline from the Configuration Manager console for settings related to Nomad. Baselines are used in Configuration Manager (CM) to help manage compliance settings. There are a number of reasons why you would create baselines for Nomad but specific examples include:

Using separate baselines to configure different settings for client machines and DP Servers

Defining baselines with specific settings to be applied to devices in a particular site or collection

Create different baselines to enable or disable Nomad features on devices in particular collections.

The Nomad Baseline wizard is accessible from the CM console and makes it easy to define Nomad related baselines. The files created by the wizard include a new Baseline and an associated Configuration Item that contains all the registry settings and rules used to apply Nomad registry settings.

Note

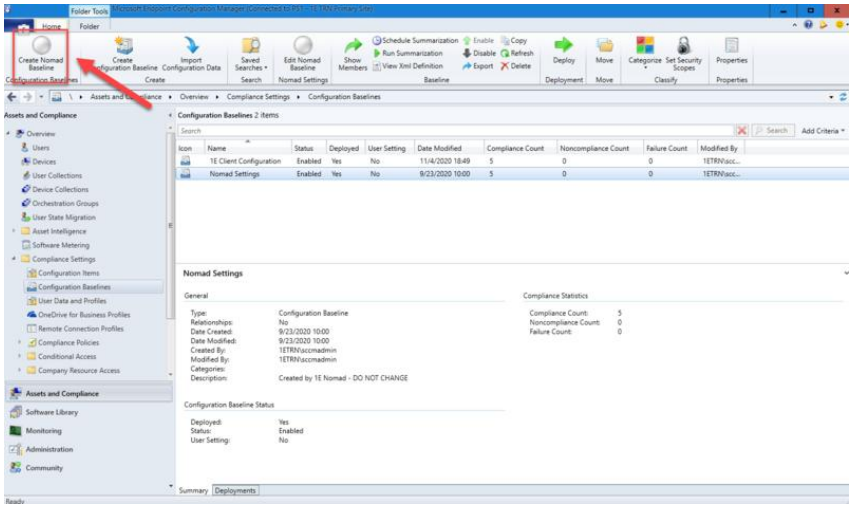
The user can choose whether to remediate or just monitor these values when deploying a particular baseline.

If the baseline is deployed just for monitoring, any non-compliance of the settings on CM clients will be reported as warnings to the server.

The evaluation or remediation of these settings depends on the interval selected in the baseline deployment.

9.6.3.2.1 Running the Nomad Baseline wizard

You can launch the Nomad Baseline wizard by clicking on the **Create Nomad Baseline** button in the **Configuration Manager→Assets and Compliance→Configuration Baselines** space.

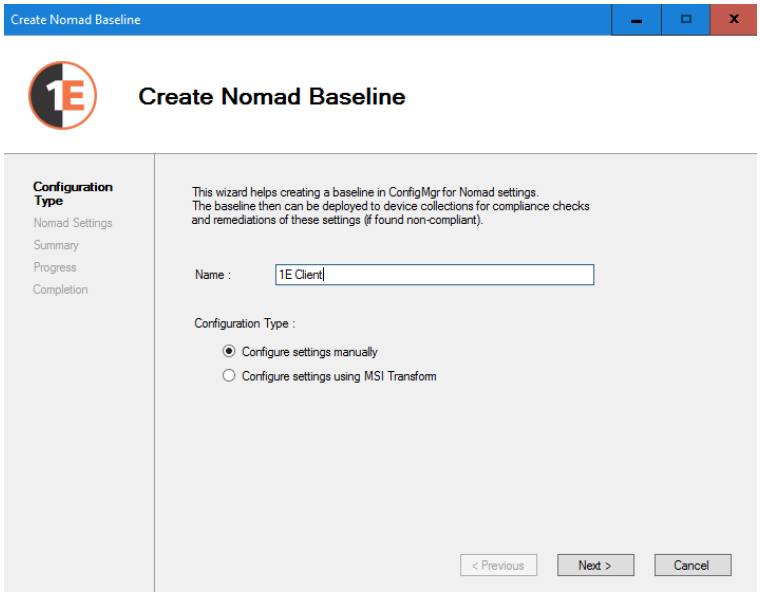


9.6.3.2.1.1 Configuration Type

The first screen of the wizard lets you define the name of the baseline and how the baseline will be populated.

You have two choices for **Configuration Type**:

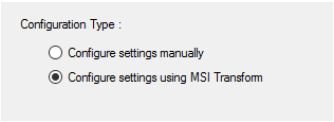
Option	Description
Configure settings manually	Select this option to populate the baseline from scratch using the screens in the wizard.
Configure settings using MSI Transform	Select this option to pre-populate the screens in the wizard by importing Nomad MSI and MST files. When this option is selected a new screen appears called **Import MST**. Before using this option you will need to have configured an MST file and have the associated Nomad installer file to hand.



9.6.3.2.1.2 Import MST

Note

This screen is only displayed if you selected the **Configure settings using MSI Transform** option on the **Configuration Type** screen.

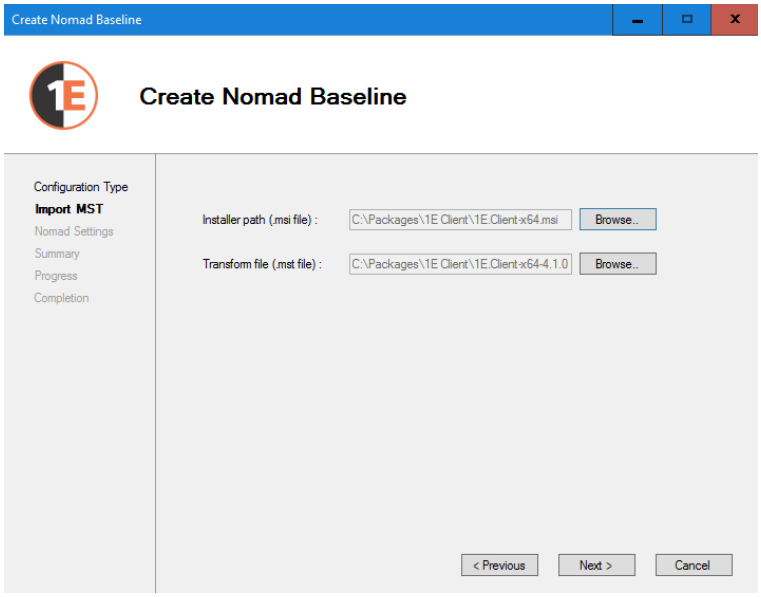


Click **Browse...** to the installer MSI file and the corresponding MST file for your chosen package.

By clicking **Next**, the wizard extracts the registry differences between the MSI and MST file and adds any corresponding rows to the **Nomad Settings** views.

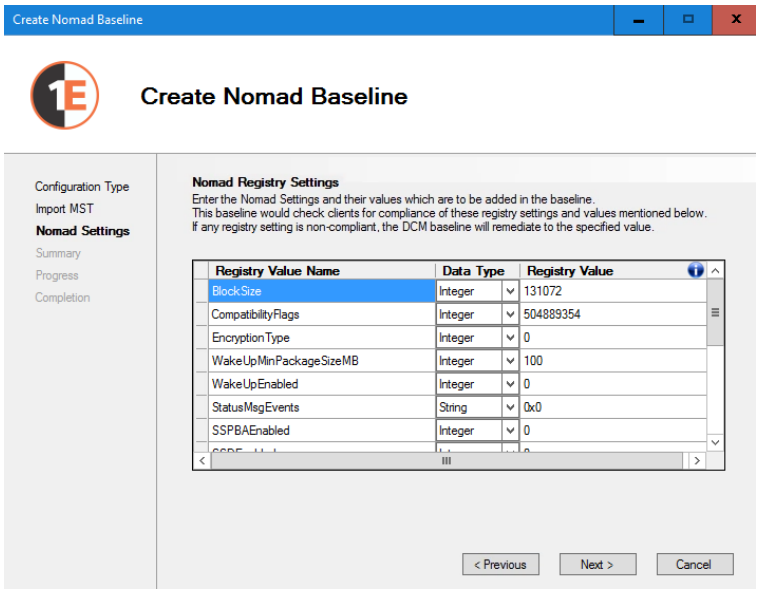
Note

Only the registry changes seen in the MST file are imported any other changes in the MST are ignored.

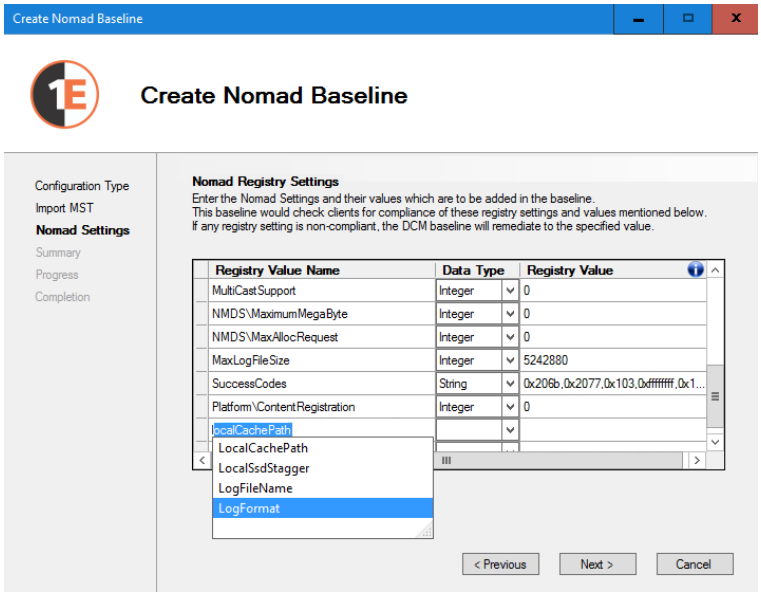


9.6.3.2.1.3 Nomad Settings

The **Nomad Settings** screen where the Nomad Registry Settings can be entered and edited.



To add a registry entry Type into the **Registry Value Name** field. The wizard provides suggestions for auto-completing the entry.



For integer values you can also enter hex numbers preceded by **0x**.

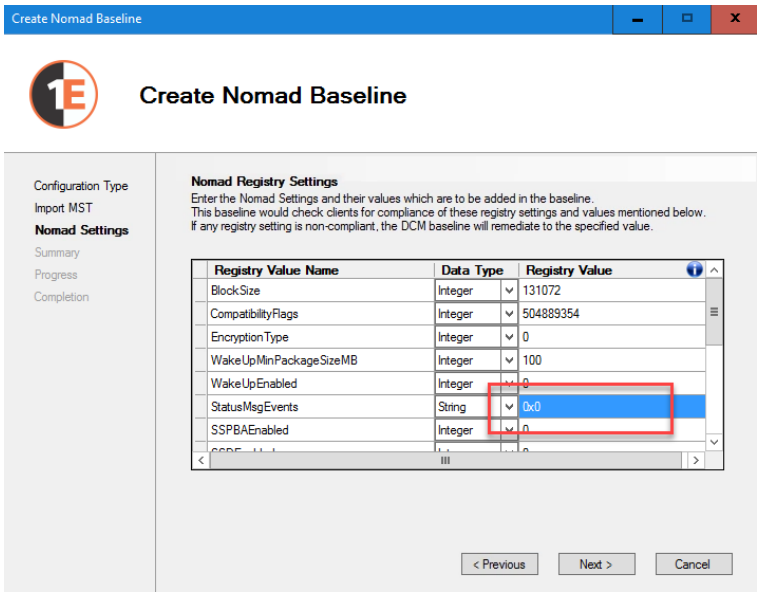
The **Nomad Settings** screen is validated by clicking the **Next** button.

The validations are:

Empty values not allowed

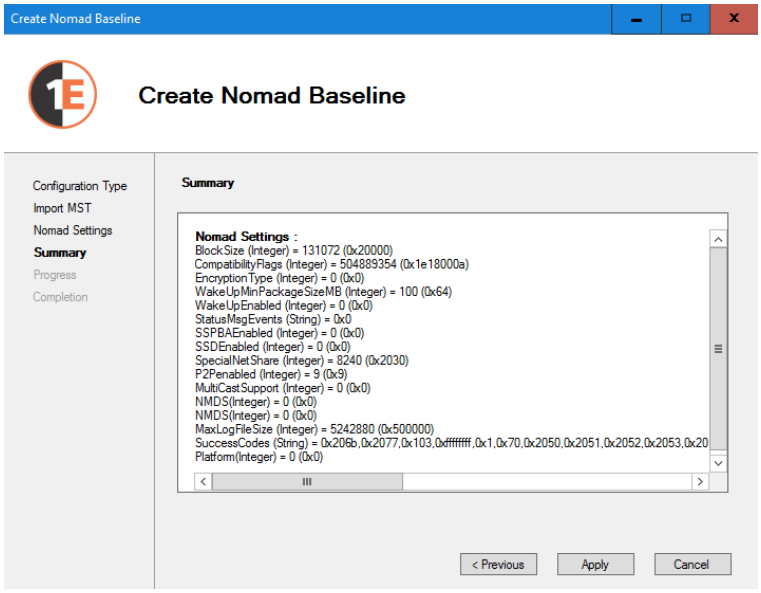
Duplicate Nomad registry settings are not allowed

When the data type is specified as an integer - only numbers (in decimal and hexadecimal format) are allowed.



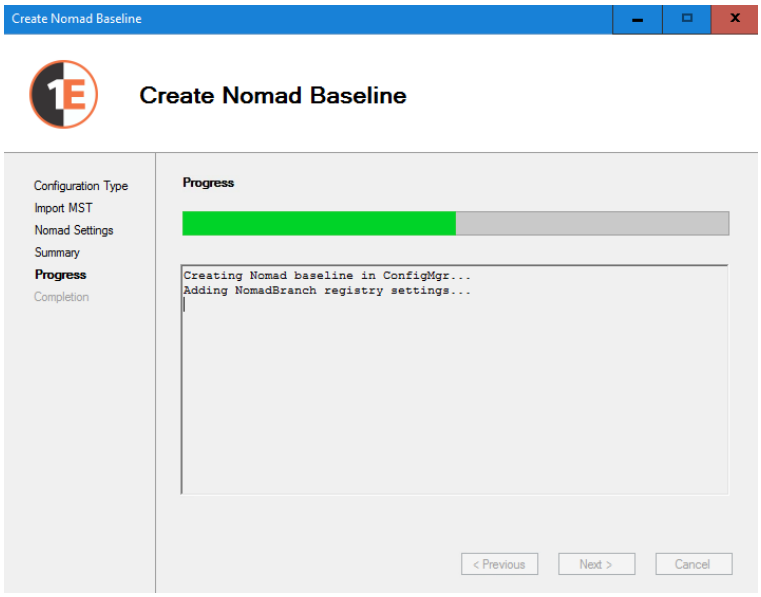
9.6.3.2.1.4 Summary

The **Summary** screen shows all the settings entered on the previous screens and lets you do a final review before clicking **Apply**.



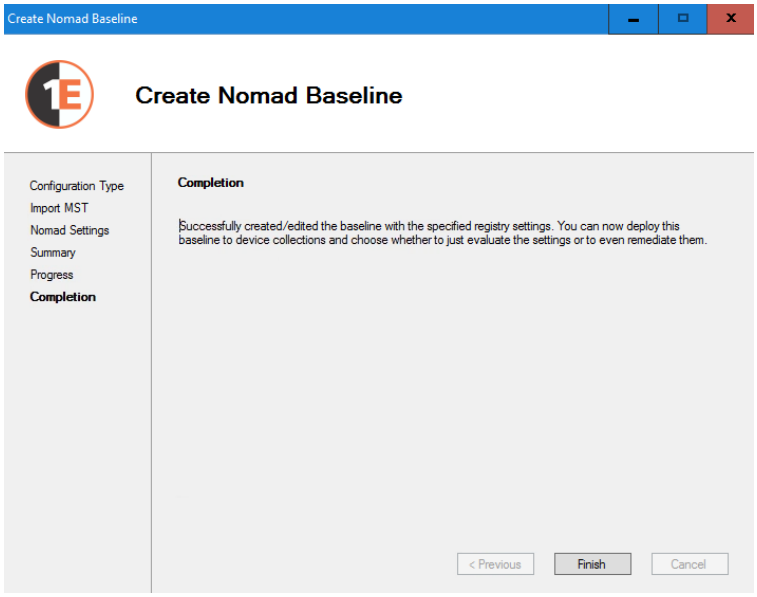
9.6.3.2.1.5 Progress

After clicking **Apply**, the wizard creates the Nomad Baseline in CM. This screen shows the current progress of the installation.



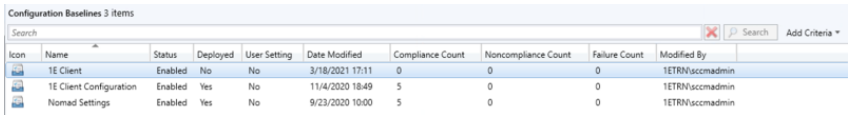
9.6.3.2.1.6 Completion

When the wizard successfully completes, you can deploy the baseline to CM device collections and choose whether to evaluate the settings or also remediate them.

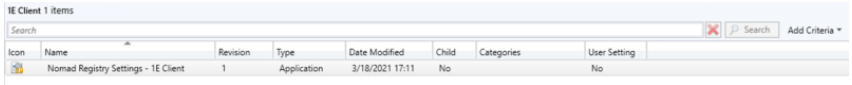


9.6.3.2.2 Nomad Baselines created in the Configuration Manager Configuration Baselines view

After clicking **Apply** on the **Summary** screen a baseline will be created with the settings made in the wizard.



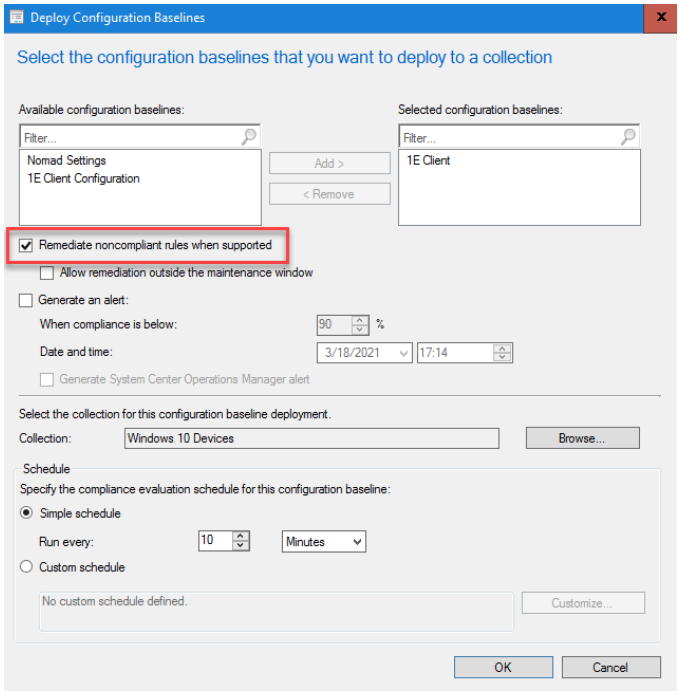
The created baseline will also contain a Configuration Item that defines the registry values and rules that determine what the baseline will remediate.



9.6.3.2.3 Deploying the baseline

The baseline created by the Nomad Baseline Wizard can be deployed to a device collection from the Configuration Manager console.

When the **Deploy Configuration Baselines** dialog is displayed you should check the **Remediate noncompliant rules when supported** checkbox if you want to remediate any values in the Nomad registry that vary from the baseline.



9.6.3.3 CacheCleaner

The downloaded content in the Nomad cache consume disk space, therefore management of the cache is critical. Because files may be re-used and distributed to other devices on the same subnet or site, the simple solution of deleting the files as soon as they have finished downloading and executing is not sufficient. Instead, Nomad has a cache cleaner utility that automatically but intelligently maintains control over the cache's disk usage.

Nomad cache is used in a number of deployment scenarios, for example scenarios and how you can monitor those deployments using the Nomad app refer to:

Deploying software with Configuration Manager

Deploying software in large networks

Deploying updates for Office 365

Using Nomad with Operating System Deployment OSD.

9.6.3.3.1 Cache clean cycle versus CacheCleaner

There are two ways to clean the cache:

The cache clean cycle - which runs automatically on a cycle and clears the unused content from the cache as a preference (default off).

The CacheCleaner and its cache cleaner rules - which is either run by Nomad during an active download or manually from the command-line.

CacheCleaner can be run when required in addition to the automated cache clean cycle, for example when reserving space for new contents to be downloaded by manually running it from

the command-line. CacheCleaner deletes content based on its priority and doesn't check its last usage date. So it is possible that content which is lower in priority but has been recently used, or is used regularly (like WIM files), may also get deleted when CacheCleaner runs. This mechanism therefore acts more as an emergency option to free up disk space but may result in the deletion of content that is likely to be used (which must then be downloaded again when needed). The cache clean cycle helps to maintain the low profile of the Nomad cache by removing content that is less likely to be used.

Both cache clean cycle and CacheCleaner methods are described in detail in:

Cleaning the cache using the cache clean cycle

Cleaning the cache using CacheCleaner.

9.6.3.3.2 Cleaning the cache using the cache clean cycle

The automated cache clean cycle runs automatically on a regular configurable interval. Nomad was designed to cache content that Configuration Manager has requested or that has been pre-cached using Content Distribution. Because of this the content accumulated in the Nomad Cache can become quite extensive, with a large degree of it no longer relevant or useful. For example, a Windows software update which has been superseded by a newer update is no longer relevant or useful and can be safely removed. The cache clean cycle helps to manage the Nomad cache, remove aged and irrelevant content and minimize its impact on the host machine.

The cache clean cycle is turned off by default, so the registry entries must be set before it will start to regularly clean the cache.

9.6.3.3.2.1 Configuration options

This option is configured by setting the following registry values or installer properties:

Registry Value	Default Value	Installer Property	Description
CacheCleanCycleHrs	0 (turned off)	CACHECLEANCYCLEHRS	The first automatic cache clean runs randomly between 10 to 60 mins of service start up. Subsequent cache clean cycles run after the number of hours specified. 0 means feature turned off. No cache cleaning cycle would run. Changing this registry entry performs an internal restart.

Registry Value	Default Value	Installer Property	Description
			The minimum value is 4. The maximum value is 168 (Once a week)
CacheCleanSubnetLookup	1 (turned on)	CACHECLEANSUBNETLOOKUP	Before deleting content, Nomad checks if it is on any other client in the same subnet, and will only delete local content if the same is present on at least one other client on the same subnet. To disable subnet lookup, set the value to 0. Its value can be 0 or 1. The default value is 1, subnet lookup is enabled. New setting introduced in 8.0.
MaxCacheDays	0 (turned off)	MAXCACHEDAYS	Set to delete application or package content that last triggered Nomad elections before the specified number of days from the date the cache cleaner runs. This ensures that only application or package content that have triggered elections recently will be kept in the cache. 0 means that application and package content will not be deleted automatically when the cache cleaner runs.

Registry Value	Default Value	Installer Property	Description
MaxCacheDaysThreshold	0 (turned off)	MAXCACHEDAYSTHRESHOLD	This is the maximum number of days content is present on a client. If it's not zero, then content will be deleted without any other checks once it reaches the threshold. If the threshold has a value greater than zero and less than 30, Nomad uses the threshold of 30 days and creates an associated log. Default value is 0. New setting introduced in 8.0.
MaxPreCacheDays	0 (turned off)	MAXPRECACHEDAYS	Set to delete pre-cached content that last triggered Nomad elections before the specified number of days from the date the cache cleaner runs. This ensures that only pre-cached content that has triggered elections recently will be kept in the cache. 0 means that pre-cached content will not be deleted automatically when the cache cleaner runs.
MaxSUCacheDays	0 (turned off)	MAXSUCACHEDAYS	Set to delete software updates that last triggered Nomad elections before the specified number of days from the date the cache cleaner runs.

Registry Value	Default Value	Installer Property	Description
			This ensures that only software updates that have triggered elections recently will be kept in the cache. 0 means that software updates will not be deleted automatically when the cache cleaner runs.
DpCacheCleanupEnabled	0 (turned off)	DPCACHECLEANUPENABLED	Deletes all LSZ files in a Distribution Point (DP) cache whose content is no longer distributed, that is not present in ContentLib. To enable DP Cache Cleaner, set the value of registry to 1 (any value except for 0 enables this feature).

9.6.3.3.2.2 Cache clean cycle delete conditions

When the cache clean cycle runs, it will check the type of each content and the last election date associated with it. There are four main types of content, and these will be marked for deletion if the following delete conditions are true:

Content type	Delete condition
Pre-cached	last election date + MaxPreCacheDays > cache clean cycle run date
Application or package	last election date + MaxCacheDays > cache clean cycle run date
Office 365 update byte-range	last election date + MaxSUCacheDays > cache clean cycle run date
Software updates related to SMSTSNomad jobs	

The cache clean cycle will then also check the following, for all content other than Office 365 update byte-ranges:

The content should be present on at least one of the Nomad subnet peers with an equal or a higher percentage of content

The network has broadcasts enabled

If both of these conditions are also true, the content will be deleted.

9.6.3.3.2.3 Caveats

The following points describe various caveats related to the way that the cache clean cycle works:

If pre-cache content is deleted by the cache clean cycle, but the corresponding pre-caching job still exists, Content Distribution will send the download notification again to the client

> **Note**
>
> If your Nomad policy is to not delete pre-caching jobs, you should turn off deletion of pre-cached content by setting the MaxPreCacheDays registry value to 0.

Application upgrades and uninstallation via Software Center require content to be present on the machines (the current version is required for uninstallation and the previous version is required for upgrade scenarios). If the content has been deleted by the cache clean cycle, the content would be downloaded again at uninstall or upgrade time. Because of the way that the cache clean cycle delete conditions are applied Nomad retains one copy of the content per subnet, so even if such a download request comes the content would be downloaded from a Nomad peer and not a DP

ByteRange content is not checked to be present on subnet peers

Cache optimization does not work for content that is to be activated later on

Cache optimization does work on Sensitive Servers.

9.6.3.3.3 Cleaning the cache using CacheCleaner

To maintain the cache Nomad uses a set of basic rules that lets you decide the cache's effect on overall disk usage and performs automatic cleaning when necessary. When a job is advertised, automatic cache cleaning could occur under the following circumstances:

If the percentage of available disk space is less than the PercentAvailableDisk setting after downloading an incoming package, according to its download package size, automatic cache cleaning is initiated before the download takes place

Nomad then assesses how much space could be cleared by deleting cache folders that are eligible for deletion. A cache folder is deemed eligible for deletion if its cache priority value is lower than or equal to the cache priority value of the incoming package. The cache priority value is set on the Nomad command-line using the pc argument, or set in the Nomad properties page when using Configuration Manager. By default, if no value is specified, packages have a cache priority of 1

If the assessment determines there would still not be sufficient space available: no deletion will take place, the download is aborted and an error logged, which may be one of:

Insufficient disk or cache space available to download the Program...

Insufficient cache space available to achieve a Max Cache Size of X

If the assessment determines there would be sufficient space available in the cache: the folders are deleted in order according to their cache priority until the required disk space is available.

9.6.3.3.3.1 Cache cleaner and Configuration Manager

When Nomad is used with Configuration Manager the cache cleaner will also:

Purge linked contents from the Configuration Manager cache

Purge older versions from the Configuration Manager cache before downloading the content for a newer version.

The cache cleaner mechanism also works with the priority job control to ensure that suspended lower priority job caches are not cleaned to make way for the higher priority job unless absolutely necessary.

9.6.3.3.3.2 Command-line switches

CacheCleaner is an executable that can be used to explicitly purge the Nomad cache. By default, the Nomad cache is not purged unless there is an active download. In most cases, available disk space is not really an issue, but there may be circumstances where you may want to manage the cache to keep the disk usage overhead to a minimum. Please refer to Cache management for further information about managing the cache.

It is installed as part of Nomad and the format of the command-line is:

```
CacheCleaner.exe -switch
```

Where *switch* is one of the following (case sensitive):

Switch name	Default value	Range	Description
-CachePriority	1	1-9	Only cache contents with a priority equal to or lower than the *CachePriority* are purged. Used in conjunction with *Pkgsize*to emulate the behavior of the cache cleaner when an actual package is being downloaded.
-Debug			Sets the debug level for *CacheCleaner* and it can be passed on the command-line. If it is not, the value from Nomad registry is used. If Debug is already defined, using this argument adds to the logging level.
-Deleteall			Deletes all cache content where the priority is less than or equal to the value for Force. If the

Switch name	Default value	Range	Description
			command-line does not include *Force*, then *Deleteall* deletes all cache content where the priority is 1. Works in conjunction with the *Force* .

-DeletePkg			The ID of the package or content to be deleted from the cache. The value must be set to the PackageID or ContentID string that identifies the content to be deleted. Must be used in conjunction with *PkgVer* .
			
			`-DeletePkg=PRI0000A -PkgVer=*`
			
			`-DeletePkg=Content_9b9ccd56-9fbf-4587-98e7-725fcfa8e70f -PkgVer=*`

-Force			Content whose cache priority is less than or equal to the *CachePriority* value are purged. Used in conjunction with the *Deleteall* and *MaxCacheAge*.
-MaxCacheAge		1-1461	The maximum number of days before the contents of a cache is purged. If set, *CacheCleaner* deletes cache contents which are older than this value. This argument is ignored if *DeletePkg* and *Deleteall* is used on the command-line. If the command-line includes *Force* , all caches with a priority less than or equal to *CachePriority* will have their content purged. If *CachePriority* is not included on the command-line, all caches with a priority=1 will have their content purged.
-PercentAvailableDisk	10	1-99	Deletes the lowest cache priority content until the set percentage of available disk is available.
-Pkgsize			Only caches with a priority equal to or lower than the *CachePriority* value will have their contents purged. Used in conjunction with *CachePriority* to emulate the behavior of the cache cleaner when an actual package is being downloaded.

Switch name	Default value	Range	Description

			Determine the space to be cleared when running *cachecleaner.exe* with *PercentAvailableDisk* . The *PkgSize* value is by default specified in bytes but can be set to MB by appending MB to the value.
			
			For example, the following are equivalent:
			
			`-Pkgsize=1048576`
			`-Pkgsize=1MB`

-PkgVer			Identifies the content version to be deleted and must be used in conjunction with *DeletePkg* . Deletes content from both the Nomad and Configuration Manager client caches that corresponds to the version number and the Package ID (or Content ID). The special value -PkgVer=* may be used when the user is unsure of the specific version of the package in the cache. **Note** Setting -PkgVer=* will delete any version of the content with the ID specified in the DeletePkg argument from the Nomad cache only – it will not delete from the Configuration Manager client cache. **Note** If you want to remove A*pplication or Software Updates content*, then the -PkgVer will usually need to be set to "1".

Note

If the Nomad cache is deleted while another client is accessing it, the other client will recover by downloading directly from the DP. This is by design and ensures recovery occurs in order to complete a successful download.

9.6.3.3.3.3 CacheCleaner examples

In the following examples, there is no requirement to specify the path to CacheCleaner.exe because the path to Nomad executables is set in the PATH environment variable:

Example	Description
Set the cache cleaner to run as a Configuration Manager program.	You can set the cache cleaner to run as a Configuration Manager program and advertise it to all Nomad systems in a single operation. You can also schedule this as a regular housekeeping job, ensuring that the cache is kept under control automatically. To purge the cache when the total free disk space is at 20% run: `CacheCleaner.exe –PercentAvailableDisk=20`
Ensure that content in the cache is not kept for more than 30 day.	To ensure that content in the cache is not kept for more than 30 days, run: `CacheCleaner.exe –MaxCacheAge=30`
Delete a particular package and version.	To delete a particular package and version, run: `CacheCleaner.exe –DeletePkg=L0A00001 –PkgVer=1`
Purge the contents of a cache with a priority of 3 or lower.	To purge the contents of a cache with a priority of 3 or lower, run: `CacheCleaner.exe –DeleteAll -Force=3`
Purge the contents of a cache with a particular priority and size.	To purge the contents of a cache with a particular priority and size, run: `CacheCleaner.exe –PkgSize=10485760 –CachePriority=6`

9.6.4 Nomad OS Deployment task sequence actions

Nomad support for Configuration Manager OS Deployment.

Nomad task sequence actions are described in greater detail in the following pages.

9.6.4.1 1E Nomad task sequence actions

Please click on a link for more information about a custom task sequence action and its configuration.

9.6.4.1.1 Additional task sequence actions

Below is an additional standard action required by 1E OSD task sequences, that does not exist (yet) out-of-box action when **Nomad OSD Tools** is installed.

9.6.4.1.1.1 Reset Nomad Cache

Ensures the Nomad cache is located on the correct partition. This action is necessary after repartitioning the disk.

You must manually create this step using **Add > General > Run Command Line**.

Parameter	Value
Name	Reset Nomad Cache
Command line	cmd /c md %SMSTSLocalDataDrive%\ProgramData\1E\NomadBranch && cmd /c reg add HKLM\Software\1E\NomadBranch /v LocalCachePath /d %SMSTSLocalDataDrive%\ProgramData\1E\NomadBranch\ /t REG_SZ /f

9.6.4.1.2 Set Nomad as Download Program

Sets *SMSTSNomad.exe* as the download program during a task sequence. This is accomplished by setting the *SMSTSDownLoadProgram* task sequence variable to *SMSTSNomad.exe*.

This custom action is available in the 1E Nomad task sequence actions.

> **Note**
>
> We recommend that this is the first action to be run in the task sequence.

SMSTSNomad.exe supports the use of Configuration Manager's **OSDDownloadContent.exe** directly from a Run Command Line step in a Task Sequence, as well as the previously supported **Download Package Content Native** Configuration Manager Task Sequence Step. No additional configuration is required to make this work. NomadBranch.exe supports SMSTSNomad.exe.

Nomad leverages the Configuration Manager SMSTSDownloadProgram task sequence variable. When this variable is set to the path to an executable, the task sequence engine calls the executable whenever it has to download some content. For this to work effectively, Nomad uses SMSTSNomad.exe.

To avoid the overhead of having to manually set the SMSTSDownloadProgram variable to SMSTSNomad.exe in your task sequence, use the custom task sequence action Set Nomad as Download Program. The following are the content types that are supported by SMSTSNomad.exe:

Packages

OS Images

Boot Images

Applications

Driver packages

Drivers (via Auto apply drivers TS action).

Action	Notes
When run, this task:	This task sequence action:
Sets *SMSTSNomad.exe* as the download program for the duration of the task sequence.	Recommended as the first action to run in the task sequence so that any content required during all the subsequent actions uses Nomad as the download provider.

9.6.4.1.2.1 Configurable parameters

Parameter	Default value	Description
Name	Set Nomad as Download Program.	The name for the custom task sequence action.
Description	Action to set Nomad as Download Program.	The description for the custom task sequence action.
Always return success	Checked.	Checking this option will set Nomad to return a success even when a download fails. This is useful to prevent failing over to BITS.
Allow downloads from cloud distribution points	Not checked.	Checking this option allows Nomad to download content from cloud DPs. Please refer to the notes below about the limitations of this feature.

9.6.4.1.2.2 Allow downloads from cloud distribution points

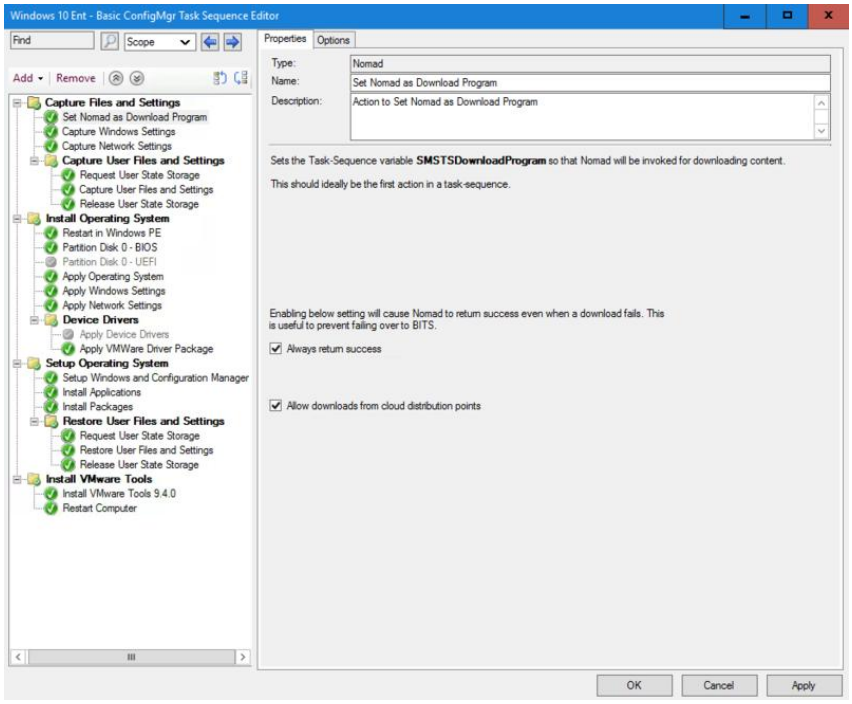
This feature was introduced in Nomad 8.1 to allow them to work around a limitation in Configuration Manager where downloading content from the cloud is not officially supported for third-parties. The feature also works in WinPE.

This feature is not supported on clients older than Nomad 8,1, where the step will fail with error 42. If you have older clients, then you should:

On the **Set Nomad as Download Program** step, enable the option **Continue on Error.** This will allow the step to work as required, except older clients will not download from a cloud DP.

Add a new custom step immediately after, called **Validate Nomad as Download Program**, that runs the following command line, and includes **Success codes 0 3010 42**. This will fail for any other return codes, and ensure any errors reported by Nomad 8.1 clients will stop the Task Sequence as normal.

```
cmd /c exit %_SMSTSLastActionRetCode%
```



9.6.4.1.3 Create Nomad Application Policy

Creates a Nomad application policy and is used in a task sequence during the provisioning phase prior to any applications being installed. It uses the NomadPackageLocator.exe command-line switches tool to enable Nomad to be used as an Alternative Download Provider during provisioning. When the application policy is no longer required it can be removed using the Delete Nomad Application Policy action.

This custom action is available in the **1E Nomad task sequence actions**.

Actions	Notes
When run, this task: Creates the Nomad application policy and enables subsequent application downloads to use Nomad as an alternative download provider.	This task sequence action: Only applies to OSD task sequences and must be run during the Setup Operating Systems phase specifically after the Setup Windows and Configuration Manager action of the task sequence prior to any applications being installed.

9.6.4.1.3.1 Configurable parameters

Parameter	Default value	Description
Name	Create Nomad Application Policy.	Name for the custom task sequence action.
Description	Action to create Nomad Application policy.	Description for the custom task sequence action.

9.6.4.1.4 Delete Nomad Application Policy

Deletes a Nomad application policy previously created using the Create Nomad Application Policy action. It uses the NomadPackageLocator.exe command-line switches tool to remove the previously created Nomad application policy.

This custom action is available in the **1E Nomad task sequence actions**.

Actions	Notes
When run, this task:	This task sequence action:
Deletes the Nomad application policy	Only applies to OSD task sequences and should be run during the Setup Operating System phase of the task sequence after all applications have been installed.

9.6.4.1.4.1 Configurable parameters

Parameter	Default value	Description
Name	Deletes Nomad Application Policy.	Name for the custom task sequence action.
Description	Action to delete Nomad Application policy.	Description for the custom task sequence action.

9.6.4.1.5 Install and Configure Nomad in WinPE

Installs and configures Nomad in WinPE. Typically, to support the use of pre-staged content.

This custom action is available in the **1E Nomad task sequence actions**.

Actions	Notes
When run, this task:	This task sequence action:

Actions	Notes
Creates the Nomad registry values and sets the parameters passed from the task sequence action.	Is specifically for use in WinPE and requires *NomadBranch.exe*, *SMSNomad.exe* and *SNOttfps.dll* to be added to the WinPE image (the *NomadBranchTools.msi* in Configuration Manager does this automatically).
Disables the firewall in the WinPE environment if set in the task sequence action.	Must be set as one of the tasks following Restart in Windows PE and before Apply Operating System.
Self-installs Nomad.	
Configures registry COM.	
Enables multicast if set in the task sequence action.	
Starts the Nomad service.	

9.6.4.1.5.1 Configurable parameters

Parameter	Default value	Description
Name	Install and Configure Nomad in WinPE	Name for the custom task sequence action.
Description	Action to Install and configure Nomad in WinPE	Description for the custom task sequence action.
Workrate	80	Sets the work rate. This is the proportion of available (free) bandwidth to use.
P2P Port	1779	Port used to broadcast election messages.
SpecialNetShare	8224 (0x2020)	Must be an integer. See more SpecialNetShare for more information.

Parameter	Default value	Description
P2PEnabled	9	Must be an integer. See P2PEnabled for more information.
P2P Http port	5080	This option is only available if HTTP P2P has been enabled in P2PEnabled. It defines the port used for Nomad P2P communication over HTTP and must be the same value used on all Nomad clients.
P2P Https port	5443	This option is only available if HTTPS P2P has been enabled in P2PEnabled. It defines the port used for Nomad P2P communication over HTTPS and must be the same value used on all Nomad clients.
Use PKI cert for client auth	Disabled (unchecked)	Enables certificate-based client authentication, which requires a PKI-issued certificate. Selecting this option sets bit 0x2 of P2PSslSettings.
Use PKI cert for server auth	Disabled (unchecked)	Configures Nomad to use a PKI certificate for server authentication when HTTPS P2P is enabled (bit 0x40 set in P2PEnabled). If this option is not checked and bit 0x40 in P2PEnabled is set, Nomad will use a self-signed certificate for server authentication.
Compatibility Flags	0x210000A	Must be an integer. See CompatibilityFlags for more information.
Log file size	10485760 (10MB)	Sets the maximum size for the Nomad log file.
MADCAP scope		MADCAP scope for multicast. Either a scope name, or of the form *<MADCAP_ServerIP>,<MADCAP_Scope_IP>,<TTL>* or *<MADCAP_ServerIP>, <MADCAP_Scope_IP>*. See MultiCastMADCAPScope for more information.
Multicast TTL		Optional multicast time to live. See MultiCastMADCAPScope for more information.
Disable firewall	Enabled by default.	Disables the Windows PE firewall so that NomadPackageLocator and Nomad can communicate with other peers on the local network.

Parameter	Default value	Description
Use FIPS Encryption	Disabled (unchecked)	Sets EncryptionType to 0x1 (FIPS compliant encryption). This must be the same on all Nomad clients.
Enable Single Site Download	Disabled (unchecked)	Enables the SSD feature. For Nomad running in WinPE, sets the SSDEnabled registry value to 0x1 so that SSD is enabled, but the device will be set to just retrieve downloads via SSD and not to put themselves forward to provide content.
Max. machines from 1E Platform	10	The maximum number of devices (i.e. machines) with the content (package, application or software update) that Nomad can retrieve from Content Distribution in one call. The maximum value is 20.
1E Platform Background Channel URL List	""	This is a list of URL containing each of the Tachyon Platform Background Channels in your organization, and is normally the same list as used by your 1E Client devices. Please refer to #UUID4b0c8700283e161c08696047Occ47bc0_id_TachyonclientsettingsBackgroundChannelUrl. **Note** Nomad clients connect to Content Distribution via Tachyon Switches and a proxy feature of Background Channel.

9.6.4.1.5.2 Non-Configurable settings

Setting	Default value	Description
P2PElectionWeight	10	Helps determine the outcome of Nomad elections. The higher the value, the more chances the device has to win the election.
EncryptionType	0	Determines the type of encryption used by Nomad for communications between Nomad peers.
DPNotAvailableCodes	0x205A, 0x205D	This registry entry contains a comma-separated list of return codes, see Nomad return codes for a list of the possible ones. If Nomad encounters one of these during download, it will attempt a retry from an alternative DP. It gets the list of possible DPs from Configuration Manager. The two return

Setting	Default value	Description
		codes set as default are the only ones that are applicable to DP availability: 0x205A – in valid special package path (set using *--pp*) 0x205D – DP path not found Under normal circumstances, you would not change this from the default value. You may want to not allow failover to an alternative DP altogether, in which case you would set the value to " " in the registry. Or you may only want to fail over if the DP path was not found, in which case you would set the value to 0x205D only.

9.6.4.1.6 Save Nomad Cache

Saves the Nomad cache either in WinPE or a full Microsoft Windows operating system. It copies, links or moves previously downloaded content to the protected task sequence runtime folder so that it is not deleted by the standard **Apply Operating System** task sequence action.

> **Note**
>
> When used in WinPE the Install and Configure Nomad in WinPE action must be run first.

This custom action is available in the **1E Nomad task sequence actions**.

Actions	Notes
When run, this task: Locates the Nomad cache on the local drive. Deletes the Configuration Manager cache if the Wipe CCM Cache checkbox is checked in the task sequence action Properties.	This task sequence action: Must be performed after the last Pre-stage Content Using Nomad typically before the Apply Operating System action and, or prior to booting into WinPE if performing an OS refresh. Save Nomad Cache does the following: **Save Nomad Cache** preserves the Nomad log files long with the contents of the Nomad cache. They are restored again after the OS has been deployed when **Restore Nomad Cache** runs. **Save Nomad Cache** also appends a time stamp to the name of the Nomad log files to prevent any possibility of name conflicts during the subsequent **Restore Nomad Cache** step. **Save Nomad Cache** only copies/moves the downloaded content. Specifically it only copies folders that end with the _Cache suffix

Actions	Notes
	that contain the downloaded packages and any associated .LSZ or .LST files. All other content is left behind. This minimizes any chance of name conflicts during the subsequent **Restore Nomad Cache** step. The first time it runs, **Save Nomad Cache** modifies the active Nomad cache location to point into the SMSTaskSequence protected directory. Any subsequent downloads with then go directly into the protected location, removing the need for any further Save Cache Action steps.

9.6.4.1.6.1 Configurable parameters

Parameter	Default value	Description
Name	Save Nomad Cache	The name for the custom task sequence action.
Description	Action to save Nomad cache prior to cleaning the disk	The description for the custom task sequence action.
Operation	Move	May be set to one of Copy, Move and either copies the cache contents to the new location, moves the cache contents to the new location or links the new location to the existing cache location.
Wipe CCM Cache	Enabled by default.	When checked, it sets the action to delete the Configuration Manager cache. **Note** Only works if Configuration Manager is using default locations for the CCM Cache.

Note

The Alternate Cache Path parameter was only required when using redirect, and since redirect is now deprecated the parameter has been withdrawn.

9.6.4.1.7 Restore Nomad Cache

Restores the Nomad cache in the new Operating System during provisioning after the 1E Client has been installed with the Nomad module enabled. This action only needs to be included in the task

sequence if Save Nomad Cache is run prior to applying the new Operating System. Refer to Stage 1E Client Package and Install 1E Client for details on how to install the 1E Client in the task sequence.

This custom action is available in the **1E Nomad task sequence actions**.

Actions	Notes
When run, this task: Reads the Nomad cache location from the registry. Activates all packages in the cache if the **Activate All** Content checkbox is checked in the custom task sequence action properties. By default, this checkbox is unchecked.	This task sequence action: The 1E Client must be installed with the Nomad module enabled prior to executing the **Restore Nomad Cache** action when the **Activate All** option is enabled.

9.6.4.1.7.1 Configurable parameters

Parameter	Default value	Description
Name	Restore Nomad Cache.	Name for the custom task sequence action.
Description	Action to restore Nomad cache post operating system deployment.	Description for the custom task sequence action.
Operation	Link	May be set to one of Copy, Move or Link and either copies, moves or links the *%SMSTSMDataPath%\NomadBranch*location to the existing cache location. **Note** For Link, only a hard link is supported so the Nomad cache and *%_SMSTSMDataPath%* must be in the same file system.
Activate All Content	Disabled by default.	If this option is enabled, Nomad validates all content in the Nomad cache and may take some time to complete. The 1E Client must be installed prior to executing the Restore Nomad Cache step when this option is enabled. Activating the content requires the 1E Nomad Branch service to be running, so when

Parameter	Default value	Description
		this option is selected the step will check every 10 seconds until the service is available. If it does not start within 10 minutes, the step will fail. Without the **-ActivateAll** option selected, Nomad validates content as it's needed, and so speeds up the OSD process. Any non-activated content will not be available to other computers. It's possible to run **NomadBranch.exe -ActivateAll** as a command-line as a separate thread (so the actual OSD task sequence executes as fast as possible).

Note

The Alternate Cache Path parameter is no longer required as Nomad will read the cache location stored in the Nomad registry (and since we recommend applying this step after Nomad has been installed in the new OS, any alternative path to the default will automatically be picked up and used).

9.6.4.1.8 Get Migration Settings

Provides support for optional encryption in Nomad PBA, and Provides computer association details in 1E Application Migration. Used in computer **Replace** and **Refresh** (Wipe and Load destructive and non-destructive) scenarios, it is configured to run under either the capture phase or the restore phase, depending on the scenario.

Note

It is independent of 1E Nomad PBA task sequence actions but is designed to be used in conjunction with them.

This custom action is available in the **1E Nomad task sequence actions**.

	When run, this task: Provides an encryption key to the task sequence action by querying Configuration Manager for a computer association or by generating one itself. Makes the name of the source machine available during a restore by relying on its name stored in the computer association. The end result of successful execution is the following three variables are set: OSDStateEncryptDecryptKey PBAComputerName
Actions	SourceComputerName
Context	Get Migration Settings integrates with Nomad Peer BackUp Assistant (PBA), providing a cryptographic key that can be used to secure captured user data stored on a PBA host. For WSA type deployments, it is also possible for user data to be encrypted and stored onto USB media, if PBA is not available. Step behaviour will depend on user requirements and deployment scenario. Before describing the operation of Get Migration Settings fully, a brief explanation of the different deployment scenarios in which the step operates is provided. *Replace Scenarios* This is where the user is being migrated to new or replacement hardware. A computer association in ConfigMgr is a native object that defines the logical relationship between the old and new computer. When the computer association is created in the site, an encryption key is automatically created and stored in the site database. In this scenario, the step will attempt to identify the appropriate computer association in order to obtain the key. For non-WSA type deployments, the presence of a valid computer association is mandatory and the step will fail if it is not found. WSA deployments also allow users to enter the name of the new computer at the time the Assistant runs, forgoing the need for the pre-provisioned computer association. *Wipe and Load* A Wipe and Load can be destructive (disk reformat and data loss) and non-destructive (file level wipe of the disk where areas of the file system can be preserved). Wipe and Load non-destructive user state capture utilizes file system hard links and therefore does not require external storage or data encryption.

	When run, this task: Provides an encryption key to the task sequence action by querying Configuration Manager for a computer association or by generating one itself. Makes the name of the source machine available during a restore by relying on its name stored in the computer association. The end result of successful execution is the following three variables are set: OSDStateEncryptDecryptKey PBAComputerName
Actions	SourceComputerName

Wipe and Load destructive requires user data is saved off onto another device (Nomad PBA) or external device before reformat of the disk (USB media can be used as an alternative to Nomad PBA when using WSA). For this scenario, a ConfigMgr Computer Association is not used. Get Migration Settings will itself generate a unique encryption key based upon the ConfigMgr client identifier and AES 256 hashing algorithm. The key is stored in the task sequence environment for access during capture and restore in the native variable **OSDStateEncryptDecryptKey.**

Operation

Get Migration Settings is designed to support both the **Replace** and **Refresh** (Wipe and Load) deployment scenarios. The step's behaviour is different depending on deployment scenario. The step, by default will assume a **Replace** scenario. In order to operate for **Refresh** (Wipe and Load), the task sequence variable **DEPLOYMENTTYPE = REFRESH**, must be set prior to executing the step.

As well as provisioning the USMT encryption key, the step is also responsible for instantiating TS variables **SourceComputerName** and **PBAComputerName**. During the restore process, the source machine name is used to identify the location of captured user data if using Nomad PBA (PBAComputerName) as well as resolving the list of applications to install as defined by 1E Application Migration (SourceComputerName).

By default, the step will attempt to provide a key for encryption of captured user data.

> **Note**
>
> The method of generating an encryption key depends on the deployment scenario, summarized in the following table.

When run, this task:

Provides an encryption key to the task sequence action by querying Configuration Manager for a computer association or by generating one itself.

Makes the name of the source machine available during a restore by relying on its name stored in the computer association.

The end result of successful execution is the following three variables are set:

OSDStateEncryptDecryptKey

PBAComputerName

Actions SourceComputerName

Customers that do not wish to use a **ConfigMgr Computer Association** in key provisioning have the option of using **Get Migration Settings** to generate the key instead.

Customers that do not require encryption are able to disable key provisioning by setting the TS variable **1EDisableUSMTEncryption = True** prior to running the step. In this case, the step's only function is in providing the source machine name for 1E Application Migration.

OS Deployment type	ConfigMgr Computer Association	Get Migration Settings
Replace Capture/Restore	✔	
WSA-Replace Capture/Restore	✔	✔
Wipe and Load Non-Destructive	n/a	
Wipe and Load Destructive		✔
WSA-Wipe and Load Destructive		✔

All WSA type deployments require Nomad 6.3.200 and above.

Task sequence position

When run, this task:

Provides an encryption key to the task sequence action by querying Configuration Manager for a computer association or by generating one itself.

Makes the name of the source machine available during a restore by relying on its name stored in the computer association.

The end result of successful execution is the following three variables are set:

OSDStateEncryptDecryptKey

PBAComputerName

Actions SourceComputerName

The table below indicates the use of the step for different deployment scenarios. The Get Migration Settings step can operate in one of 2 modes: **Capture** and **Restore**. Mode is set in the step UI.

In **Capture** mode, the step is inserted prior to the **Capture User Files and Settings** step, and will typically reside in the **Capture User Files and Settings** group. This is used for **Replace Capture** and **Wipe and Load** task sequences.

In **Restore** mode, the step is inserted prior to the **Restore User Files and Settings** step, and will typically reside in the **Restore User Files and Settings** group. This is only used for a **Replace Restore** type task sequence. It is not required for **Wipe and Load** task sequences.

For**Wipe and Load Non-Destructive** task sequences, the step does not provision an encryption key as file system hard-links are used negating any requirement for secure storage, in this case the step will only set the **SourceComputerName** variable for use in 1E Application Migration.

OS Deployment type (WSA and Non-WSA)	**Get Migration Settings**	
Replace Capture/Restore	✔	✔
Wipe and Load Destructive (Refresh OS)	✔	
Wipe and Load Non-Destructive (Refresh OS)	✔ (No encryption	

	When run, this task: Provides an encryption key to the task sequence action by querying Configuration Manager for a computer association or by generating one itself. Makes the name of the source machine available during a restore by relying on its name stored in the computer association. The end result of successful execution is the following three variables are set: OSDStateEncryptDecryptKey PBAComputerName	
Actions	SourceComputerName	
		key provisioned)
	In-place Upgrade	n/a

Key recovery

If you need to recover the key generated by the step (perhaps your Wipe and Load Destructive or Replace Restore TS failed before restoring the user data) you can do so using the command line tool **1eUsmtKeyGen.exe.** This tool is part of Installing Nomad Branch Tools and is installed at location <ProgramFiles>\Microsoft Configuration Manager\AdminConsole\bin\NomadBranchAdminUIExt. It can be called via the Windows Console as shown below:

It takes the Configuration Manager client guid of the source machine as an argument and generates the exact key that would have been generated during the TS. To know the Configuration Manager client guid of any computer, please consult the 'SMS_Unique_Identifier0' column in the view 'dbo.v_R_System' of the config manager database.

While entering the argument, please remember that:

If the client guid contains the prefix "GUID:" it MUST be included (see above screenshot).

The case of the argument does not matter; two arguments differing only in case result in the same key being generated.

When run, this task:

Provides an encryption key to the task sequence action by querying Configuration Manager for a computer association or by generating one itself.

Makes the name of the source machine available during a restore by relying on its name stored in the computer association.

The end result of successful execution is the following three variables are set:

OSDStateEncryptDecryptKey

PBAComputerName

Actions

SourceComputerName

It should be the client guid of the source computer, i.e. the machine from where the user state is being migrated, not that of the destination computer where the state is being migrated to.

The generated key will be printed in base64 format on the Windows Console. You can copy it and use it as is with the usmt "/key" option to recover the user data.

Associated variables

Variable	Description
OSDStateEncryptDecryptKey	Native variable that hosts the key used to secure captured user data.
PBAComputerName	Name of the computer on which user data was captured.
SourceComputerName	Name of the computer for which the Application Migration list is obtained. Usually the same as PBAComputer.
1EDisableUSMTEncryption	If true, then an encryption key is not provisioned.
DeploymentType	If set to Refresh, then an encryption key is not provisioned.

	When run, this task: Provides an encryption key to the task sequence action by querying Configuration Manager for a computer association or by generating one itself. Makes the name of the source machine available during a restore by relying on its name stored in the computer association. The end result of successful execution is the following three variables are set: OSDStateEncryptDecryptKey PBAComputerName SourceComputerName		
Actions			
Configurable parameters	Parameter	Default value	Description
	Name	Get Migration Settings.	Name for the custom task sequence action.
	Description	Action to get encryption key for user state and name of the source computer if needed.	Description for the custom task sequence action.
	Capture user state		Used during the state capture phase.
	Restore user state		Used during the state restore phase.
Notes	Get Migration Settings contacts Content Distribution via the proxy feature of the Tachyon Background Channel. It gets the URL for the Background Channel from the Nomad registry PlatformURL setting, which is configured automatically by Nomad on startup by querying the value that the Tachyon client is using (stored in the **1E.Client.conf** file).		

9.6.4.1.9 Stage 1E Client Package

Downloads the 1E Client package ready for installation by the Install 1E Client Task Sequence step. It's typically executed in Windows PE and must be included before the Install 1E Client step in the task sequence.

This custom action is available in the **1E Nomad task sequence actions**.

Actions	Notes
When run, this task: Downloads the 1E Client package and sets the path in the task sequence *NomadInstallPath* variable.	This task sequence action must: Only be run in the provisioning phase just before Setup Windows and ConfigMgr task sequences Refer to a Nomad package containing a single .msi (1E.Client-x64.msi/1E.Client-x86.msi), which is run on the client, the package can also contain a single Windows Installer Transform (.mst file) and a single Windows Installer Patch (.msp file) that will be applied when the Install 1E Client step is executed.

9.6.4.1.9.1 Configurable parameters

Parameter	Default value	Description
Name	Stage 1E Client Package	Name for the custom task sequence step
Description	Action to stage the 1E Client package for installation in the new OS.	Description for the custom task sequence step.
1E Client Package	n\a	Name of the 1E Client package.

9.6.4.1.10 Install 1E Client

Installs the 1E Client. The Stage 1E Client Package step must be to be included before this step in the Task Sequence. The 1E Client installer and any Transform or Patch that should be applied during installation must be included in the 1E Client Package referenced in the Stage 1E Client Package step.

> **Note**
>
> You must include a **Restart Computer** step after the **Install 1E Client** step. This is because the client installation adds the Nomad binaries folder to the system path, but because the Task Sequence (running as system) is already running it must be restarted to pick up the system path change. Subsequent steps in the Task Sequence that use Nomad will fail if this reboot is not included.

This custom action is available in the **1E Nomad task sequence actions**.

Actions	Notes
When run, this task: Reads the *NomadinstallPath* task sequence variable (Set by the Stage 1E Client Package action) for the location of the installer and installs the 1E Client If an *.mst* file is found in the root of the package, it adds the transform automatically with the installation. If multiple *.mst* files are present in the root of the package, the TRANSFORMS installer property referencing the *.mst* file must be added in the command-line otherwise this step fails If an .msp file (patch) is found in the root of the package, it will be applied during installation of the 1E Client.	This task sequence action: Waits for the 1E Nomad Branch service to start. It checks every 15 seconds until a configurable timeout expires (default 10 mins). Once the Nomad service is found running, the step completes successfully. If the timeout is reached without the Nomad service running, the step fails. There are two TS variables to manage this behavior: **EnableNomadStartUpChecks** - Default is true. If set to false then the step does not wait for the Nomad service to come up after 1E Client installation. This should only be set to false when the **Install 1E Client** action is not enable the Nomad client module. **NomadStartUpChecksTimeout** - Default is 10. Defines the number of minutes the step will wait for the Nomad service to start. If you notice the Nomad service taking longer than 10 minutes to be fully up and running in your environment, you can increase this value. The accepted ranges of this variable, is 10 to 60. If the specified value is not in range, it's set to a default 10 minutes. **Note** From Nomad 7.0.200, the **Install 1E Client** action supports installing a 1E Client patch. To do this: Include the patch in the 1E Client package referenced in the Stage 1E Client Package Step Ensure there's only one MSP file, the latest cumulative 1E Client hotfix, included in the package source If there's an MSP present in the package when the Install 1E Client setup runs, it will be installed. To implement these changes, you must include the hotfix MSP in the 1E Client

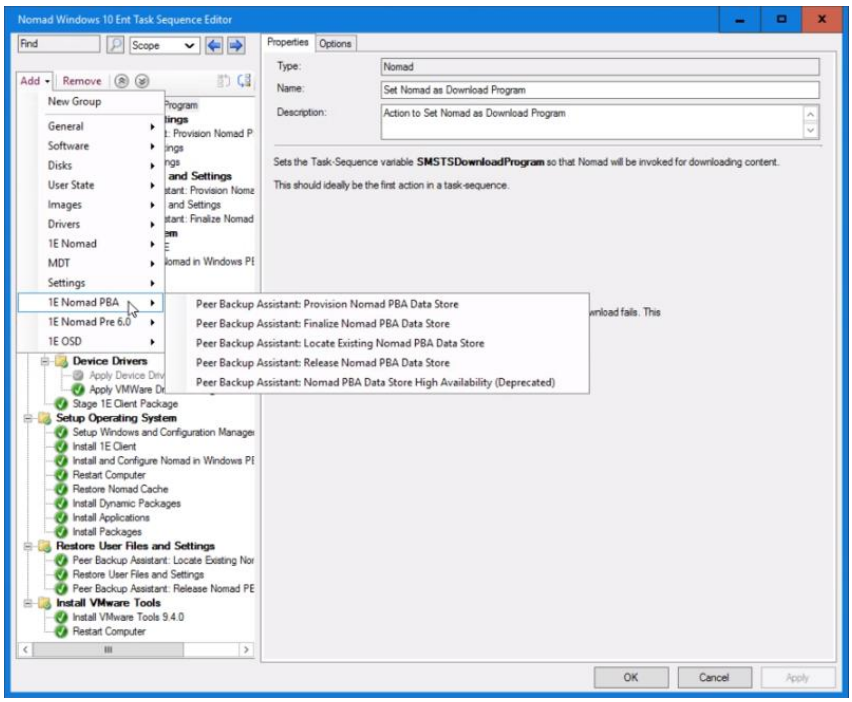
Actions	Notes
	package referenced in the Stage 1E Client Package step in your Task Sequences.

9.6.4.1.10.1 Configurable parameters

Parameter	Default value	Description
Name	Install 1E Client	Name for the custom task sequence step.
Description	Action to install 1E Client in the new OS.	Description of the custom task sequence step.
Additional installation commands		Additional installation parameters.

9.6.4.2 1E Nomad PBA task sequence actions

Please click on a link for more information about a custom task sequence action and its configuration.



9.6.4.2.1 Peer Backup Assistant: Provision Nomad PBA Data Store

Provisions a PBA data store prior to saving user state using USMT. It is the first step of the Peer backup assistance sequence (**USMT Capture User State** follows).

Note

PBA supports the use of multiple backup data stores, for more details see High-Availability Peer Backup Assistant. If the task sequence variable form of the Cache space parameter is used (see below) then the variable referenced must be set before running this action.

This custom action is available in the **1E Nomad PBA task sequence actions**.

Actions	Notes
This task: Polls Nomad peers enabled for PBA to find one with a data store where the user state may be saved. The peer that responds with the largest percentage of available disk is selected. Sets the following task sequence variables for subsequent actions: *PBAComputerName*: a label used to refer to the cache in following Nomad actions *PBAHostComputerName*: Host name of the data store machine. *OSDStateStorePath*: tells USMT where to save user state to then retrieve it from, i.e. the location of the Nomad cache *NMDS_REMOTE*: set to the same value as *OSDStateStorePath*. This is not required, but it is available for backwards compatibility.	This task sequence action: Is the first action in the saving phase of user state migration Must be followed by **USMT Capture User State** action **Note** If the task sequence variable *1EWSA_USMTSizeInMB* is set, the step will use its assigned value when polling.

9.6.4.2.1.1 Configurable parameters

Parameter	Default value	Description
Name	Peer Backup Assistant: Provision Nomad PBA Data Store	Name for the custom task sequence action.
Description	Action to find a PBA data store for saving user state	Description for the custom task sequence action.

Parameter	Default value	Description
Use Nomad's size estimation	Disabled by default.	If enabled, the estimation is passed to NMDS_POLL.
Static cache space	100	Estimated cache space in MB required to store the user state. This can either be a number, the default being 100, or the name of a task sequence variable holding the value delimited by '%', e.g. " *%USMTEstimate%*.

9.6.4.2.2 Peer Backup Assistant: Finalize Nomad PBA Data Store

Closes the connection to the PBA data store after user state is saved with **USMT Capture User State**.

> **Note**
>
> This step replaces the Peer Backup Assistant: Close Nomad PBA Data Store (deprecated) and the Peer Backup Assistant: High Availability (deprecated) steps. You can continue using the deprecated steps if you have already deployed them, but you cannot modify them. Going forward, we recommend you migrate to this new task sequence step.

This custom action is available in the **1E Nomad PBA task sequence actions** .

Actions	When run, this task: Closes the connection to the PBA data store after the user state is saved with **USMT Capture User State**. Optionally, stores user state data locally if there is enough disk space.
Context	This task sequence action: Must be run after the **Provision Nomad PBA Data Store** and **USMT Capture User State** actions.
Associated variables	n/a

Configurable parameters

Parameter	Default value	Description
Name	Peer Backup Assistant: Finalize	Name for the custom task sequence action.

When run, this task:

Closes the connection to the PBA data store after the user state is saved with **USMT Capture User State**.

Actions	Optionally, stores user state data locally if there is enough disk space.		
	Nomad PBA Data Store		
	Description	Action to close the connection to the Nomad PBA data store after saving the user state.	Description for the custom task sequence action.
	Enable HA	False	Enable high availability. **Note** If the task sequence variable 1EDisablePBA_HA = True, then High Availability is disabled. This variable is automatically set for Remote WSA deployments.
	Minimum	1	The minimum number of PBA data store backups. The number of data stores must be available when PBA-HA starts the backup, else if fails. Must be between 1 and 6 Must be equal to or greater than the Synchronous value.
	Maximum	1	The maximum number of PBA data store backups. Must be between 1 and 6.
	Synchronous	1	The number of successful backups to create before moving on to the next task sequence action.

	When run, this task: Closes the connection to the PBA data store after the user state is saved with **USMT Capture User State**.
Actions	Optionally, stores user state data locally if there is enough disk space.
	Must be between 1 and the value in Maximum. You can set the value to 0, but we do not recommend it as it causes the next task sequence to execute immediately with no guarantee of a successful backup.

9.6.4.2.3 Peer Backup Assistant: Locate Existing Nomad PBA Data Store

Finds saved user data, prior to restoring user state using the **USMT Restore User State** action.

> **Note**
>
> The Peer Backup Assistant: Close Nomad PBS Data Store and (usually) OS refresh or OS install on bare-metal actions must be run first. If saving user data was run as a separate task, insert an action in the current task sequence that sets the *PBAComputerName* TS variable to the same value that is set in the saving task sequence. This identifies the Nomad cache in the network where the user data is saved.

This custom action is available in the **1E Nomad PBA task sequence actions** .

Actions	Notes
When run, this task: Finds the PBA enabled Nomad peer on which the user state migration data has been cached. Sets these task sequence variables for subsequent steps: *OSDStateStorePath*: Tells USMT where to restore user state from, i.e. the location of the Nomad cache. *NMDS_REMOTE*: Set to the same value as *OSDStateStorePath*. This is not required, but it is available for backwards compatibility.	This task sequence action: The first action in the restoring phase of user state migration.

9.6.4.2.3.1 Configurable parameters

Parameter	Default value	Description
Name	Peer Backup Assistant: Locate Existing Nomad PBA Data Store.	Name for the custom task sequence action.
Description	Action to locate cached data prior to restoring user state.	Description for the custom task sequence action.

9.6.4.2.4 Peer Backup Assistant: Release Nomad PBA Data Store

Releases saved user data in the Nomad cache, after restoring user state with **USMT Restore User State**.

> **Note**
>
> The **USMT Restore User State** action must have been run successfully.

This custom action is available in the **1E Nomad PBA task sequence actions** .

Actions	Tasks
When run, this task: Deletes the cached user state data from the PBA enabled Nomad peer. Sets the following task sequence variables for subsequent actions: *PBAComputerName*: A label used to refer to the cache in following Nomad actions.	This task sequence action: Is the final action in the restoring phase of user state migration Is not essential because the cache is deleted by Nomad automatically after 7 days (default configuration).

9.6.4.2.4.1 Configurable parameters

Parameter	Default value	Description
Name	Peer Backup Assistant: Release Nomad PBA Data Store.	Name for the custom task sequence action.
Description	Action to release the Nomad PBA data store after restoring user state.	Description for the custom task sequence action.

9.6.4.2.5 Peer Backup Assistant: Close Nomad PBA Data Store (deprecated)

> **Note**

> This step has been replaced by Peer Backup Assistant: Finalize Nomad PBA Data Store. Existing deployments will still work, but you cannot modify them. Going forward, we recommend using its replacement.

This step closes the connection after user state is saved by **USMT Capture User State**. ThePeer Backup Assistant: Provision Nomad PBA Data Store and **USMT Capture User State** actions must have been run.

Actions	Notes
When run, this task: Sends a completion message to the Nomad peer to indicate that the user state migration data has been cached. Sets the following task sequence variables for subsequent actions: *PBAComputerName*: A label used to refer to the cache in following Nomad actions.	This task sequence action: Is the final action in the saving phase of user state migration.

9.6.4.2.5.1 Configurable parameters

Parameter	Default value	Description
Name	Peer Backup Assistant: Close Nomad PBA Data Store.	Name for the custom task sequence action.
Description	Action to close the PBA data store connection after saving user state.	Description for the custom task sequence action.

9.6.4.2.6 Peer Backup Assistant: High Availability (deprecated)

> **Note**
>
> This step is deprecated, and you should use the Peer Backup Assistant: Finalize Nomad PBA Data Store instead. Existing deployments will still work, but you cannot modify them. Going forward, we recommend using its replacement.

This step stores additional backup copies of the PBA data store, after the primary data store has been created with Peer Backup Assistant: Provision Nomad PBA Data Store and after the USMT data has been saved andc losed with Peer Backup Assistant: Close Nomad PBA Data Store (deprecated).

The following actions must have been run successfully:

Peer Backup Assistant: Provision Nomad PBA Data Store

USMT Save User State

Peer Backup Assistant: Close Nomad PBA Data Store (deprecated).

This custom action is available in the **1E Nomad PBA task sequence actions** .

Actions	Notes
When run, this task: Polls Nomad peers enabled for PBA to find the required number of data stores where the user state may be saved. Backs up the primary data store on each Nomad peer after locating the PBA data stores.	This task sequence: Must have the minimum and maximum number of PBA data stored to create defined Must have the number of synchronous backups that must be completed successfully defined before continuing with the next action in the task sequence. The remainder of the additional backups are performed asynchronously while the other task sequence actions are running.

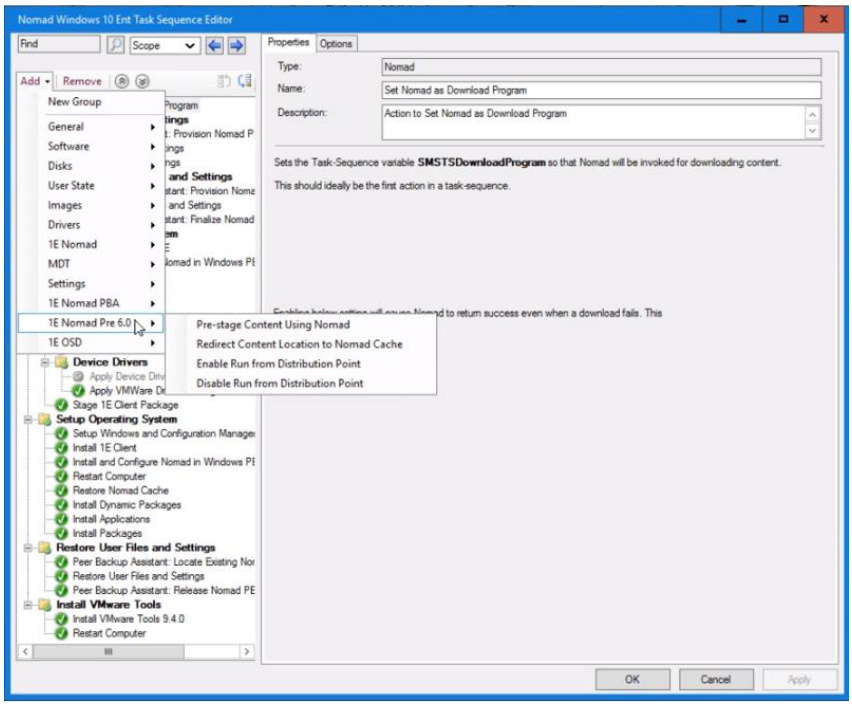
9.6.4.2.6.1 Configurable parameters

Parameter	Default value	Description
Name	Peer Backup Assistant: High Availability.	Name for the custom task sequence step.
Description	Action to find additional PBA data stores for saving user state.	Description for the custom task sequence action.
Minimum	1	The minimum number of PBA data store backups. Must be at least 1 and not greater than 6. The specified number (minimum) of data stores must be available when PBA-HA starts backing up the data. If the minimum number of data stores will not respond, then the PBA-HA task sequence step will fail. **Note** The minimum should be greater than or equal to the Synchronous value. If the minimum number is less than the Synchronous value, the task sequence may fail even though the minimum number of backups have been done.

Parameter	Default value	Description
Maximum	1	The maximum number of PBA data store backups. Must be at least equal to the minimum and not greater than 6.
Synchronous	1	The number of backups that must be performed successfully before moving onto the next action in the task sequence. Must be 0 or more and not greater than the value set for the maximum. **Note** It is possible, but not recommended, to set this value to 0. If this is done, the next action in the task sequence will start immediately, but there will be no guarantee that any backups have been successful.

9.6.4.3 1E Nomad Pre 6.0 task sequence actions

Please click on a link for more information about a custom task sequence action and its configuration.



9.6.4.3.1 Pre-stage Content Using Nomad

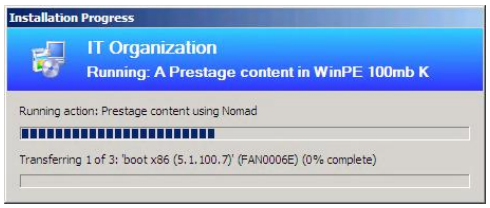
Pre-stages content using Nomad, either in WinPE or a full Microsoft Windows operating system. It uses the NomadPackageLocator tool to locate any locally available copies of content, as set in the

References in the custom task sequence action properties. If no local copies are available, it will download the content from the DP and store it locally. It then configures the Task Sequence to use this locally stored content.

We recommend, when using the **Pre-stage Content Using Nomad** step, that the content is downloaded to the local branch and the task sequence is pointed to the Nomad cache that contains it. When using Redirect Content Location to the Nomad Cache (deprecated) this is a requirement as it cannot make use of all the Nomad download functionality.

Use **Pre-Stage content Using Nomad** in preference to **Redirect Content Location to the Nomad Cache (deprecated)** to make use of all the Nomad features. Use the **Redirect Content Location to the Nomad Cache (deprecated)** if you want to have exactly the same *NomadPackageLocator* functionality provided in earlier releases of Nomad.

While **Pre-stage content Using Nomad** is running, a progress bar is displayed on the Installation Progress dialog on the target machine:



Note

When used in WinPE, the Install and Configure Nomad in WinPE action must be run first.

This custom action is available in the **1E Nomad Pre 6.0 task sequence actions**.

Actions	Notes
When run, this task: Uses NomadPackageLocator.exe command-line switches to locate locally available copies of the content, as set in References in the custom task sequence action properties. If no local copies are available, it will download the content from the DP and store it locally. Updates the task sequence to use the locally downloaded content. If the Require Nomad checkbox is checked in the action properties, fail the task sequence step if the *NomadPackageLocator* download fails. If the Show error checkbox is checked in the action properties, display the error dialog if the *NomadPackageLocator* download fails.	The following points should be taken into account when using this task sequence action: Prior to using any of the content downloaded using the Pre-stage content Using Nomad task sequence action, you must run the Save Nomad Cache task sequence action.

Actions	Notes
If the Use Multicast checkbox is checked in the action properties, *NomadPackageLocator* will invoke *NomadBranch* with multicast enabled. If the All references checkbox is checked in the action properties, all referenced content will be selected.	

9.6.4.3.1.1 Configurable parameters

Parameter	Default value	Description
Name	Pre-stage Content Using Nomad.	The name for the custom task sequence action.
Description	Action to pre-stage content in WinPE using Nomad.	Sets the description for the custom task sequence action.
Require Nomad	Enabled by default.	When this checkbox is checked, it sets a requirement for another Nomad client on the same subnet to have the content, if this is not the case the task sequence step will fail. When this checkbox is not checked the task sequence will attempt to continue without using Nomad if there is no Nomad client on the same subnet with the content.
Show error dialog	Disabled by default.	When this checkbox is checked, an error dialog is displayed to the Configuration Manager administrator when the *NomadPackageLocator* download fails.
Use HTTP	Enabled by default.	When this checkbox is checked, *NomadPackageLocator* uses the HTTP location for the content if it is not available locally. **Note** In Configuration Manager 2012, if this option is not enabled when using this task sequence step, all selected packages must be copied to the SMB share on the DP using the Data Access > Copy the content in this package to a package share on distribution points option in the properties of each package, otherwise the download fails.

Parameter	Default value	Description
Use Multicast	Disabled by default.	When this checkbox is checked, *NomadPackageLocator* invokes *NomadBranch* with multicast enabled.
All references	Disabled by default.	When this checkbox is checked, all referenced content is selected (and any added subsequently to the task sequence will be automatically selected). When it is unchecked, all referenced content is deselected.
References	This field is pre-filled with all content set for downloading in the task sequence.	This field is pre-filled with all content set for downloading in the task sequence. Checking the checkbox next to each item will set the use of *NomadPackageLocator* for that content. **Note** There is a limit of 255 characters on a task sequence action's command line. If this was exceeded because there are many selected references, a popup dialogue will appear saying so when the Apply or OK button is pressed. Either reduce the number of references by creating more, separate, task sequences to pre-stage content, or select the **All references** checkbox which will use a wildcard for the references.

9.6.4.3.2 Redirect Content Location to the Nomad Cache (deprecated)

Note

This action is deprecated and is currently provided for backwards compatibility only, Use **Pre-stage Content Using Nomad** instead.

This custom task sequence action redirects the task sequence's content location to the Nomad cache on another host. Used in either WinPE or a full Microsoft Windows Operating System, it used the Nomad NomadPackageLocatortool to locate the content on a Nomad cache on the local subnet.

The *NomadPackageLocator* program sends out a Nomad package status request for each of the packages listed in the OSD task sequence it is running within. If any of the content is available on other Nomad clients on the local subnet, it updates the path variables in the task sequence to point at the folder location (usually located in the local or remote Nomad cache folder). If not, the default path (i.e. the path to the distribution point) is left intact.

Both the Redirect Content Location to Nomad Cache and Pre-stage Content Using Nomad rely on the fact that the content has been downloaded to the local branch and point the task sequence to the Nomad cache that

contains the content. Use Pre-stage Content Using Nomad in preference to Redirect Content Location to Nomad Cache to make use of all the Nomad features. Use the Redirect Content Location to Nomad Cache if you require exactly the same *NomadPackageLocator* functionality provided in earlier releases of Nomad.

Note

When used in WinPE, the Install and Configure Nomad in WinPE action must be run first.

This custom action is available in the **1E Nomad Pre 6.0 task sequence actions**.

Actions	Notes
When run, this task: Locates the Nomad cache on the local subnet. Updates the task sequence to use local subnet content. If the Require nomad checkbox is checked in the action properties, fail the task sequence step if the *NomadPackageLocator* download fails. If the Show error dialog is checked in the action properties, display the error dialog if the *NomadPackageLocator* download fails. If the All references checkbox is checked in the action properties, all referenced content will be selected.	This task sequence action: Is typically performed prior to the apply operating system action but may be used multiple times throughout the task sequence, particularly during the provisioning phase.

9.6.4.3.2.1 Configurable parameters

Parameter	Default value	Description
Name	Redirect Content Location to Nomad Cache.	Name for the custom task sequence action.
Description	Action to redirect content location to Nomad cache.	Description for the custom task sequence action.
Require Nomad	Enabled by default.	When this checkbox is checked, the task sequence action fails if the *NomadPackageLocator* download fails. If this is not checked, the task sequence attempts to download the

Parameter	Default value	Description
		content by other means if the *NomadPackageLocator* download fails.
Failover to DP(s)	Disabled by default.	When this option is checked, the content download can failover to downloading from the DPs if the *NomadPackageLocator* fails to find the content cached on the local subnet.
Show error dialog	Disabled by default.	When this checkbox is checked, an error dialog is to the Configuration Manager administrator if the *NomadPackageLocator* download fails.
Force Nomad client	Blank by default.	Set the name for a specific Nomad client whose cache you want to use. This prevents *NomadPackageLocator* from polling for a Nomad client whose cache contains the content.
Nomad share name	Blank by default.	Should only be used if the Nomad clients where OSD content has been pre-cached are configured with the Hidden Nomad share option set to 0x10. See SpecialNetShare for more information. When the pre-cache Nomad client is set to use the hidden share, set the value to *NomadSHR$*.
Multicast scope		Should only be set if you want the *NomadPackageLocator* requests to span subnets when trying to locate a package. In this instance, the request is will be multicast and the scope must be set here. **Note** This will only work if the network has been configured to allow multicast across subnets.
All references	Disabled by default.	When this checkbox is checked, all referenced content will be selected (and any added subsequently to the task sequence will be automatically selected too). When it is unchecked, all referenced content will be deselected.
References	Pre-filled with all content set for	Pre-filled with all content set for downloading in the task sequence. Checking the checkbox next to each item will set the use of *NomadPackageLocator* for that content.

Parameter	Default value	Description
	downloading in the Task Sequence.	**Note** There is a limit of 255 characters on a task sequence action's command line. If this was exceeded because there are many selected references, a popup dialogue will appear saying so when the Apply or OK button is pressed. Either reduce the number of references by creating more, separate, task sequences to redirect content, or select the All references checkbox which will use a wildcard for the references.

9.6.4.3.3 Enable Run from Distribution Point

Used in the following instances:

In conjunction with the pre-stage content using Nomad action to avoid making a local copy of the Nomad share.

It is used during the provisioning phase, prior to any package being installed, to enable classic packages to run from the DP. This is so that *SMSNomad.exe* can be used as an alternative download provider during OSD.

When the **Run from distribution point** property is no longer required, remove it using the Disable Run from Distribution Point custom task sequence.

This custom action is available in the **1E Nomad Pre 6.0 task sequence actions**.

Actions	Notes
When run, this task:	This task sequence action:
Sets the task sequence to run from the DP.	Only applies to OSD task sequences and should be run prior to installing classic packages using the SMSNomad.exe command Can be run anywhere in the task sequence after the Restart in Windows PE action, that would be used as part of a Refresh OS Deployment task sequence Must have the Copy the content in this package to a package share on distribution points option enabled for classic packages that are set to Run from the DP.

9.6.4.3.3.1 Configurable parameters

Parameter	Default value	Description
Name	Enable Run from DP.	The name for the custom task sequence step.
Description	Action to Enable Run from the DP.	The description for the custom task sequence action.

9.6.4.3.4 Disable Run from Distribution Point

Reverts the task sequence variables that were set using the Enable Run from Distribution Point custom task sequence action back to their default values.

This custom action is available in the **1E Nomad Pre 6.0 task sequence actions**.

Actions	Notes
When run, this task:	This task sequence action:
Sets the task sequence to download on-demand.	Only applies to OSD task sequences after installing all classic packages using the *SMSNomad.exe* command and only if the Enable Run from Distribution Point had previously been run.

9.6.4.3.4.1 Configurable Parameters

Parameter	Default value	Description
Name	Disable Run from the DP.	The name for the custom task sequence step.
Description	Action to Disable Run from Distribution Point.	Description for the custom task sequence step.

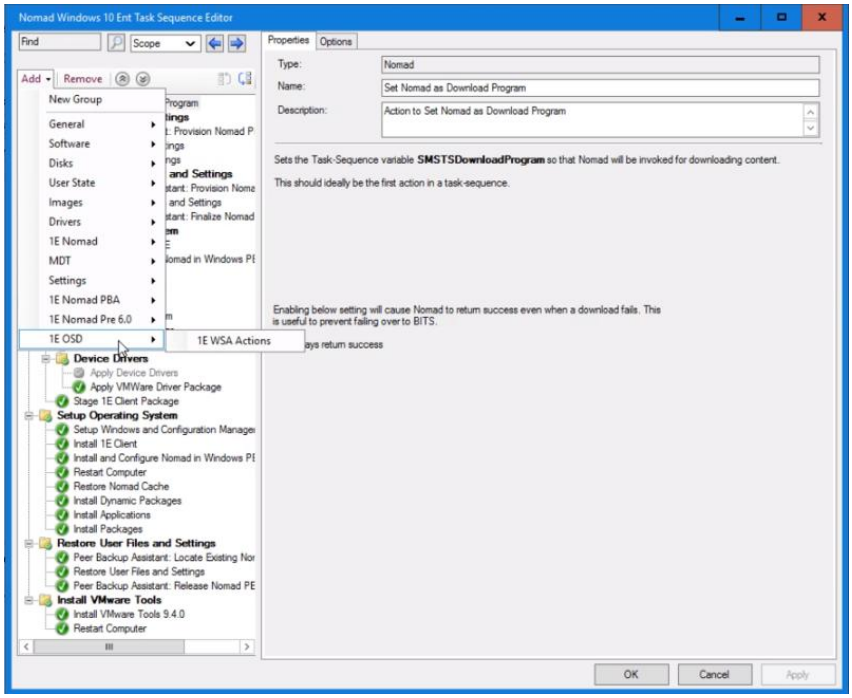
9.6.4.41E OSD task sequence actions

Depending on the 1E OSD Tools that you have installed, you may also see custom task sequence actions for:

BIOS TO UEFI 1.4 - 1E OSD task sequence actions

1E task sequence actions.

Please click on a link below for more information about a custom task sequence action and its configuration.



9.6.4.4.1 1E WSA Actions

The 1E WSA Actions action is an essential component of the WSA deployment task sequence. Its position and configuration within the task sequence is critical to ensuring the task sequence completes successfully. The action performs one or more of the following functions depending on the selection made when configuring the step:

Initialize

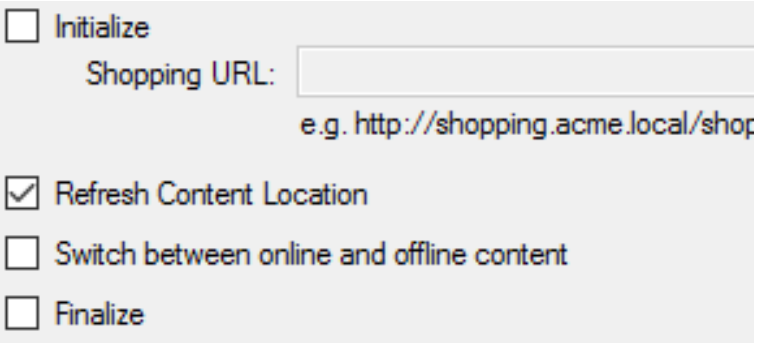
Refresh Content Location

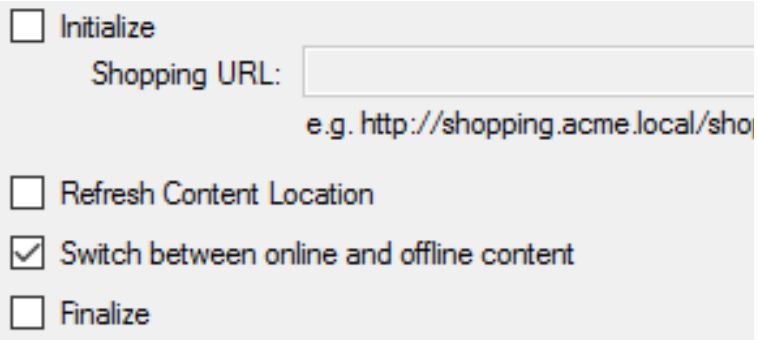
Switch between online and offline content

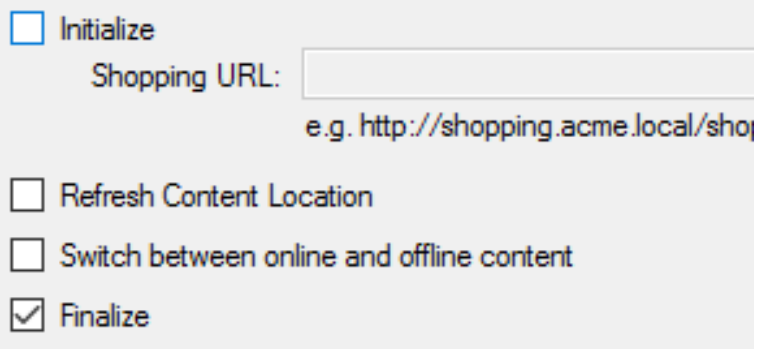
Finalize.

This custom action is available in the **1E OSD task sequence actions**.

Actions	Notes
1E WSA Actions (Initialize)	**Initialize** step should be placed at the very beginning of the task sequence. If the checkbox for **Initialize** is enabled, then all other checkboxes must be disabled. Using the Shopping URL provided, the step will attempt to obtain a WSA order record for the localhost.

Actions	Notes
 Contacts the Shopping server and attempts to identify a valid WSA order record for the host.	Only orders in the "TS Running" state are considered. If a valid WSA order is found, the step will download the order attributes and populate the task sequence environment. The many order attributes dictate the behavior of the task sequence. For instance, they indicate if USB media is required, they provide the credentials for the WiFi and VPN connections to be made and indicate if Application Migration is required. If the step cannot contact the Shopping server it will fail. Once the attributes have been obtained, if these indicate that USB media is required, and it has not been detected, then it will notify the user for the USB media.
1E WSA Actions (Refresh Content Location)  Ensures task sequence referenced content paths, defined in the current task sequence environment, are refreshed and always valid.	**Refresh Content Locations** step should be placed after any step that repartitions a disk. The checkboxes for **Refresh Content Locations** and **Switch between online and offline c ontent** can be both enabled at the same time. Under certain circumstances, a deployment may require the use of USB media for content or user data storage. In the case of content, the environment must reflect the correct local file system path before allowing the task sequence to attempt access. Operations such a restart of the host, re-partition of the disk and installation of the new OS may impact the validity of existing paths.

Actions	Notes
	The step updates the paths if required ensuring access to the content is maintained for the running task sequence.
1E WSA Actions (Switch between online and offline content)  Switches the task sequence between online and offline mode, based upon prevailing network connectivity, and attempts to establish a network connection when building over WiFi.	**Switch between online and offline c ontent** step should be placed... The checkboxes for **Refresh Content Locations** and **Switch between online and offline c ontent** can be both enabled at the same time. If network connectivity is unavailable, and the step is running in WinPE, then the step will configure the task sequence to run in offline media mode. Offline mode requires _SMSTSMediaType is set to FullMedia and the content locations defined in the task sequence environment are set to local file system paths. When in the full OS, the step will configure the task sequence to run in online mode by setting _SMSTSMediaType to BootMedia if it has been previously set to FullMedia. The step will also attempt to establish a network connection if the deployment is being performed over a WiFi connection.
1E WSA Actions (Finalize)	**Finalize** step should be positioned as the last step in the task sequence. If the checkbox for **Finalize** is enabled, then all other checkboxes must be disabled.

Actions	Notes
 Performs WSA finalization tasks once the main body of the task sequence has completed.	The step will perform cleanup operations at the end of the task sequence. *USB Cleanup* If USB media was required to complete the deployment, then the step may be required to remove all content stored on the device. Cleanup is based upon the setting made in the WSA deployment published in Shopping. **Note** Content stored on the USB device will always be restored to the local Nomad cache in the new OS. For any captured user data, this will always be removed from the device if the USMT restore succeeded. *Task Sequence status* The step will record the outcome of the task sequence in the registry: **Software\1E\WSA\TSExecutionHistory\TaskSequenceId** For zero touch restores, the step will also update the order status in Shopping to indicate that the order is closed.

Configurable Parameters

Parameter	Default Value	Description
Name	WSA Actions	Name for the custom task sequence action.

Parameter	Default Value	Description
Description	Action to configure Windows Servicing Assistant environment	Description for the custom task sequence action.
Initialize	Checked	Used to initialize the deployment.
Shopping URL		Specifies the URL of the Shopping server.
Refresh Content Locations	Unchecked	Used to maintain access to cached content.
Switch between online and offline content	Unchecked	Used to ensure the task sequence continues to function when connectivity to the ConfigMgr site is unavailable.
Finalize	Unchecked	Used to clean up the deployment.

9.6.4.5 Peer Backup Assistant - PBA

The Peer Backup Assistant (PBA) feature enables files and settings data to be backed-up to a peer device so that they can be maintained when the device is being migrated to a new Operating System. Using PBA, you can avoid the cost of State Migration Point servers to hold the backup data, as peer devices can be used to provide this storage. The risk of losing user data through the migration process is also greatly reduced in the process.

Note

Please note the:

Nomad PBA Task Sequence steps are not designed for use with offline USMT or WinPE

-NMDS_POLL command-line option for the NomadPackageLocator.exe tool cannot be used in WinPE

-NMDS_<command> command-line options for NomadBranch.exe have not been tested in WinPE, so their behavior may be unpredictable in that environment.

9.6.4.5.1 An overview of PBA

There are two types of devices involved in the PBA feature:

PBA hosts – devices running Nomad that have been configured to host a data store

PBA clients – devices running Nomad that ask for PBA data stores by broadcasting a request on the local subnet for suitable hosts. Local PBA hosts respond to these requests and the winner is chosen according to its suitability.

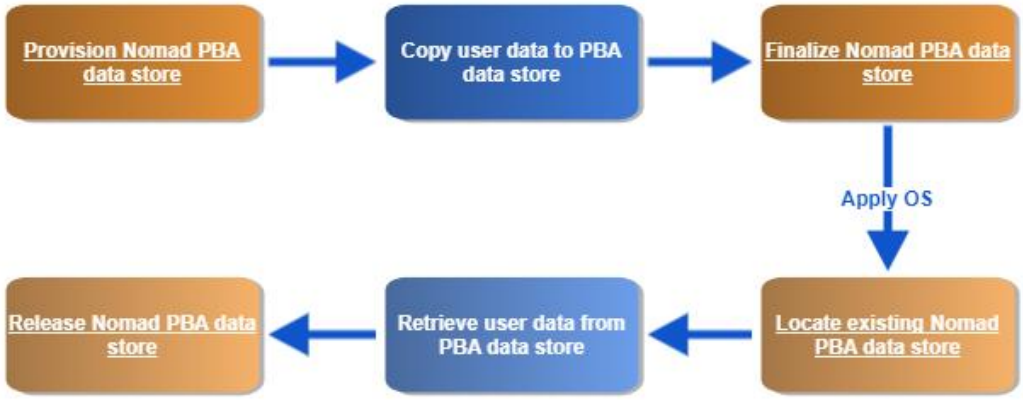
The host aspect is disabled by default but can be enabled by a Nomad administrator, whereas the client aspect is always available.

The PBA feature is implemented in the Configuration Manager OS deployment process using custom Task Sequence steps that complement the built-in Capture User State and Restore User State steps. This completely automates the migration of user data and settings using available storage on peers during an OS refresh or device replacement.

The initial step in the process initiates a local election to request the required amount of storage space from peers. Peers that are configured to act as PBA Hosts will respond to this election if they match the administrator-defined criteria (Is there enough disk space on a system to store the data? Are there other connections already in place? Are disk quotas enforced?) to store the User State Migration Tool (USMT) data.

The requesting system will then evaluate the responses and select the best candidate. The selected host then reserves the storage space. When the Capture User State step has completed, PBA transfers the migration data to the selected host, where it is stored ready to be restored later in the Task Sequence. Data can be encrypted using the built-in encryption capability of the User State Migration Tool in the Capture User State step. At this stage, Nomad can transfer copies of the data to other peers (High Availability feature) to increase the availability of the data should any of the hosts go offline before the data has been restored.

The OS deployment proceeds until the state restore phase takes place, at which point PBA locates the backed-up data using a broadcast query, restores the data to the device and deletes it from the host. The diagram below illustrates the PBA task sequence actions (in orange) and the data flow (in blue). If for any reason the restore step is not executed or fails, the migration data will remain available on the host(s) for 7 days (configurable), after which it will be deleted.



9.6.4.5.2 Single Site PBA

9.6.4.5.3 Single Site PBA

Peer Backup Assistant (PBA) enables Nomad clients to use local storage on peers to temporarily store user state data during an OS deployment, removing the need for Configuration Manager State Migration Points. By default, it uses network broadcasts to identify peers with available storage on the local subnet. Single Site Peer Backup Assistant (SSPBA) uses Single Site Download (SSD) features to enable Nomad to use storage available on PBA hosts in adjacent subnets. This enables you to:

Designate appropriate devices to provide the Nomad PBA data store for all devices on the site, not just the local subnet

Avoid the issue where clients on particular subnets do not have sufficient disk space to offer the role of a Nomad PBA data store.

To set up SSPBA, you need to ensure the following:

Tachyon Platform 5.2 or later is installed and running successfully

The Content Distribution database is populated with information about sites and their associated subnets

9.6.4.5.3.1 High-level overview of how to enable SSD

The following information applies to both new and existing installations of Nomad:

Make sure that Tachyon Platform is installed in your environment and is used as a content location metadata repository, for more information refer to Introducing Tachyon

Within Content Distribution, populate the SSD sites and subnet information. A sample PowerShell script called **PostADSitesandSubnets.ps1** is included in the Nomad installation files, which reads sites and subnets from AD

Nomad captures a list of background channels from the 1E Client in the BackgroundChannelUrl and uses the first working URL as the PlatformURL by appending /Proxy/ContentDistribution/ if this PlatformURL is unreachable it attempts to connect to the next BackgroundChannelUrl, for details about BackgroundChannelUrl refer to Nomad architecture

Enable SSD on all Nomad agents, by modifying **HKLM\Software\1E\NomadBranch\SSDEnabled** to 3, this enables SSD for both "Provide" and "Consume" modes, specifically Nomad will provide content to other peers and consume content from other peers

If you already have Nomad installed and are only now enabling SSD, then ensure **HKLM\Software\1E\NomadBranch\Platform\ContentRegistration** is set to 1, in other words, Nomad will register downloaded content with Content Distribution, this is automatically enabled for new installations of Nomad and SSD.

> **Tip**
>
> If you have clients on networks where broadcasts are disabled (for example wireless) then enable local SSD by setting SSDEnabled=7. Also set ContentProviderOnWifi=1.

9.6.4.5.3.2 Building a subnet profile in Content Distribution

For Content Distribution to build a subnet profile for SSD and the peer backup assistant feature, Nomad must communicate with its web service. When the Nomad service starts, it connects and registers the hosting device by name with Content Distribution, which returns a device ID in the form of a GUID that enables it to uniquely identify the Nomad client and its default subnet. If it is unable to communicate with Content Distribution, it retries every 5 minutes until it succeeds (as long as SSD is enabled). An attempt to communicate with Content Distribution is also made prior to a package download to register its status.

Please refer to Enabling SSD in WinPE to make use of Nomad SSD in OS Deployment.

The following points should be noted:

On a multi-NIC host, only one NIC gets registered, and a wired interface takes precedence over a wireless interface during registration

If Nomad fails initially to register an adapter, it retries every 5 minutes (for as long as SSD is enabled) until it succeeds

Wireless adapters can be configured to act as SSD content providers and consumers. Use the ContentProviderOnWiFi registry setting to do this

If the initial device registration was successful when the Nomad service started, but Content Distribution later becomes unavailable, when Nomad subsequently downloads and caches a package it will not be able to register the package with Content Distribution (see below for details). Nomad does not re-attempt package registration, so Content Distribution will not know that this particular Nomad host has the package.

9.6.4.5.3.3 Example PowerShell scripts

You can get information about sites and subnets from AD, or by other means. Example PowerShell scripts can be used for retrieving information about sites and their associated subnets from the AD and updating the Content Distribution database.

Example Active Directory Single Site script — Sample script that scans the Active Directory (AD) environment for all sites and subnets and stores the information in the Content Distribution locations table.

Example Single Site script — Sample script that provides two functions to update sites and subnets in the Content Distribution locations table: DeleteAllLocations and AddLocation().

Example Location Discovery script — Sample script to enable and disable the location discovery feature, along with the option to run it and load site, subnet and information in Content Distribution.

Content Distribution purge configuration script — Sample script to view or update Purge Configuration in the Content Distribution Service defined in the ContentDistribution PurgeSettings table if it is configured.

9.6.4.5.3.4 Enabling SSPBA

SSPBA can be enabled at install time using the MODULE.NOMAD.SSPBAENABLED installer property. Post-installation SSPBA can be enabled by setting the following registry values:

Update the SSPBAEnabled registry value to 1.

Update the SSDEnabled registry value to 0x3 to enable Content Distribution integration required for this feature to work.

When SSPBA is enabled, PBA will initially attempt to find suitable PBA data stores on the local subnet. If it does not find one, it will send the request to neighboring subnets using the information held in Content Distribution.

9.6.4.5.4 High Availability PBA (HAPBA)

High Availability PBA is implemented with the custom finalize Nomad PBA store task sequence action and requires no configuration of the underlying Nomad system, for details refer to Peer Backup Assistant: Finalize Nomad PBA Data Store.

HAPBA ensures that USMT data is stored and made available on multiple devices during the migration process to minimize risk and maximize success. Implementing HAPBA enables you to save USMT data:

In multiple locations (up to a maximum of 6) to help mitigate risk during migration

Without the need to regenerate it using the USMT save action.

Backups can be created synchronously or asynchronously. The administrator can set a value in the task sequence action that specifies the number of backups that must be successfully implemented synchronously before the task sequence continues; the remainder of the backups will be performed asynchronously while the other task sequence actions are running. This helps you manage the balance between enabling the task sequence to run promptly while ensuring sufficient backups are in place to maximize the chances of success.

HAPBA also works with SSPBA to enable the backups to reside on devices local to the site but external to the subnet of the device being migrated.

> **Note**
>
> If the task sequence variable **1EDisablePBA_HA** = True, then High Availability is disabled. This variable is automatically set for Remote WSA deployments.

9.6.4.5.5 Configuring PBA hosts

To configure a suitable Nomad client in the local branch to be a potential Peer Backup Assistant (PBA) host:

Under the *NomadBranch\NMDS* registry key, update the *MaximumMegaByte* registry value to the maximum combined size of the caches you want the PBA host to support. The default value is *0* which means that Nomad client will not reply to PBA requests.

Modify other PBA NMDS registry values to suit your environment and usage.

You can configure a number of devices in a branch to be PBA hosts for scalability.

9.6.4.5.6 Using PBA with HTTP and HTTPS P2P

By default, Nomad uses Windows file shares to share content and PBA storage with peers over SMB. You can configure Nomad to use HTTP or HTTPS to avoid the use of file shares and SMB, for details refer to Peer copy over HTTP or HTTPS. When Nomad is configured to use Peer copy over HTTP or HTTPS, a file share is not created. In this scenario the storage is exposed to peers through the HTTP server implemented in Nomad for sharing its cache. A local user account is created to secure access to the migration data store through Windows authentication.

9.6.4.5.6.1 Certificate-based Client Authentication

When Nomad is configured to use HTTPS for peer-to-peer communication, you can optionally enable Certificate-basedAuthentication. In this scenario a local user account is not created. Access to the user state store is authenticated using a client certificate.

9.6.4.5.7 Using PBA with Configuration Manager task sequences

To integrate PBA into a Configuration Manager migration task sequence for a device targeted to get a new OS:

Choose Nomad's estimation or provide a static estimate to reserve a minimum amount of disk space for user data retrieved with the User State Migration Tool (USMT) on the target device. USMT is a Microsoft command-line utility program that integrates with Configuration Manager task sequences to transfer user files and settings between devices. For suggestions of how to estimate the migration store size see Microsoft's article on estimating migration store size.

Use the provision Nomad PBA data store task sequence action to provision a data store with the name of the device being migrated and the estimated size of the USMT data. It broadcasts a request on the local subnet, and any of the locally configured PBA hosts will respond if they have the estimated space available in their PBA store. The task sequence also stores the location of the winning PBA host and share using the *%NMDS_REMOTE%* variable into the *OSDStateStorePath* task sequence variable.

Backup the USMT data to the stored share, using the USMT Capture User State task sequence action.

Use the finalize Nomad PBA data store task sequence action to close the data store. This tells the PBA host that the copy is completed and disconnects from it.

For increased availability, create extra copies of the backed-up USMT data using HA features of the finalize Nomad PBA data store task sequence action.

Migrate the target device to the new OS.

Use the locate existing Nomad PBA data store task sequence action to locate an existing data store with the name of the device being migrated. This finds the PBA host that holds the named data store on the local subnet and creates a connection to it for retrieving the data.

Restore the USMT data from the data store on the located PBA host, using the USMT Restore User State task sequence action.

Use the release Nomad PBA data store task sequence action to release the data store with the name of the device being migrated.

9.6.4.5.7.1 PBA NMDS commands

The PBA task sequence actions use some underlying *NomadBranch.exe* command-line arguments to implement their actions which are invoked using a *NomadPackageLocator.exe* wrapper to set task sequence variables that *NomadBranch.exe* relies on. So of the two Command-Line Interfaces, *NomadPackageLocator.exe* is the preferred and safer interface to use.

> **Note**
>
> We recommend that you implement PBA using the custom PBA Task Sequence steps described above. For reference, the table below identifies commands executed by these steps.

Task sequence step	NomadBranch command-line arguments
Peer backup assistant – provision Nomad PBA data store	NMDS_POLL
Peer backup assistant – close Nomad PBA data store	NMDS_COMPLETE
Peer backup assistant – high-availability	NMDS_HA
Peer backup assistant – locate existing Nomad PBA data store	NMDS_FIND
Peer backup assistant – release Nomad PBA data store	NMDS_DELETE

In addition to these commands, the following registry values can be updated in *HKLM\Software\1E\NomadBranch\NMDS* to define the behavior of PBA on the devices that are to be used as hosts for PBA data stores. These registry values are only required on PBA hosts where the data store resides and not on PBA clients requesting the store.

9.6.4.5.7.2 Enabling NMDS

The *MaximumMegaByte* registry value is set to 0 by default which means the Nomad clients will not reply to PBA requests.

To enable a Nomad client to be a PBA host:

On the host, update the *MaximumMegaByte* registry value to the maximum amount of space in MB that can be used for all the PBA data stores combined.

Restart the *NomadBranch* service.

9.6.4.5.7.3 Disabling NMDS

To disable PBA:

Update the *MaximumMegaByte* registry value to *0*.

Restart the *NomadBranch* service.

9.6.4.5.7.4 NMDS registry values

The following registry values relate to PBA and are set in *HKLM\Software\1E\NomadBranch\NMDS*:

CachePath

EnforceQuotas

MaxAllocRequest

MaxConcurrency

MaximumMegaByte

PostCompleteTimeoutHours

PreCompleteTimeoutHours.

9.6.4.5.7.5 Nomad installer command-line arguments

The following installer arguments can be set on the Nomad installer command-line to configure NMDS:

MODULE.NOMAD.ENFORCEQUOTAS

MODULE.NOMAD.MAXALLOCREQUEST

MODULE.NOMAD.MAXCONCURRENCY

MODULE.NOMAD.MAXIMUMMEGABYTE

MODULE.NOMAD.POSTCOMPLETETIMEOUTHOURS

MODULE.NOMAD.PRECOMPLETETIMEOUTHOURS

9.6.4.5.7.6 Using PBA from a client

The following illustrates the high-level order that the PBA process is initialized, used and completed during Task Sequence execution.

Run the NMDS_POLL command from the PBA client that requires a network share to store its data. This requests a named PBA share on the local subnet. The locally configured PBA hosts will hold an election to decide the PBA host for this request.

Copy files to the network share created on the winning PBA host.

Run the NMDS_COMPLETE command from the PBA client that requested the share. This tells the PBA host that the copy to the named share is been completed and disconnects from it.

Optionally, create extra backups by running NMDS_HA.

Perform the OS refresh.

Run the NMDS_FIND command from the PBA client that requested the share. This locates the PBA host that holds the named share on the local subnet.

Copy files from its share.

Run the NMDS_DELETE command from the PBA client that requested the share. This deletes the named share from the PBA host.

For details on the *NomadBranch.exe* commands refer to NomadBranch.exe command-line switches. *NomadPackageLocator.exe* can also accept the PBA NMDS commands, but it invokes *NomadBranch.exe* to do the work.

9.6.4.5.8 Secondary PBA backup data store

Note

Support for this configuration is deprecated and is currently provided for backwards compatibility only. The PBA task sequence dialogs do not support this option, therefore some scripting would be required to achieve the same functionality.

Please use High Availability (HAPBA) instead.

Note

Please note the:

Nomad PBA Task Sequence steps are not designed for use with offline USMT or WinPE

-NMDS_POLL command-line option for the NomadPackageLocator.exe tool cannot be used in WinPE

-NMDS_<command> command-line options for NomadBranch.exe have not been tested in WinPE, so their behavior may be unpredictable in that environment.

The implementation of the secondary cache uses an optional third parameter available in the NMDS_POLL command:

```
NomadBranch.exe -NMDS_POLL,<name>,<size>[,<ignore_offer>]
```

Where *<ignore_offer>* is used to specify the name of a NMDS host that already has the user data cached. Thus, when *NMDS_POLL* is run a second time with the same *<name>* and *<size>* values as on the first call, it effectively allows a second NMDS host to offer its services as a cache. In this way user state can be saved to two caches, for increased resilience. On restore, the first cache that responds to the *NMDS_FIND* request will be the one used.

A typical task sequence to use this feature looks something like this:

...

(First save)

Peer Backup Assistant: Provision Nomad PBA Data Store (which runs NomadPackageLocator.exe -NMDS_POLL,%COMPUTERNAME%,<cache_space_in_MB> behind the scenes)

Capture User State (using USMT)

Peer Backup Assistant: Close Nomad PBA Data Store.

...

(Second save)

Run Command Line action to execute a script that will extract the hostname of the NMDS host used for the first save and set an environment variable, e.g. *PBAFirstHost*.

The value to be used can be extracted from the *OSDStateStorePath* environment variable set by the "Provision" step in the first save.

The *OSDStateStorePath* value is of the form "*hostname**sharename*", and *PBAFirstHost* should be set to the *hostname* part. See example scripts below.

Run Command Line action to execute "*NomadPackageLocator.exe -NMDS_POLL,%COMPUTERNAME%,<cache_space_in_MB>,%PBAFirstHost%*". This replaces the Peer Backup Assistant: Provision Nomad PBA Data Store step used in the First save.

> Note that using *NomadPackageLocator.exe* rather than *NomadBranch.exe* additionally sets key environment variables, specifically *OSDStateStorePath*.

Capture User State (using USMT), again

Peer Backup Assistant: Close Nomad PBA Data Store (again).

...

(After applying or refreshing O/S, restore user state in the usual PBA way)

Peer Backup Assistant: Locate Existing Nomad PBA Data Store (One of the caches will be selected.)

Restore User State (USMT)

Peer Backup Assistant: Release Nomad PBA Data Store.

...

> **Note**
>
> Only one *NMDS_DELETE*call, invoked by the Release Nomad PBA Data Store action will have any effect, and it will delete the cache on only one host (the one that responded to the Locate Existing Nomad PBA Data Store request). The other cache will expire automatically after 7 days (default setting), but this may be a problem if space is tight on the Nomad cache hosts.
>
> To get round the problem, append these actions to the task sequence above:

Peer Backup Assistant: Locate Existing Nomad PBA Data Store (This will find the second cache, now that the first has been deleted.)

Peer Backup Assistant: Release Nomad PBA Data Store (To delete the second cache).

9.6.4.5.8.1 Example scripts

Here are two example scripts to implement PBA secondary backup data store:

9.6.4.5.8.1.1 VBS

```
Option Explicit
Dim oTSEnv, arrTemp
Set oTSEnv = CreateObject("Microsoft.SMS.TSEnvironment")
'Get Hostname from OSDStateStorePath
arrTemp = Split(oTSEnv("OSDStateStorePath"),"\")
'Set PBAFirstHost Variable
oTSEnv("PBAFirstHost") = arrTemp(2)
```

9.6.4.5.8.1.2 Powershell

```
$tsenv = New-Object -COMObject Microsoft.SMS.TSEnvironment
#Get Hostname from OSDStateStorePath
$arrTemp = $tsenv.value("OSDStateStorePath").Split("\")
```

```
#Set PBAFirstHost Variable
$tsenv.value("PBAFirstHost") = $arrTemp[2]
```

9.6.5 Supported Platforms

A list of all the platforms supported by Nomad, and the software required to allow Nomad to be installed or to work.

9.6.5.1 Tachyon Platform

Although not a requirement for generally using Nomad, the Tachyon Platform must be installed and available before you can use certain features.

The following features use Content Distribution and require Tachyon platform and platform features of Nomad to be enabled:

Nomad app provides visibility of content distribution activity.

Single Site Download (SSD) (SSD).

Single Site Peer Backup Assistant - SSPBA (SSPBA).

High Availability PBA (HAPBA) (HAPBA).

Get Migration Settings task sequence action used to manage computer associations.

Nomad Pre-caching.

Nomad Download Pause.

> **Note**
>
> Nomad versions prior to Nomad 7.1 used ActiveEfficiency to support similar features. Tachyon platform previously included ActiveEfficiency.

The following features were provided in versions older than Nomad 7.1

1E Client Health - now provided by the Guaranteed State feature of the platform.

Nomad Dashboard - now provided by Nomad app feature of the platform.

For everything you need to know about getting the platform installed and running in your network, please refer to Planning for Tachyon.

Refer to Server software for Tachyon server requirements and information that will help you design and plan the implementation of Tachyon in your organization.

9.6.5.2 Nomad Administration Tools

Category	Product	Notes
Windows OS	OS versions supported by	

Category	Product	Notes
	Configuration Manager versions are listed below.	
Microsoft Endpoint Manager Configuration Manager	MECM CB 2203 MECM CB 2111 MECM CB 2107 MECM CB 2103 MECM CB 2010	1E maintains a testing cycle for our products relative to the Current Branch release cycle. Please refer to Microsoft Rapid-Release Cycle on https://support.1e.com/ for the latest information on future releases of CM Current Branch, and any advisories related to these releases. **Note** When using CB 1910, be sure to apply Hotfix rollup KB4537079 or later to sites. Prior to this update, there is an issue that prevents Alternate Content Providers downloading certain types of content referenced in Task Sequences. **Note** Microsoft, and therefore 1E, no longer support CB1706. If you are running CB1706 and find that NomadAdminUI is not working as expected, we recommend you apply KB4036267 to address the issue. For each Configuration Manager site server where you intend to administer task sequence packages to use Tachyon as the alternate download provider, you need to ensure that: The Configuration Manager Admin Console must be installed on the site server – as is the case in a default Configuration Manager installation. This is a prerequisite for installing the Admin Console GUI extensions, which must be installed on the site server before installing on any remote Configuration Manager console. Ensure you meet the prerequisites for Configuration Manager if you are using the **BIOS to UEFI** feature: BIOS TO UEFI 1.4 - Requirements.

Category	Product	Notes
		Note If these conditions are not met, the Tachyon settings for task sequences will not be created correctly. This is the case even if you install a remote Configuration Manager Admin Console with the Nomad Admin Console GUI extension, except for Nomad Branch Tools, which are required to be installed on Configuration Manager Site Server only.
Runtime libraries	Visual C++ 2013 Redistributable ASP.NET Core Framework 3.1 .NET Framework 4.8	**Note** .NET Framework is required for the **Admin Console GUI extensions**, the **Download Monitor**, and **NomadBranch GUI**. It is not a requirement for other features of Nomad.
Antivirus	Nomad is able to work with Antivirus systems provided they have certain exclusions configured.	It is likely that performance will be impaired by antivirus programs. To mitigate this, we have detailed suggested antivirus exclusions you can implement. Please refer to Nomad post-installation tasks.

Nomad client

The 1E Client (with Nomad client enabled) must be installed on client devices and Configuration Manager Distribution Points.

Category	Product	Notes
Windows OS	Windows Server 2022	The zip for 1E Client for Windows is available for download from the 1E Exchange.
	Windows Server 2019	Professional and Enterprise editions are supported for Windows 10 and Wndows 11.
	Windows Server 2016	All versions are provided with 32-bit & 64-installers, and can be installed on physical and virtual computers.

Category	Product	Notes
	Windows 11 CB 21H2 Windows 10 CB 21H2 Windows 10 CB 21H1 Windows 10 CB 20H2	**Note** This list shows only those OS versions in mainstream support by Microsoft, and therefore supported by Tachyon, and by 1E Client 8.1. Please refer to Constraints of Legacy OS regarding the end of mainstream support. For Microsoft product lifecycle details, please refer to https://support.microsoft.com/en-us/lifecycle/search. Refer to Support for Microsoft Rapid-Release Cycle on https://support.1e.com/ for details of which Current Branch versions are supported by 1E products, and known issues regarding specific versions. For Windows Server 2016 Core Server installations: Only 64-bit versions are supported Distribution Points on this OS do not support PXE or Multicast. For installation guidance on Windows, please refer to Deploying 1E Client on Windows. Nomad and Nomad Multicast require MSXML6 to communicate with the Configuration Manager client. This is present in all the supported versions of Windows (with the required service packs). Peer copy over HTTP or HTTPS is the recommended method of peer sharing content.
Runtime libraries	.NET Framework 4.8	.NET Framework is required only for the following features of 1E Client:

Category	Product	Notes
	.NET Framework 4.7.2 .NET Framework 4.7.1 .NET Framework 4.7 .NET Framework 4.6.2 .NET Framework 4.6.1 .NET Framework 4.6	The Real-Time Control Center feature of the 1E Client (also known as 1E Client UI and Interaction module) supports Experience Engagements (Announcements and Surveys), and ITSM Support Tickets Windows Servicing Assistant (WSA) feature of the Shopping client module, which supports OS deployment, upgrades and migrations. **Note** This list is automatically updated to show only those .NET Framework versions in mainstream support by Microsoft, and therefore supported by 1E, and by Tachyon 8.1. For Microsoft product lifecycle details, please refer to https://support.microsoft.com/en-us/lifecycle/search.
Other Windows Software	Visual C++ 2013 Redistributable Nomad 7.0 (or later) PowerShell 3.0 (or later)	1E Client installer includes the redistributable package for Visual C++ 2013. 1E Client provides client features. It also includes the Nomad client module which replaces the legacy branch client. Tachyon client features can optionally use Nomad to download content (feature enabled by default) if the Nomad client module in is enabled (module disabled by default) or Nomad Branch 7.0 or later is running. PowerShell is not a prerequisite for the installation of the 1E Client. PowerShell is used by some Tachyon instructions (that have PowerShell commands embedded or scripts that are downloaded) and some of these require PowerShell 3.0 or later. For more details, please refer to Downloading client content and Nomad integration.

Category	Product	Notes
Microsoft Endpoint Manager Configuration Manager Client	MECM CB 2203 MECM CB 2111 MECM CB 2107 MECM CB 2103 MECM CB 2010	**Note** This list is automatically updated to show only those Configuration Manager versions in mainstream support by Microsoft, and therefore supported by 1E, and by Nomad 8.1. For Microsoft product lifecycle details, please refer to https://support.microsoft.com/en-us/lifecycle/search. Please refer to the Support for Microsoft Rapid-Release Cycle on https://support.1e.com/ for details of which Current Branch versions are supported by 1E products, and known issues regarding specific versions. 1E maintains a testing cycle for our products relative to the Current Branch release cycle. Please refer to Microsoft Rapid-Release Cycle on https://support.1e.com/ for the latest information on future releases of CM Current Branch, and any advisories related to these releases. **Note** When using CB 1910, be sure to apply Hotfix rollup KB4537079 or later to sites. Prior to this update, there is an issue that prevents Alternate Content Providers downloading certain types of content referenced in Task Sequences. **Note** If IIS filtering is enabled on Distribution Points, you may encounter problems during downloads if certain types of content are present in the download. Please refer to IIS Request Filtering.

Category	Product	Notes
		(Microsoft Endpoint Configuration Manager is also known as Configuration Manager, ConfigMgr, Config Man, CM and SCCM among other names. Version names include 2012 and Current Branch or CB.)
Antivirus	Nomad is able to work with Antivirus systems provided they have certain exclusions configured.	It is likely that Tachyon performance will be impaired by antivirus programs. To mitigate this, we have detailed suggested antivirus exclusions you can implement. Please refer to Nomad post-installation tasks.

9.6.5.3 Legacy OS constraints

In this documentation, the following are referred to as legacy OS. Below are described some known issues for these OS.

1E does not provide support for 1E products on the following OS unless the OS is explicitly listed as being supported for a specific 1E product or product feature. This is because Microsoft has ended mainstream support for these OS or they are not significantly used by business organizations.

Windows XP *	**Windows Server 2003 ***
Windows Vista	**Windows Server 2008**
Windows 7	**Windows Server 2008 R2**
Windows 8.0	**Windows Server 2012**
Windows 8.1	**Windows Server 2012 R2**

> **Note**
>
> 1E Client 8.1 and later will not install on Windows XP and Windows Server 2003. Please contact 1E if you intend to continue using any of the other legacy OS. If you experience an issue, then please try replicating the issue on a supported OS.

For Microsoft product lifecycle details, please refer to https://support.microsoft.com/en-us/lifecycle/search.

9.6.5.3.1 PowerShell limitations

PowerShell version 3.0 (required by some Tachyon instructions) is not supported on Windows XP, Vista and Server 2003. However, PowerShell 2.0 is supported on the following OS versions:

Windows XP SP3

Vista SP1 & SP2

Windows Server 2003 R2 & SP2.

9.6.5.3.2 Certificate limitations - SHA2

Like most software vendors, 1E software requires the OS to support SHA2. If your organization has a PKI configured to use SHA2 256 or higher encryption, then your legacy OS may have already been updated to support it.

Windows XP and Server 2003 require an update as described in **KB968730.** Microsoft no longer provides this hotfix as a download. You must contact Microsoft Support if you need it

Windows 7 and Server 2008 R2 require an update as described in **KB3033929**. This update is not available for Vista and Server 2008

Windows 8, 8.1, Server 2012, Server 2012 R2 and later OS already support SHA2.

9.6.5.3.3 Certificate limitations - encrypted certificate requests

Windows XP and Server 2003 are unable to encrypt certificate requests, whereas later OS are able to support higher more secure RPC authentication levels. If you are using a Microsoft CA and expect these clients to request (enrol) certificates then the CA must have its IF_ENFORCEENCRYPTICERTREQUEST flag disabled. It is disabled by default on Windows 2003 and 2008 CA, but is enabled by default on Windows 2012 CA.

To determine which InterfaceFlags are set, execute the following command on the CA server:

```
certutil -getreg CA\InterfaceFlags
```

If the following is specified then it means the flag is enabled.

```
IF_ENFORCEENCRYPTICERTREQUEST -- 200 (512)
```

To disable the encrypt certificate requests flag, execute the following commands on the CA server:

```
certutil -setreg CA\InterfaceFlags -IF_ENFORCEENCRYPTICERTREQUEST
sc stop certsvc
  sc start certsvc
```

9.6.5.3.4 Certificate limitations - signing certificates missing

On Windows computers, the installation MSI files, and binary executable and DLL files of 1E software are digitally signed. The 1E code signing certificate uses a timestamping certificate as its countersignature. 1E occasionally changes its code signing certificate, and uses it for new releases and patches for older versions, as shown in the table(s) below.

Root Certificate Authorities are implicitly trusted to validate certificates, and their certificates must be correctly installed to do this. Your computers should already have the necessary **root CA** certificates installed, however this may have been prevented by your organization's security policies, or inability to connect to the Internet, or they are legacy OS. In general this is not an issue because by default Windows allows software to be installed and run without validation, although you may see a warning or experience a delay. However, you *must* have relevant CA certificates installed if you are using 1E Client (which self-validates its own files), or your organization has applied more secure polices (for example UAC, AppLocker or SmartScreen).

Typical reasons for issues with signing certificate are:

If your organization has disabled **Automatic Root Certificates Update** then you must ensure the relevant **root CA** certificates are correctly installed on each computer

If computers do not have access to the Internet then you must ensure the relevant **root and issuing CA** certificates are correctly installed on each computer, numbered in the table(s) below.

The signature algorithm of the 1E code signing certificate is SHA256RSA. In most cases, the file digest algorithm of an authenticode signature is SHA256, and the countersignature is a RFC3161 compliant timestamp. The exception is on legacy OS (Windows XP, Vista, Server 2003 and Server 2008) which require the file digest algorithm of an authenticode signature to be SHA1, and a legacy countersignature.

The table below applies to software and hotfixes released in 2020.

2020	**Signing certificate**	**Timestamping certificates**
Certificate	1E Limited	TIMESTAMP-SHA256-2019-10-15 ***and*** DigiCert Timestamp Responder
Issuing CA	**DigiCert EV Code Signing CA (SHA2)** Thumbprint: 60ee3fc53d4bdfd1697ae5beae1cab1c0f3ad4e3	**DigiCert SHA2 Assured ID Timestamping CA** Thumbprint: 3ba63a6e4841355772debef9cdcf4d5af353a297 ***and*** **DigiCert Assured ID CA-1** Thumbprint: 19a09b5a36f4dd99727df783c17a51231a56c117
Root CA	**DigiCert High Assurance EV Root CA** Thumbprint: 5fb7ee0633e259dbad0c4c9ae6d38f1a61c7dc25	**DigiCert Assured ID Root CA** Thumbprint: 0563b8630d62d75abbc8ab1e4bdfb5a899b24d43

This is described in Digital signing certificates. To verify if you affected by this issue see 1E Digital Signing Certificates.

9.6.5.3.5 Certificate limitations - expired root certificates

Ensure that your Root CA Certificates are up-to-date on clients and servers. The **Automatic Root Certificates Update** feature is enabled by default, but its configuration may have been changed or restricted by Group Policy **Turn off Automatic Root Certificates Update**.

If this GPO is enabled, then you will see *DisableRootAutoUpdate = 1 (dword)* in *HKLM\Software\Policies\Microsoft\SystemCertificates\AuthRoot.*

9.6.6 1E Companion Products

A list of the feature dependencies between Nomad and other 1E companion products.

This page describes the dependencies to and from Nomad in regard to certain features that are implemented across companion 1E products. To view the general platform related dependencies for Nomad please refer to Supported Platforms.

9.6.6.1 1E companion products that Nomad depends on

Supported versions of 1E companion products that Nomad features depend on.

Products and features that Nomad depends on	Supported versions of companion products	
Tachyon Platform	Nomad Download Pause feature is an optional feature of Nomad and requires a full Tachyon infrastructure.	Nomad 7.0.200 Nomad 7.0.100 Nomad 7.0 Nomad 7.1 Nomad 8.0 Nomad 8.1

9.6.6.2 1E companion products that depend on Nomad

Supported versions of 1E companion products with features that depend on Nomad.

For products that depend on the 1E Client, please refer to 1E Companion Products that depend on 1E Client 8.0.

Products and features that depend on Nomad	Supported versions of companion products	
Tachyon Platform	Tachyon clients can optionally use Nomad (1E Client with Nomad client features enabled) to provide more efficient downloading of content.	1E Client 5.1 (with Nomad client enabled) 1E Client 5.0 (with Nomad client enabled) 1E Client 4.1 (with Nomad client enabled).

9.6.7 Communication ports

Diagrams and tables with all the external Nomad communication ports. Useful, if needed, for network and device firewalls.

9.6.7.1 Networking

Due to the nature of how proxy servers can be implemented, some of which can be quite complex, you may need to consult your networking specialist to see if exceptions need to be added to enable Nomad's peer-copy over HTTP or HTTPS.

The following are the ports used by Nomad client on clients and on Distribution Points. The table does not include Configuration Manager communications, which can be found here: https://docs.microsoft.com/en-us/sccm/core/plan-design/hierarchy/communications-between-endpoints.

Ports	Notes	Configurable
UDP 1779	Default port Nomad uses for listening to elections to determine the master on a subnet, control traffic and for content transfer if you have Connectionless enabled. A firewall exception must exist for this port. Nomad will create one automatically for Windows firewall, but not for other firewall software.	Yes, during installation.
TCP 80 (HTTP) or	Used when the Nomad master requests LSZ files from Nomad running on the DP and when the	No, for communications with CM components. Nomad service on startup reads the configured ports from CM

Ports	Notes	Configurable
TCP 443 (HTTPS)	Nomad master downloads content using Nomad as provider. Communications depend on how the DP is configured. Configuration Manager is configured to use either HTTP or HTTPS. If Nomad clients and Content Distribution are configured to use HTTP/S, Nomad clients using SSD register and query for content.	client registry and uses the same for LSZ generation. Yes, for communications with Tachyon Platform using Nomad's PlatformURL setting.
TCP 5080 (HTTP) or TCP 5443 (HTTPS)	Default HTTP port to use for peer copy. If you are using a custom port, ensure that all agents use the same custom port. From Nomad 6.2, peer copy can be enabled over HTTP (default 5080) or HTTPS (default 5443). You can customize the ports for this feature in the host registry but a change to the default impacts Nomad's peer backup assistant which is used to capture user data on remote peers during OS deployments.	Yes, during installation.
TCP 139 (SMB) and TCP 445 (SMB over TCP)	Required only if SMB is enabled. Used for peer-to-peer content transfer between the Nomad master and Nomad peers. Communications depend on how the DP is configured. That is HTTP, HTTPS, SMB or SMB over TCP. For Configuration Manager the default is HTTP or HTTPS. Windows Firewall automatically adds the exception when you enable **File and Print Sharing** but you may have to do this manually if you are using a different firewall product.	No. SMB ports cannot be configured.
TCP 137 (SMB) and TCP 139 (SMB)	Required only if SMB is enabled. Used by SMB for data transfer and related communications. It is used to resolve NetBIOS names during a transfer. UDP NetBIOS name query packets are sent to this port.	No. SMB ports cannot be configured.

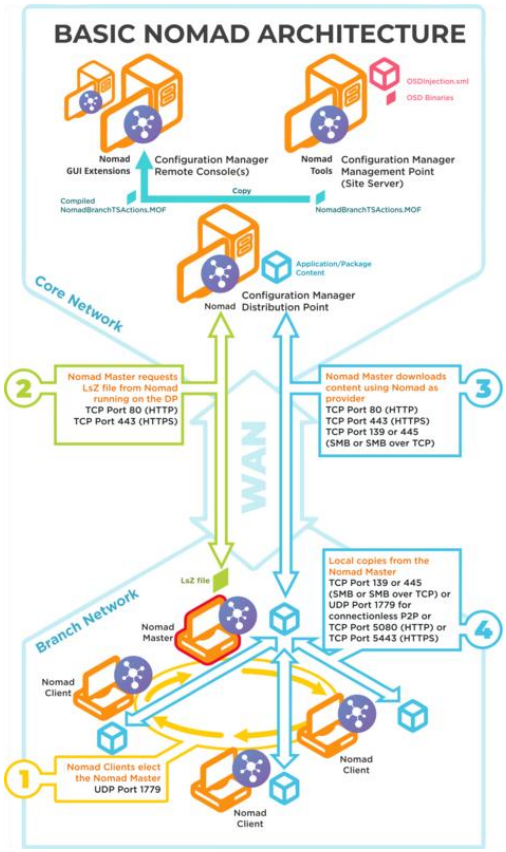
Ports	Notes	Configurable
	Windows Firewall automatically adds the exception when you enable **File and Print Sharing** but you may have to do this manually if you are using a different firewall product.	

Nomad can use ephemeral ports (not discussed here). Ephemeral or high ports can either be UDP or TCP depending on the protocols used and are used to send information out. In a typical client-server communication, these are ports opened by the client on its own machine in order to send something to the server and they are closed as soon as the transmission is done, hence the term ephemeral. From a security perspective, it is not an issue.

Most firewalls will allow outgoing communications by default so in all likelihood, you will not need to do any firewall configuration. However, if your firewall blocks these outbound communications, consult the documentation for your firewall on how to enable these types of communications.

9.6.7.2 Basic Nomad architecture

Click image to enlarge.

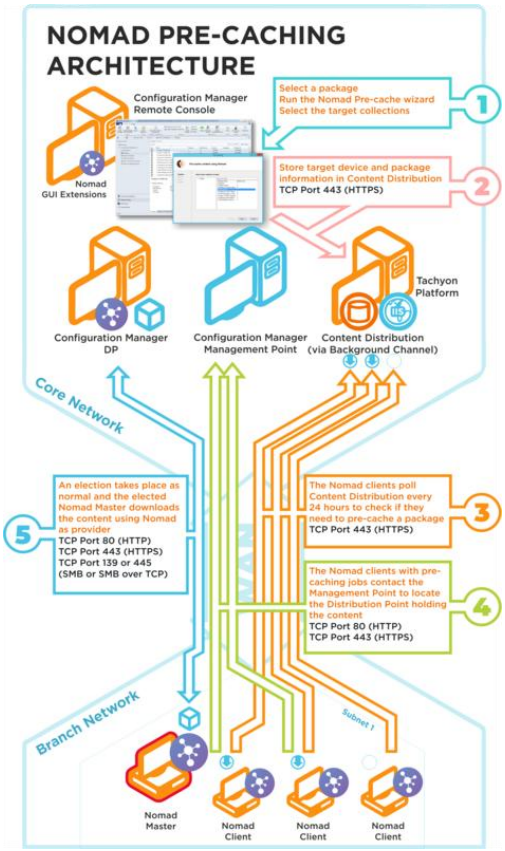


Ports	Notes
UDP 1779	**Step 1** By default, Nomad uses UDP Port 1779 to communicate during the election process for determining the master on a subnet. The Nomad installer will automatically add *NomadBranch.exe*,*NomadPackageLocator.exe* and *PackageStatusRequest.exe* to the list of excepted programs in the native Windows Firewall. The default value for the port may be changed at install time using the MODULE.NOMAD.P2PPORT installer property or post-installation by changing the P2P_Port registry value. If you change the default port, you must ensure all Nomad clients communicate using the same port. The Nomad port (by default UPD Port 1779) must be open on all wireless access points to facilitate Nomad peer-to-peer communications. Not all vendors enable this port by default, please refer to the specific device vendor's documentation for details on how to enable ports on each WAP device.
TCP 80 (HTTP) TCP 443 (HTTPS)	**Step 2** Nomad Master requests LSZ file from Nomad running on the DP.
TCP 80 (HTTP) TCP 443 (HTTPS) TCP 139 (SMB) TCP 445 (SMB over TCP)	**Step 3** Nomad Master downloads content using Nomad as provider. This communication depends on how the DP is configured. It may be one of the following: HTTP HTTPS SMB SMB over TCP For Configuration Manager the default setting is HTTP or HTTPS.
TCP 139 (SMB) TCP 445 (SMB over TCP)	**Step 4** Local copies from the Nomad master. The recommended way to facilitate Nomad cache access is to enable Windows File and Print Sharing. If this is not feasible on your network environment you can configure Nomad to use

Ports	Notes
UDP 1779 (used for connectionless P2P) TCP 5080 (HTTP) TCP 5443 (HTTPS)	different means to access network shares, see Nomad cache for more details on configuring this option. Connections may use one of the following: SMB SMB over TCP Connectionless P2P HTTP HTTPS

9.6.7.3 Nomad pre-caching architecture and ports

Click image to enlarge.

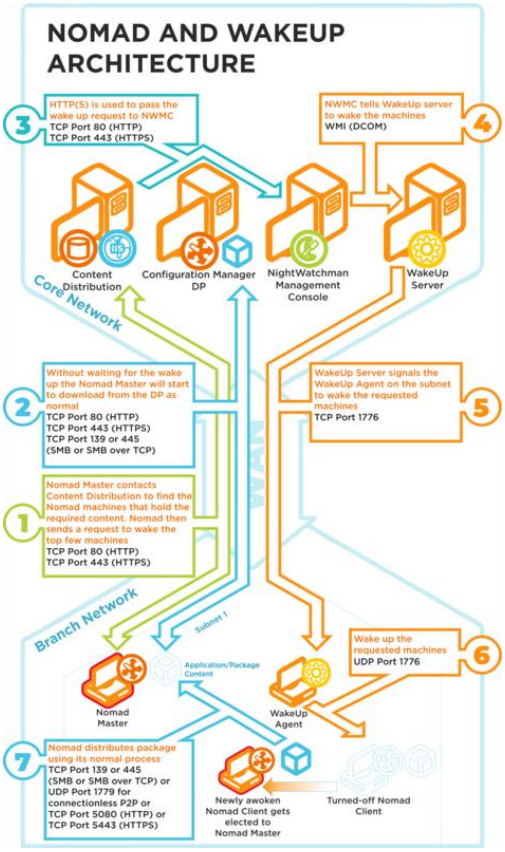


The Nomad pre-caching uses the following ports in its communications. If a site server is configured to use custom ports, pre-caching will use those ports to communicate with a management or distribution points. To ensure high-availability, pre-caching falls back to next available site server if it fails to communicate with a management or distribution point.

Ports	Description
N/A	**Step 1** Choose a package and run the Nomad pre-caching wizard, selecting the target device collection. This step does not require any port configuration but the Nomad Configuration Manager console extensions must be installed in the Configuration Manager Console.
TCP 80 (HTTP) TCP 443 (HTTPS)	**Step 2** The Nomad pre-caching wizard stores the target device and package information in Tachyon.
TCP 80 (HTTP) TCP 443 (HTTPS)	**Step 3** The Nomad clients, where the pre-cache feature has been enabled, poll Tachyon every 24 hours to see if they need to pre-cache some content. This takes the form of pre-caching notifications that tell the Nomad clients they need to process a download job to fetch the specified content.
TCP 80 (HTTP) TCP 443 (HTTPS)	**Step 4** The Nomad clients, with pre-caching notifications, contact the Management Point to locate the Distribution Point that holds the content. This may use HTTP or HTTPS depending on how the Management Point is configured.
TCP 80 (HTTP) TCP 443 (HTTPS) TCP 139 (SMB) TCP 445 (SMB over TCP)	**Step 5** A Nomad Master election takes place and the elected master processes the job by downloading the pre-cache content using Nomad as provider. This is then distributed locally to the Nomad peers that also require the pre-cached content. This communication depends on how the DP is configured. It may be one of the following: HTTP HTTPS SMB SMB over TCP For Configuration Manager the default setting is either HTTP or HTTPS.

9.6.7.4 Nomad and WakeUp integration architecture and ports

Click image to enlarge.

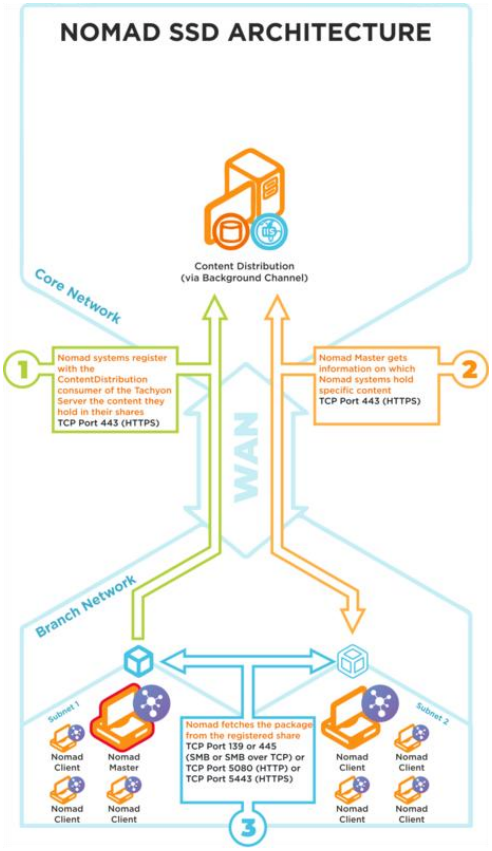


Ports	Description
TCP 80 (HTTP)	**Step 1**
TCP 443 (HTTPS)	Nomad Master contacts Content Distribution and gets a list of Nomad devices that hold the content it requires. Nomad sends a request to wake the top 5 devices on the list. Refer to WakeUpBatchSize for details about how you can set the maximum number of machines to wake up in a single call.
TCP 80 (HTTP) TCP 443 (HTTPS) TCP 139 (SMB) TCP 445 (SMB over TCP)	**Step 2** Without waiting for any devices to be awoken, the Nomad master starts to download content from the DP. This communication depends on how the DP is configured. It may be one of the following: HTTP

Ports	Description
	HTTPS SMB SMB over TCP For Configuration Manager, the default setting is HTTP or HTTPS.
TCP 80 (HTTP) TCP 443 (HTTPS)	**Step 3** Content Distribution posts the wake message from Nomad to the NightWatchman Management Center Web API.
WMI (DCOM)	**Step 4** NightWatchman Management Center tells the WakeUp server to wake the requested devices.
TCP 1776	**Step 5** WakeUp Server signals the WakeUp Agent on the appropriate subnet to wake the requested devices.
UDP 1776	**Step 6** The WakeUp agent on the subnet sends a wakeup request to the requested devices.
TCP 139 (SMB) TCP 445 (SMB over TCP) UDP 1779 (connectionless P2P)	**Step 7** As part of its standard behavior, Nomad holds regular elections (every 5 minutes) to determine the most appropriate master. If a device is found (i.e. one that has been recently awoken) that holds more of the required content, it stops downloading from the DP and fetches the content from the new device's cache. This may be via SMB or via connectionless P2P, depending on the configuration of Nomad.

9.6.7.5 Nomad SSD architecture and ports

Click image to enlarge.



Nomad SSD uses the following ports in its communications:

Ports	Notes
TCP 80 (HTTP)	**Step 1**
TCP 443 (HTTPS)	Nomad systems on the branch site register in Content Distribution the content they hold in their shares
TCP 80 (HTTP)	**Step 2**
TCP 443 (HTTPS)	Nomad Masters get information on which Nomad systems hold specific content
TCP 80 (HTTP)	**Step 3**
TCP 443 (HTTPS)	Nomad Master fetches a package from the registered Nomad share on a neighboring subnet
TCP 139 (SMB)	
TCP 445 (SMB over TCP)	

We recommend that the latest version of Tachyon Platform is installed to support this feature, please refer to Requirements for more details.

9.6.8 Log files

Names and locations of log files created by Nomad.

9.6.8.1 Nomad logs

The default location for all Nomad logs is the folder *%ALLUSERSPROFILE%\1E*

For issues relating to	Required log files	Location of log files
1E Client	*1E.Client.log* *NomadBranchUninstall-YYY-MM-DDThh_mm_ss_000Z.log*	Default location: %ALLUSERSPROFILE%\1E\Client\
Nomad client	*NomadBranch.log*	Default location: %ALLUSERSPROFILE%\1E\NomadBranch\ Optional location if installed using 1E Client Deployment Assistant (CDA): C:\WINDOWS\CCM\Logs\
OS deployment	*NomadPackageLocator.log* *NBCacheActions.log* All Configuration Manager logs including *SMSTS.log*	The path changes at the different stages of an OS deployment.
Nomad and ContentDistribution integration	*ContentDistribution.log*	%ALLUSERSPROFILE%\1E\ContentDistribution\
Delivery Optimization monitoring and reporting	*NomadBranch.DO.log*	Default location: %ALLUSERSPROFILE%\1E\NomadBranch\ NomadBranch.DO.log is created when Delivery Optimization monitoring and reporting are enabled using the

For issues relating to	Required log files	Location of log files
		DeliveryOptimizationReportingEnabled registry value.

9.6.8.1.1 Logging Levels

The table below describes the logging levels which are configurable for server components.

Value	Description
Error	Only outputs errors. An error is a serious problem, typically requiring operator intervention of some sort to restore full functionality.
Warn	Outputs errors and warnings. A warning indicates a potential problem, where the system can nonetheless function without intervention.
Info	Outputs general information in addition to errors and warnings. This is the default.
Debug	Outputs debugging information in addition to all the previous levels.

Warning

Logging levels should only be changed from **info** only if requested by 1E Support and reset to **info** after investigation is complete.

Tip

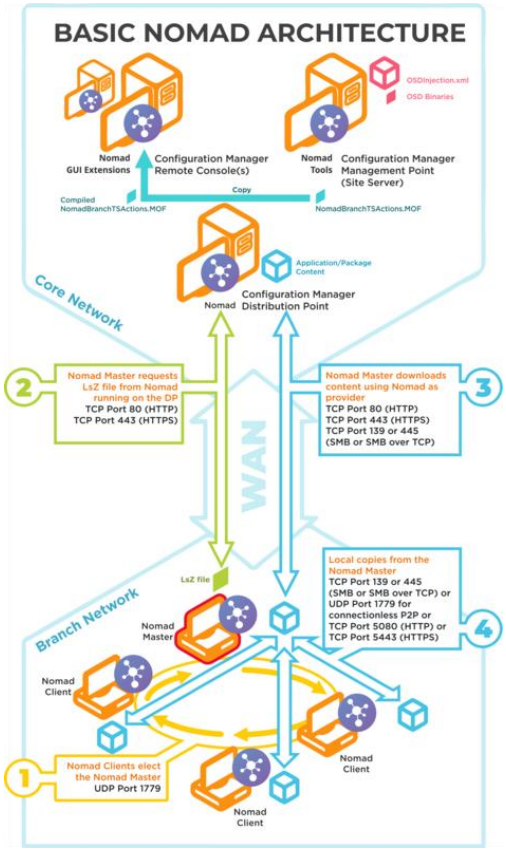
The method of configuring logging levels uses the above text values, where -log=0 is the default to mean the same as `-log=info`.

9.6.9 Nomad architecture

A description of Nomad and its components and how they connect. The page provides a brief overview of each feature and links to other pages with more detail.

9.6.9.1 Basic Nomad architecture

Click image to enlarge.

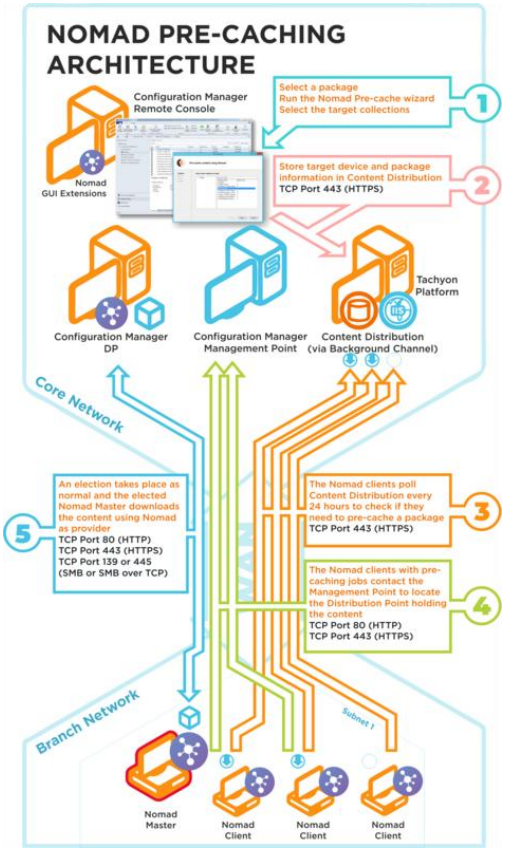


Ports	Notes
UDP 1779	**Step 1** By default, Nomad uses UDP Port 1779 to communicate during the election process for determining the master on a subnet. The Nomad installer will automatically add *NomadBranch.exe*,*NomadPackageLocator.exe* and *PackageStatusRequest.exe* to the list of excepted programs in the native Windows Firewall. The default value for the port may be changed at install time using the MODULE.NOMAD.P2PPORT installer property or post-installation by changing the P2P_Port registry value. If you change the default port, you must ensure all Nomad clients communicate using the same port. The Nomad port (by default UPD Port 1779) must be open on all wireless access points to facilitate Nomad peer-to-peer communications. Not all vendors enable this port by default, please refer to the specific device vendor's documentation for details on how to enable ports on each WAP device.
TCP 80 (HTTP)	**Step 2**

Ports	Notes
TCP 443 (HTTPS)	Nomad Master requests LSZ file from Nomad running on the DP.
TCP 80 (HTTP) TCP 443 (HTTPS) TCP 139 (SMB) TCP 445 (SMB over TCP)	**Step 3** Nomad Master downloads content using Nomad as provider. This communication depends on how the DP is configured. It may be one of the following: HTTP HTTPS SMB SMB over TCP For Configuration Manager the default setting is HTTP or HTTPS.
TCP 139 (SMB) TCP 445 (SMB over TCP) UDP 1779 (used for connectionless P2P) TCP 5080 (HTTP) TCP 5443 (HTTPS)	**Step 4** Local copies from the Nomad master. The recommended way to facilitate Nomad cache access is to enable Windows File and Print Sharing. If this is not feasible on your network environment you can configure Nomad to use different means to access network shares, see Nomad cache for more details on configuring this option. Connections may use one of the following: SMB SMB over TCP Connectionless P2P HTTP HTTPS

9.6.9.2 Nomad pre-caching architecture and ports

Click image to enlarge.



The Nomad pre-caching uses the following ports in its communications. If a site server is configured to use custom ports, pre-caching will use those ports to communicate with a management or distribution points. To ensure high-availability, pre-caching falls back to next available site server if it fails to communicate with a management or distribution point.

Ports	Description
N/A	**Step 1** Choose a package and run the Nomad pre-caching wizard, selecting the target device collection. This step does not require any port configuration but the Nomad Configuration Manager console extensions must be installed in the Configuration Manager Console.
TCP 80 (HTTP) TCP 443 (HTTPS)	**Step 2** The Nomad pre-caching wizard stores the target device and package information in Tachyon.
TCP 80 (HTTP)	**Step 3** The Nomad clients, where the pre-cache feature has been enabled, poll Tachyon every 24 hours to see if they need to pre-cache some content. This takes the form

Ports	Description
TCP 443 (HTTPS)	of pre-caching notifications that tell the Nomad clients they need to process a download job to fetch the specified content.
TCP 80 (HTTP) TCP 443 (HTTPS)	**Step 4** The Nomad clients, with pre-caching notifications, contact the Management Point to locate the Distribution Point that holds the content. This may use HTTP or HTTPS depending on how the Management Point is configured.
TCP 80 (HTTP) TCP 443 (HTTPS) TCP 139 (SMB) TCP 445 (SMB over TCP)	**Step 5** A Nomad Master election takes place and the elected master processes the job by downloading the pre-cache content using Nomad as provider. This is then distributed locally to the Nomad peers that also require the pre-cached content. This communication depends on how the DP is configured. It may be one of the following: HTTP HTTPS SMB SMB over TCP For Configuration Manager the default setting is either HTTP or HTTPS.

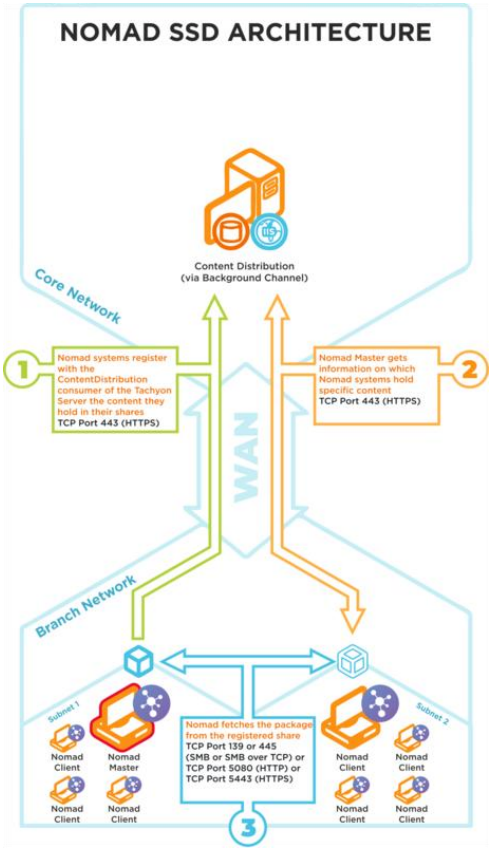
9.6.9.3 Nomad and 1E WakeUp integration architecture and ports

Nomad integration with WakeUp enables Nomad to share content from its devices that are holding particular content, even if those devices are offline. One reason why peers in the local subnet may not respond to the request even though they have content in their caches is that they are offline (shutdown, in hibernate or sleep mode). However, if WakeUp is integrated, the Nomad client would know which offline device has the content and can wake it up when it queried Content Distribution.

The wake up list is maintained by Content Distribution and is the same list that Single Site Download (SSD) uses. Separate lists of peers are returned for subnet and site. This feature requires Nomad SSD to be enabled, Content Distribution and a NightWatchman infrastructure. The feature is enabled during installation of NightWatchman Management Center. Please refer to Nomad Preparation for requirements.

9.6.9.4 Nomad SSD architecture and ports

Click image to enlarge.



Nomad SSD uses the following ports in its communications:

Ports	Notes
TCP 80 (HTTP)	**Step 1**
TCP 443 (HTTPS)	Nomad systems on the branch site register in Content Distribution the content they hold in their shares
TCP 80 (HTTP)	**Step 2**
TCP 443 (HTTPS)	Nomad Masters get information on which Nomad systems hold specific content
TCP 80 (HTTP)	**Step 3**
TCP 443 (HTTPS)	Nomad Master fetches a package from the registered Nomad share on a neighboring subnet
TCP 139 (SMB)	
TCP 445 (SMB over TCP)	

We recommend that the latest version of Tachyon Platform is installed to support this feature, please refer to Requirements for more details.

9.6.10 Nomad command-line switches

Nomad accepts configuration changes that can be specified on the command-line. The command-line options for Nomad should be denoted using double dashes (--) or double slashes (//) to distinguish them from the main install command-line.

For Configuration Manager additional Nomad options for controlling the Nomad Provider are denoted using double plusses (++).

The references for the command-line switches for both the Nomad executable files are given under the following links.

SMSNomad.exe command-line switches

NomadBranch.exe command-line switches

The references for the command-line switches for Nomad utilities are given under the following links:

NomadPackageLocator.exe command-line switches

TSEnv2 command-line switches

CacheCleaner.exe command-line switches

9.6.10.1 SMSNomad.exe command-line switches

This executable does not normally need to be run on a command-line, but details are provided here for reference purposes. SMSNomad.exe is normally installed as part of Nomad and configured using Configuration Manager Admin console extensions. It is also available in Nomad OSD tools in order to include in WinPE images so that Nomad can be used in OS Deployments.

Please refer to Distributing software with Nomad and Configuration Manager: Nomad tab for different types of content and Installing Nomad Branch Tools for a step-by-step guide to installing Nomad Branch Tools, which contains the Nomad Configuration Manager console extensions and Nomad OSD tools.

The format of the Nomad command-line is as follows:

```
SMSNomad.exe [switches] InstallCommandLine
```

Where InstallCommandLine is the command-line required for the target installation. For example:

```
SMSNomad.exe --wr=20 setup.exe
SMSNomad.exe msiexec.exe /i install.msi /qn
```

> **Note**
>
> The double dash is required to distinguish the Nomad command-line switches from the Configuration Manager command-line switches.

The following table shows the Nomad command-line switches and their description:

Switch	Default value	Description
--//		Use this option to enable the use of double slash arguments in the target command-line (required by *cscript.exe)*. For example, the following command-line sets *cscript* to not display its logo while running: `smsnomad.exe --// cscript.exe //Nologo`
--contentid		The content identifier.
--cp		Supported in dd-alone mode only. `--cp=CachePath` Can be used to override the cache path (destination directory) of the download. This does not support peer sharing. As the new CachePath location is not shared, peer machines will not be able to copy from this cache. This feature is suitable for protecting bandwidth when downloading to single devices. This value is set for the duration of the program. **Note** When modifying the cache path using cp the relocated cache will not be cleaned out by the cache cleaner.
--debug	9	The debug level. This value is set in the registry and is retained. 1 – minimal logging 9 – registry changes 25 – increased logging. Should only be used if requested by 1E support.
--hash		The hash for the package to download and used to verify the integrity of the package on the DP. `--hash=PackageHash`
--hf		Stands for hash first. If the package is partially available in the local cache, causes a hash check to run on it. If the hash check passes, the cached package is used and no download occurs. Since hash check runs by default on fully downloaded packages, this switch is relevant only for partially downloaded content.

Switch	Default value	Description
--inst		Causes SMSNomad to quit immediately after downloading the package, instead of waiting for the package command line to finish.
--mc		Specifies that this package may be multicast if required. If multicast is not licensed, a warning is logged and the standard peer-to-peer functionality used. This value is set for the duration of the program.
--p2p		Turns peer-to-peer communications off for the duration of the current package transfer.
--pc	1	Priority for keeping the cache. Use values between 1 (the lowest priority) and 9 (the highest priority). If 0 is specified, then the default 1 is used.
--pkgid		Package identifier for the package to download. `--pkgid=PackageID`
--pp		Sets *PackagePath* to be the directory containing the source files to be downloaded prior to installation. This value is set for the duration of the program. Supported in standalone mode only. `--pp=PackagePath` **Note** This option is required in standalone mode.
--prestage		This option enables Nomad to download a package without the need to run any executable in the package. Supported in standalone mode only. It replaces the need for a dummy program command-line, for example: "`cmd.exe /c echo nothing`"
--s		This standalone mode option should be used when running Nomad independently of Configuration Manager. The *--pp* package path option is mandatory if this option is used. This value is set for the duration of the program.
--s2		As above, however, if the package is already cached, unlike *--s*, *--s*2 will re-run the target command line.

Switch	Default value	Description
--timeout		Duration (in seconds) after which the download will time out. `--timeout=seconds`
--ver		Version of the package to download. `--ver=PackageVersion`
--wr	80	The work rate. This is the proportion of available (i.e., free) bandwidth. The range is 1 to 100, although it is not a simple percentage. This value is set for the duration of the program. If using intraday work rates and the *--wr* switch only, then the lower of the two values is used. For more details on intraday work rates. Please refer to MaxWorkRates for more details about intraday work rates.
--wro		Override the intraday work rate. When *--wro* and *--wr* are combined on the Nomad command-line then the value for the *--wr* switch will be used in preference to the intraday work rate set in the registry. If only the *--wro* switch is used, then any intraday value is overridden with a default maximum of 80%. Please refer to MaxWorkRates for more details about intraday work rates.

9.6.10.2 NomadBranch.exe command-line switches

Peer Backup Assistant (NMDS) switches

This executable does not normally need to be run on a command-line, but details are provided here for reference purposes.

It is normally installed as part of Nomad and configured using Configuration Manager Admin console extensions. Please refer to Nomad tab for different types of content. It is also available in Nomad OSD tools in order to include in WinPE images so that Nomad can be used in OS Deployments. Please refer to Installing Nomad Branch Tools.

The format of the Nomad service command-line is as follows:

```
NomadBranch.exe [switches]
```

Note

In contrast to the SMSNomad executable command-line switches, the service uses single dashes before the arguments.

Nomad service switches

Switch	Description
-cancel	Stops the current Nomad content download job immediately, which then exits with an error condition. This is intended for use by an administrator when a problem has occurred and a running job is taking an excessively long time.
-debug	Sets the debug level for the NomadBranch service where typical values are: 1=general logging, 31=maximum logging. The value is set in the registry and retained. The default is 1.
-start	Starts the *NomadBranch.exe* service.
-stop	Stops the *NomadBranch.exe* service.
-activate	Forces verification of specific content in Nomad cache. `-activate=<content_ID>`
-activateall	Forces verification of all content in Nomad cache.
-cdssync	Forces re-registration of all content with Content Distribution platform.

9.6.10.2.1 Peer Backup Assistant (NMDS) switches

NMDS commands can only be used within a Configuration Manager task sequence and must be wrapped by calling NomadPackageLocator.exe, for details refer to NomadPackageLocator.exe command-line switches. NMDS functionality requires setting and making use of task sequence variables, which is not directly supported via the *NomadBranch.exe* command. We recommend you first try the predefined Nomad custom task sequence actions available from the Configuration Manager console and failing that, use the equivalent NomadPackageLocator commands. Only use *NomadBranch.exe* NMDS commands as a last resort – they are minimally documented below for completeness.

Switch	Description
–NMDS_POLL	The NMDS_POLL argument is available on either the *NomadPackageLocator.exe* (recommended) or *NomadBranch.exe* service command-line. When run, it places a request for a network share and size associated with it. It must only be used within a task sequence.

Switch	Description
–NMDS_COMPLETE	The NMDS_COMPLETE argument is available on the *NomadPackageLocator.exe* (recommended) or *NomadBranch.exe* service argument-line. It indicates that all user data has been copied to the PBA share and the connection can be closed. When run, it disconnects from its associated share and fixes its contents for the duration defined in the Nomad PostCompleteTimeoutHours registry value on the device where the share is hosted. It is only for use within a task sequence.
–NMDS_HA	The NMDS_HA argument is available on the *NomadPackageLocator.exe* (recommended) or *NomadBranch.exe* service argument-line. It creates additional backup copies of the user data that has been copied to the PBA share, so it must be run after the share has been closed using NMDS_COMPLETE. It is only for use within a task sequence.
–NMDS_FIND	The NMDS_FIND argument is available on the *NomadPackageLocator.exe* (recommended) or *NomadBranch.exe* service argument-line. When run, it locates and connects to the share associated with it. It is only for use in a task sequence.
–NMDS_DELETE	The NMDS_DELETE argument is available on the *NomadPackageLocator.exe* (recommended) or *NomadBranch.exe* service argument-line. When run, it deletes the share, contents and user associated with the shared cache. It is only for use in a task sequence.

9.6.10.2.2 NMDS_COMPLETE

Note

Please note the:

Nomad PBA Task Sequence steps are not designed for use with offline USMT or WinPE

-NMDS_POLL command-line option for the NomadPackageLocator.exe tool cannot be used in WinPE

-NMDS_<command> command-line options for NomadBranch.exe have not been tested in WinPE, so their behavior may be unpredictable in that environment.

The NMDS_COMPLETE argument is available on the *NomadPackageLocator.exe* (recommended) or *NomadBranch.exe* service argument-line. It indicates that all user data has been copied to the PBA share and the connection can be closed. When run, it disconnects from its associated share and fixes its contents for the duration defined in the Nomad PostCompleteTimeoutHours registry value on the device where the share is hosted. It is only for use within a task sequence.

It takes the following format:

NomadPackageLocator.exe -NMDS_COMPLETE,<name>

or

NomadBranch.exe -NMDS_COMPLETE,<name>

Using the following parameter:

Parameter	Description
<name>	Used to identify the shared cache and must be the same as the one used in the NMDS_POLL argument that initially requested the share. This may be up to 40 characters, consisting of 0-9 and A-Z characters and is case-insensitive.

9.6.10.2.2.1 Locating the share

Once completed, you can locate the share with the NMDS_FIND argument; this should be done within PostCompleteTimeoutHours, which defaults to 7 days.

9.6.10.2.2.2 Task sequence environment variables

NMDS_COMPLETE uses the following task sequence environment variables:

Name	Use
%PBAComputerName%	Its value should be used for the *<name>* parameter.

9.6.10.2.3 NMDS_DELETE

Note

Please note the:

Nomad PBA Task Sequence steps are not designed for use with offline USMT or WinPE

-NMDS_POLL command-line option for the NomadPackageLocator.exe tool cannot be used in WinPE

-NMDS_<command> command-line options for NomadBranch.exe have not been tested in WinPE, so their behavior may be unpredictable in that environment.

The NMDS_DELETE argument is available on the *NomadPackageLocator.exe* (recommended) or *NomadBranch.exe* service argument-line. When run, it deletes the share, contents and user associated with the shared cache. It is only for use in a task sequence.

It takes the following format:

NomadPackageLocator.exe -NMDS_DELETE,<name>

or

NomadBranch.exe -NMDS_DELETE,<name>

Using the following parameter:

Parameter	Description
<name>	Used to identify the shared cache and should be the same as the one used in the NMDS_POLL argument that initially requested the share, i.e. the value of task sequence variable %PBAComputerName%. This may be up to 40 characters, consisting of 0-9 and A-Z characters, and is case-insensitive.

Note

If you have run NMDS_COMPLETE, run NMDS_FIND prior to NMDS_DELETE otherwise errors will be generated.

NMDS_DELETE is not essential because a share is automatically deleted after a period of time determined in PostCompleteTimeoutHours, but it is good practice to use it in order to release resources.

9.6.10.2.3.1 Task sequence environment variables

NMDS_DELETE does not use any task sequence environment variables.

9.6.10.2.4 NMDS_FIND

Note

Please note the:

Nomad PBA Task Sequence steps are not designed for use with offline USMT or WinPE

-NMDS_POLL command-line option for the NomadPackageLocator.exe tool cannot be used in WinPE

-NMDS_<command> command-line options for NomadBranch.exe have not been tested in WinPE, so their behavior may be unpredictable in that environment.

The NMDS_FIND argument is available on the *NomadPackageLocator.exe* (recommended) or *NomadBranch.exe* service argument-line. When run, it locates and connects to the share associated with it. It is only for use in a task sequence.

It takes the following format:

```
NomadPackageLocator.exe -NMDS_FIND,<name>
```

or

```
NomadBranch.exe -NMDS_FIND,<name>
```

Using the following parameter:

Parameter	Description
<name>	Used to identify the shared cache and must be the same as the one used in the NMDS_POLL argument that initially requested the share, i.e. usually the value of the %PBAComputerName% of the task sequence variable. This may be up to 40 characters, consisting of 0-9 and A-Z characters, and is case-insensitive.

9.6.10.2.4.1 Storing the result

This is not necessary if NomadPackageLocator.exe is used.

The details for the located share can be set into a variable %NMDS_REMOTE% using the TSEnv2.exe function. For example, the following argument locates the shared cache for acme1234 and sets the %NMDS_REMOTE% with the details of the located share.

```
cmd /c "NomadBranch.exe -NMDS_FIND,acme1234 | TSEnv2.exe -"
```

However, NomadPackageLocator.exe sets up task sequence environment variables automatically. The equivalent of the above argument is:

```
cmd /c "NomadPackageLocator.exe -NMDS_FIND,acme1234"
```

9.6.10.2.4.2 Deleting the share and contents

Once you have finished using the items in the share, issue the NMDS_DELETE argument to delete its contents and associated share.

9.6.10.2.4.3 Task sequence environment variables

NMDS_FIND uses the following task sequence environment variables:

Name	Use
%OSDStateStorePath%	Set to the path to the share that USMT should use for restoring migrated data.
%NMDS_REMOTE%	Set to the same value as %OSDStateStorePath%. This is deprecated, and is included for reference.

9.6.10.2.5 NMDS_HA

Note

Please note the:

Nomad PBA Task Sequence steps are not designed for use with offline USMT or WinPE

-NMDS_POLL command-line option for the NomadPackageLocator.exe tool cannot be used in WinPE

-NMDS_<command> command-line options for NomadBranch.exe have not been tested in WinPE, so their behavior may be unpredictable in that environment.

The NMDS_HA argument is available on the *NomadPackageLocator.exe* (recommended) or *NomadBranch.exe* service argument-line. It creates additional backup copies of the user data that has been copied to the PBA share, so it must be run after the share has been closed using NMDS_COMPLETE. It is only for use within a task sequence.

> **Note**
>
> If configuring PBA command lines manually and using NomadPackageLocator.exe (NOT NomadBranch.exe) to run within a task sequence environment, if the task sequence variable 1EDisablePBA_HA = True, then High Availability is disabled. This variable is automatically set for Remote WSA deployments. If using NomadBranch.exe in the command line, the variable is ignored.

It takes the following format:

```
NomadPackageLocator.exe -NMDS_HA,<min_backups>,<max_backups>,<synchronous_backups>
```

or

```
 NomadBranch.exe -NMDS_HA,<name>,<store_host>,<min_backups>,<max_backups>,<synchronous_backups>
```

Using the following parameters:

Parameter	Description
<name>	Used to identify the shared cache and must be the same as the one used in the NMDS_POLL argument that initially requested the share. The version *NomadPackageLocator.exe* gets this from task sequence environment variable *%PBAComputerName%*.
<store_host>	The name of the host where the primary copy of the user data is stored. The version *NomadPackageLocator.exe* derives this from task sequence environment variable *%OSDStateStorePath%*.
<min_backups>	The minimum number of hosts to attempt to back up the user data to. Nomad will verify that this number of hosts respond to the request, although actual copying of the user data to them all may fail. This must be at least 1 and cannot be more than the maximum number of backups. If fewer than this number of backups is successful, the task sequence step fails.
<max_backups>	The maximum number of backups to attempt. The upper limit is 6.

Parameter	Description
<synchronous_backups>	The number of synchronous backups, i.e. the number of backups for which to wait before moving on to the next action in the task sequence, to ensure that at least this quantity of backups has been successful. If any backups remain they will be run in the background in parallel with the rest of the task sequence. The value can be less than the minimum number of backups but not more than the maximum. 0 is allowed but is not advisable as there is no guarantee that any backup is successful.

The output from the NomadBranch.exe version, if successful, is a comma-separated list of the host names of the extra data stores. With *NomadPackageLocator.exe* the task sequence environment variable *%PBAHAHosts%* is set to contain the list of host names.

9.6.10.2.5.1 Task Sequence environment variables

NMDS_HA uses the following task sequence environment variables:

Name	Use
%PBAComputerName%	Used as the cache ID
%OSDStateStorePath%	The full path of the share where the user data is stored. The hostname part is used to get the name of the host where the primary copy of the user data has been stored.
%PBAHAHosts%	Set to a comma-separated list of the names of the hosts with the backup copies.

9.6.10.2.6 NMDS_POLL

Note

Please note the:

Nomad PBA Task Sequence steps are not designed for use with offline USMT or WinPE

-NMDS_POLL command-line option for the NomadPackageLocator.exe tool cannot be used in WinPE

-NMDS_<command> command-line options for NomadBranch.exe have not been tested in WinPE, so their behavior may be unpredictable in that environment.

The NMDS_POLL argument is available on either the *NomadPackageLocator.exe* (recommended) or *NomadBranch.exe* service command-line. When run, it places a request for a network share and size associated with it. It must only be used within a task sequence.

Note

If configuring PBA command lines manually and using NomadPackageLocator.exe (NOT NomadBranch.exe) to run within a task sequence environment, if the task sequence variable 1EWSA_USMTSizeInMB is set, then the value assigned to this variable is used in the poll. This variable is as part of WSA deployments if user folder backup has been enabled. If using NomadBranch.exe in the command line, the variable is ignored.

It takes the following format:

```
NomadPackageLocator.exe -NMDS_POLL,<name>,<size>
```

or

```
NomadBranch.exe -NMDS_POLL,<name>,<size>[,<ignore_offer>]
```

Using the following parameters:

Parameter	Description
<name>	Used to identify the shared cache and must be used in the rest of the PBA NMDS commands. This may be up to 40 characters, consisting of 0-9 and A-Z characters, and is case-insensitive. Subsequent calls to NMDS_POLL with the same name will return the same share details as the first call.
<size>	The number of Megabytes required for the shared cache.
<ignore_offer>	Used to specify the name of a PBA host that already has the user data cached. When NMDS_POLL is run a *second* time with the same <name> and <size> values as on the first call, it effectively allows a second PBA host to offer its services as a cache. In this way user state can be saved to two caches, for increased resilience. On restore, the first cache that responds to the NMDS_FIND request will be the one used.

9.6.10.2.6.1 Requesting a cache

When NMDS_POLL is run, the Nomad machines on the local subnet responds to the request under the following conditions:

PBA is enabled on the machine

The machine has sufficient PBA allocation to cope with the requested share size

The machine has sufficient disk space to cope with the requested share size, A machine with less than 5% available disk space cannot respond to PBA requests.

The machine has spare available connections for the share

Domain controllers cannot be used for PBA data sharing. All the machines that satisfy these conditions will respond and the requesting machine picks the host that has the largest percentage of available disk space.

9.6.10.2.6.2 Creating the cache

The winning machine creates a share and user to service the request. The share and user is maintained until:

Prior to running NMDS_COMPLETE, the timeout set in the Nomad PreCompleteTimeoutHours registry value has been reached. This defaults to 3 hours.

After running NMDS_COMPLETE, the timeout set in the Nomad PostCompleteTimeoutHours registry value has been reached. This defaults to 7 days.

The NMDS_DELETE command is issued for the <name> set in the NMDS_POLL command.

When these conditions are met, the share, contents and associated user is deleted.

> **Note**
>
> When Nomad is configured to use Peer copy over HTTP or HTTPS a file share is not created. In this scenario the storage is exposed to peers through the HTTP server implemented in Nomad for sharing its cache. A local user account is created to secure access to the migration data store through Windows authentication.
>
> When Nomad is configured to use Certificate-based Client Authentication, a local user account is not created. Access to the user state store is authenticated using a client certificate.

9.6.10.2.6.3 Storing the result

This is not necessary if *NomadPackageLocator.exe* is used.

If *NomadBranch.exe* is used, the details for the winning share can be set into a variable %NMDS_REMOTE% using the *TSEnv2.exe* function. When integrating with an OSD task sequence, the *%NMDS_REMOTE%* must be used to transfer the details to the *OSDStateStorePath* task sequence variable, otherwise the user data will not be stored on the NMDS host.

For example, the following command creates a shared cache called acme1234 with 10 Mb of disk space and sets the *%NMDS_REMOTE%* with the details of the created share.

```
cmd /c "NomadBranch.exe -NMDS_POLL,acme1234,10 | TSEnv2.exe -"
```

However, *NomadPackageLocator.exe* sets up task sequence environment variables automatically. The equivalent of the above command is simply:

```
cmd /c "NomadPackageLocator.exe -NMDS_POLL,acme1234,10"
```

9.6.10.2.6.4 Fixing the contents and disconnecting

Once created, the share will only be kept for 3 hours. When you have finished copying items to the share, issue the NMDS_COMPLETE command to disconnect from it and fix the contents for 7 days. The defaults for the pre- and post- complete timeouts are configured using the Nomad

PreCompleteTimeoutHours and PostCompleteTimeoutHours registry values on the machine where the share is being hosted.

9.6.10.2.6.5 Task sequence environment variables

NMDS_POLL uses the following task sequence environment variables:

Name	Use
%PBAComputerName%	Set to the value of the *<name>* parameter
%OSDStateStorePath%	Set to the path to the share that USMT should use for storing migrated data.
%NMDS_REMOTE%	Set to the same value as *%OSDStateStorePath%*. This is deprecated and is included for reference.

9.6.10.3 NomadPackageLocator.exe command-line switches

NomadPackageLocator.exe is used by the Nomad custom task sequence actions, we recommend that these are used to perform the appropriate functions in preference to the command-line, but details are provided here for reference purposes.

It is installed as part of Nomad. It is also available in Nomad OSD tools in order to include in WinPE images so that Nomad can be used in OS Deployments. Please refer to Installing Nomad Branch Tools.

The format of the NomadPackageLocator command-line is:

```
NomadPackageLocator.exe [options]
```

9.6.10.3.1 Nomad Package Locator general command-line switches

The following table describes the general NomadPackageLocator.exe command-line switches:

Switch	Default value	Description
Debug		Enables extra logging.
FailOverToDP		Points to the distribution point if the required package cannot be found pre-cached in any local Nomad clients.
ForceNomadMachine		Name of a specific Nomad client whose cache you want to use. This prevents *NomadPackageLocator* from polling for a Nomad client whose cache contains the content.

Switch	Default value	Description
HideErrorDialog		Suppresses error messages during the image deployment task sequence for packages that cannot be located in a Nomad cache.
HTTP		Uses HTTP to download content if it is not available on the local subnet.
Port	1779	Sets the communications port.
RemoveHttpLocations		If used on the *NomadPackageLocator.exe* command-line, the HTTP locations will be cleared from the task sequence, ensuring that the content is downloaded from Nomad peers on the local subnet.
RequireNomad		If used on the *NomadPackageLocator.exe* command-line, Nomad is used for the referenced packages. If the Nomad Package Locator fails to locate all the referenced packages, it generated an error, which is used to terminate the task sequence.
Timeout	3	Maximum wait time (in seconds) between messages. Applies to each package listed in the TS environment.

9.6.10.3.2 Nomad Package Locator NMDS command-line switches

The NMDS command are used by the Nomad Peer Backup Assistant (PBA) feature. These commands invoke *NomadBranch.exe* to do most of the work, however *NomadPackageLocator.exe* is the recommended command-line interface to use because it uses and sets crucial task sequence variables.

All of the NMDS commands have corresponding custom task sequence action dialogs, and these should be used in preference to creating command line actions.

Switch	Default value	Description
NMDS_COMPLETE		The NMDS_COMPLETE argument is available on the *NomadPackageLocator.exe* (recommended) or *NomadBranch.exe* service argument-line. It indicates that all user data has been copied to the PBA share and the connection can be closed. When

Switch	Default value	Description
		run, it disconnects from its associated share and fixes its contents for the duration defined in the Nomad PostCompleteTimeoutHours registry value on the device where the share is hosted. It is only for use within a task sequence.
NMDS_DELETE		The NMDS_DELETE argument is available on the *NomadPackageLocator.exe* (recommended) or *NomadBranch.exe* service argument-line. When run, it deletes the share, contents and user associated with the shared cache. It is only for use in a task sequence.
NMDS_FIND		The NMDS_FIND argument is available on the *NomadPackageLocator.exe* (recommended) or *NomadBranch.exe* service argument-line. When run, it locates and connects to the share associated with it. It is only for use in a task sequence.
NMDS_HA		The NMDS_HA argument is available on the *NomadPackageLocator.exe* (recommended) or *NomadBranch.exe* service argument-line. It creates additional backup copies of the user data that has been copied to the PBA share, so it must be run after the share has been closed using NMDS_COMPLETE. It is only for use within a task sequence.
NMDS_POLL		The NMDS_POLL argument is available on either the *NomadPackageLocator.exe* (recommended) or *NomadBranch.exe* service command-line. When run, it places a request for a network share and size associated with it. It must only be used within a task sequence.

9.6.10.4 TSEnv2 command-line switches

TSEnv2 is an executable that can be used primarily to set or change task sequence environment variables, including "readonly" variables, those starting with an underscore, which cannot be changed with ConfigMgr's tsenv.exe tool. It also has other related functions, some of which can be performed by the NomadPackageLocator tool, refer to NomadPackageLocator.exe command-line switches for details.

TSEnv2 is installed as part of Nomad and is available with the Nomad OSD tools, so it can be included in WinPE images allowing Nomad to be used in OS Deployments, refer to Installing Nomad Branch Tools for details.

The command-line format is:

```
TSEnv2.exe [switch]
```

Where *switch* is one of the switches in the table below.

Note

There is no '-' or '/' before the switch.

Switch	Description
dump [file]	Write a binary dump of the TS variables to a file. If no file name is given, the default is *C:\tsenv2.out*.
find name	Test whether the specified variable exists and has a non-empty value. If so, the return code is *0*, otherwise it is *0x80070490 (2147943568)* which corresponds to *ELEMENT_NOT_FOUND*.
get name	Get the name of the specified variable and output it in the form.*name=value* The return code is *0* if the variable exists and has a non-empty value, otherwise it is *0x80070490 (2147943568)* which corresponds to *ELEMENT_NOT_FOUND*.
get_b64 name	Like *get* but also decodes the variable if it is in base-64 format. (Encoded values start with "eJ".) **Note** If the resulting data is not valid text and cannot be written as such, *TSEnv2* creates a binary dump file and specifies the path in its output.
get_b64z name	Like *get* but also decodes the variable if it is in base-64 format (encoded values start with "eJ") and uncompresses the result. **Note** If the resulting data is not valid text and cannot be written as such, *TSEnv2* creates a binary dump file and specifies the path in its output.
list	Outputs every variable in the form *name=value* with one name-value pair per line.
listblk	Like *list* but uses a different block-based technique. The result is always be the same.
listx	Like *list* but base-64 encoded variables (encoded values start with "eJ") are also decoded and uncompressed.
set name=value	Creates or changes the named variable using the specified value. Values up to 2954 characters are supported. If the value contains embedded whitespace or quote characters, enclose the entire *name=value* text in quotes and double the

Switch	Description
	quote characters, for example: *TSEnv2.exe set "embedded=some text and a couple of ""quotes"""* will result in setting variable *embedded* to *some text and a couple of "quotes"* **Note** Task sequence variables that start with an underscore ("_") are intended to be read-only. These may still be changed using, *TSEnv2* but exercise caution when changing values.

9.6.10.5 CacheCleaner.exe command-line switches

CacheCleaner is an executable that can be used to explicitly purge the Nomad cache. By default, the Nomad cache is not purged unless there is an active download. In most cases, available disk space is not really an issue, but there may be circumstances where you may want to manage the cache to keep the disk usage overhead to a minimum. Please refer to Cache management for further information about managing the cache.

It is installed as part of Nomad and the format of the command-line is:

```
CacheCleaner.exe -switch
```

Where *switch* is one of the following (case sensitive):

Switch name	Default value	Range	Description
-CachePriority	1	1-9	Only cache contents with a priority equal to or lower than the *CachePriority* are purged. Used in conjunction with *Pkgsize* to emulate the behavior of the cache cleaner when an actual package is being downloaded.
-Debug			Sets the debug level for *CacheCleaner* and it can be passed on the command-line. If it is not, the value from Nomad registry is used. If Debug is already defined, using this argument adds to the logging level.
-Deleteall			Deletes all cache content where the priority is less than or equal to the value for Force. If the command-line does not include *Force* , then *Deleteall* deletes all cache content where the priority is 1. Works in conjunction with the *Force* .

Switch name	Default value	Range	Description

-DeletePkg			The ID of the package or content to be deleted from the cache. The value must be set to the PackageID or ContentID string that identifies the content to be deleted. Must be used in conjunction with *PkgVer*.
			
			`-DeletePkg=PRI0000A -PkgVer=*`
			
			`-DeletePkg=Content_9b9ccd56-9fbf-4587-98e7-725fcfa8e70f -PkgVer=*`

-Force			Content whose cache priority is less than or equal to the *CachePriority* value are purged. Used in conjunction with the *Deleteall* and *MaxCacheAge*.
-MaxCacheAge		1-1461	The maximum number of days before the contents of a cache is purged. If set, *CacheCleaner* deletes cache contents which are older than this value. This argument is ignored if *DeletePkg* and *Deleteall* is used on the command-line. If the command-line includes *Force*, all caches with a priority less than or equal to *CachePriority* will have their content purged. If *CachePriority* is not included on the command-line, all caches with a priority=1 will have their content purged.
-PercentAvailableDisk	10	1-99	Deletes the lowest cache priority content until the set percentage of available disk is available.
-Pkgsize			Only caches with a priority equal to or lower than the *CachePriority* value will have their contents purged. Used in conjunction with *CachePriority* to emulate the behavior of the cache cleaner when an actual package is being downloaded. Determine the space to be cleared when running *cachecleaner.exe* with *PercentAvailableDisk*. The *PkgSize* value is by default specified in bytes but can be set to MB by appending MB to the value.

Switch name	Default value	Range	Description

			For example, the following are equivalent:
			
			`-Pkgsize=1048576`
			`-Pkgsize=1MB`

-PkgVer			Identifies the content version to be deleted and must be used in conjunction with *DeletePkg*. Deletes content from both the Nomad and Configuration Manager client caches that corresponds to the version number and the Package ID (or Content ID). The special value -PkgVer=* may be used when the user is unsure of the specific version of the package in the cache. **Note** Setting -PkgVer=* will delete any version of the content with the ID specified in the DeletePkg argument from the Nomad cache only – it will not delete from the Configuration Manager client cache. **Note** If you want to remove A*pplication or Software Updates content*, then the -PkgVer will usually need to be set to "1".

Note

If the Nomad cache is deleted while another client is accessing it, the other client will recover by downloading directly from the DP. This is by design and ensures recovery occurs in order to complete a successful download.

9.6.10.5.1 CacheCleaner examples

In the following examples, there is no requirement to specify the path to CacheCleaner.exe because the path to Nomad executables is set in the PATH environment variable:

Example	Description
Set the cache cleaner to run as a Configuration Manager program.	You can set the cache cleaner to run as a Configuration Manager program and advertise it to all Nomad systems in a single operation. You can also schedule this as a regular housekeeping job, ensuring that the cache is kept under control automatically. To purge the cache when the total free disk space is at 20% run: `CacheCleaner.exe –PercentAvailableDisk=20`
Ensure that content in the cache is not kept for more than 30 day.	To ensure that content in the cache is not kept for more than 30 days, run: `CacheCleaner.exe –MaxCacheAge=30`
Delete a particular package and version.	To delete a particular package and version, run: `CacheCleaner.exe –DeletePkg=L0A00001 –PkgVer=1`
Purge the contents of a cache with a priority of 3 or lower.	To purge the contents of a cache with a priority of 3 or lower, run: `CacheCleaner.exe –DeleteAll -Force=3`
Purge the contents of a cache with a particular priority and size.	To purge the contents of a cache with a particular priority and size, run: `CacheCleaner.exe –PkgSize=10485760 –CachePriority=6`

9.6.11 Nomad installer properties

Subject-oriented lists of Nomad installer properties. There are two Nomad installers that have usable installer properties: **1E.Client-x64.msi** (and its x86 version) and **NomadBranchAdminUIExt.msi**.

9.6.11.1 1E Client installer properties for the Nomad client module

The following headings describe the Nomad client installer properties associated with each particular area of functionality available in Nomad:

> **Note**
>
> You must use UPPERCASE when specifying the *name* of any installer property in a **mst** transform file, and preferably when including them in a msiexec command-line.
>
> Names of settings stored in the configuration file are not case-sensitive. Setting names stored in the registry may be case-sensitive and should be specified as shown.

Settings that have numeric values must be set using decimal integers, unless otherwise specified.

9.6.11.1.1 Nomad client installation settings

Nomad client installation settings exist in the 1E Client configuration file, and not in the registry. They can be specified during installation of the 1E Client as Windows installer properties, and therefore must be specified in upper-case. Settings that exist in the 1E Client configuration file can be mixed-case, and can be reconfigured after installation using 1E Client command-line parameters.

Module.Nomad.Enabled

9.6.11.1.2 Basic Nomad configuration

MODULE.NOMAD.COMPATIBILITYFLAGS, MODULE.NOMAD.DEBUG, MODULE.NOMAD.GENERATEWEREVENTS, MODULE.NOMAD.LOGNAME, MODULE.NOMAD.LOGPATH, MODULE.NOMAD.MAXLOGSIZE, MODULE.NOMAD.P2PENABLED, MODULE.NOMAD.MAXSTUCKCOUNT, MODULE.NOMAD.P2PDISQUALIFYMAXNUMPEERS, MODULE.NOMAD.P2PDISQUALIFYMAXWINDOWMINS, MODULE.NOMAD.P2PPORT, MODULE.NOMAD.P2PHTTPPORT, MODULE.NOMAD.P2PHTTPSPORT, MODULE.NOMAD.SPECIALNETSHARE

9.6.11.1.3 Peer backup assistant

The following properties relate to the PBA functionality:

MODULE.NOMAD.CACHEPATH, MODULE.NOMAD.ENFORCEQUOTAS, MODULE.NOMAD.HAACKTIMEOUTMINS, MODULE.NOMAD.MAXALLOCREQUEST, MODULE.NOMAD.MAXCONCURRENCY, MODULE.NOMAD.MAXIMUMMEGABYTE, MODULE.NOMAD.POSTCOMPLETETIMEOUTHOURS, MODULE.NOMAD.PRECOMPLETETIMEOUTHOURS, MODULE.NOMAD.SSPBAENABLED

9.6.11.1.4 Connection and download

The following installer properties relate to configuring the connection Nomad uses to download packages:

MODULE.NOMAD.BLOCKSIZE, MODULE.NOMAD.DOWNLOADTIMEOUT, MODULE.NOMAD.MAXPACKAGEFAST, MODULE.NOMAD.MAXPACKAGERAS, MODULE.NOMAD.MAXPACKAGESLOW, MODULE.NOMAD.PERMITUNCACHED, MODULE.NOMAD.WLANBLIPSECS, MODULE.NOMAD.WLANPROFILELIST

9.6.11.1.5 Nomad cache

MODULE.NOMAD.AUTHENTICATEDUSERS, MODULE.NOMAD.CACHECLEANCYCLEHRS, MODULE.NOMAD.MAXCACHEDAYS, MODULE.NOMAD.MAXCACHESIZEMB, MODULE.NOMAD.MAXPRECACHEDAYS, MODULE.NOMAD.MAXSUCACHEDAYS, MODULE.NOMAD.NOHARDLINK, MODULE.NOMAD.NOMADINHIBITEDADSITES, MODULE.NOMAD.NOMADINHIBITEDSUBNETS, MODULE.NOMAD.PERCENTAVAILABLEDISK

9.6.11.1.6 Internet facing client

MODULE.NOMAD.CERTISSUER, MODULE.NOMAD.CERTSUBJECT

9.6.11.1.7 Distribution point related

MODULE.NOMAD.DPNOTAVAILABLECODES, MODULE.NOMAD.PERMITTEDLSZSHARES, MODULE.NOMAD.RECYCLEDPDELAY, MODULE.NOMAD.SIGSFOLDER

9.6.11.1.8 Status messages

MODULE.NOMAD.MAXSTATUSFREQUENCY, MODULE.NOMAD.STATUSMSGEVENTS

9.6.11.1.9 Single site download and Nomad pre-caching features

Common: MODULE.NOMAD.CONTENTREGISTRATION, MODULE.NOMAD.MAXDEVICESFROMAE, MODULE.NOMAD.PLATFORMURL

SSD: MODULE.NOMAD.SSDENABLED

9.6.11.1.10Multicast

MODULE.NOMAD.MADCAPSCOPE, MODULE.NOMAD.MAXPACKETSPERSECOND, MODULE.NOMAD.MULTICASTSUPPORT

9.6.11.2 NomadBranchAdminUIExt installer properties

There is only one value that is of use in the NomadBranchAdminUIExt registry that defines the location of the Tachyon Platform Server for use with the Nomad Pre-caching feature: PlatformURL

9.6.11.3 Nomad client alphabetic installer properties

The following table shows the supported installer properties for the Nomad client module of the 1E Client.

> **Note**
>
> Each installer property listed below has a link to its corresponding registry value page.

9.6.11.3.1 Nomad client settings

> **Note**
>
> You must use UPPERCASE when specifying the *name* of any installer property in a **mst** transform file, and preferably when including them in a msiexec command-line.
>
> Names of settings stored in the configuration file are not case-sensitive. Setting names stored in the registry may be case-sensitive and should be specified as shown.
>
> Settings that have numeric values must be set using decimal integers, unless otherwise specified.

Installer property	Description
Module.Nomad.Enabled	Set this property to **true** to enable the Nomad client module. The default value is **false**.

Installer property	Description
	Note If enabled, when the 1E Client starts, it will attempt to automatically remove any previous installations of Nomad Branch. This setting does not have an associated Nomad registry entry and is stored in the 1E Client configuration file.
MODULE.NOMAD.AUTHENTICATEDUSERS	Determines which of the built-in security groups is granted read-only permissions to the Nomad cache.

Registry value	Default value	Notes
AuthenticatedUsers	1	Grants read-only access to the Nomad cache as follows: 0 – Everyone built-in security group and the *SMSNomadP2P&* Nomad share account. This is the least restrictive option and is not valid with HTTP or HTTPS protocol and is treated as 2 (only the *SMSNomadP2P&* Nomad share account) 1 – Authenticated Users built-in security group and the *SMSNomadP2P&* Nomad share account 2 – Only the *SMSNomadP2P&* Nomad share account. This account has also been added to NTFS permission settings. Unauthorised HTTP requests to access the caches are met with a 403 status code. The Nomad share has more information about share permissions and NTFS security. The difference between Authenticated Users and Everyone depends on the OS version, but in general Everyone includes Authenticated Users plus Guest.

Installer property	Description
MODULE.NOMAD.BLOCKSIZE	Value (in bytes) for the minimum size of each block of data Nomad copies from the package source folder. Click here to expand... Value (in bytes) for the minimum size of each block of data Nomad copies from the package source folder. **Note** Any change to this value requires a manual service restart before it can take effect. #### *9.6.11.3.1.1 BlockSize* Value (in bytes) for the minimum size of each block of data Nomad copies from the package source folder. **Note** Any change to this value requires a manual service restart before it can take effect.

Registry value	Default value	Notes	Installer property
BlockSize	131072(128KB)	Must be between 4096(4KB) to 4194304(4MB) inclusive. The default block size is 128KB The maximum block size is 4MB Multicast environments can only use the default block size. If you define a larger value for multicast environments, Nomad	MODULE.NOMAD.BLOCKSIZE

Installer property	Description
	automatically resets it to the default. Clients use the block size defined in the registry and ignore the values from the LSZ

The Dynamic Block Size (DBS) feature increases block size on high-bandwidth links to get maximum efficiency, and reduces it on low-bandwidth links to reduce the impact. Using DBS, Nomad is able to automatically decide the appropriate block size for a given link bandwidth and also adjust it as needed during the download if the link conditions change. As a result, Nomad is far more efficient and faster on all types of connection bandwidths while retaining its minimal impact on other link traffic.

Note

DBS is enabled or disabled by configuring Bit 25 in the CompatibilityFlags registry. Setting Bit 25 disables DBS and clearing Bit 25 enables DBS.

In Nomad 7.0 onwards, the DBS feature is turned off by default for new installations, and not changed for upgrades.

Prior to v6.3 the default value of BlockSize registry setting was 32KB (0x8000). From v6.3 onwards the default is 128KB (0x20000).

The installer automatically sets this to 128KB for both fresh installs and upgrades from previous versions. The only exceptions to this are:

It will use the specified value if the BLOCKSIZE property is used in the installation command line or in a MST transform, when doing a fresh install or upgrade

It will retain the previous value of BLOCKSIZE if it was set to anything other than 32KB (the older default), when doing an upgrade.

Registry value	Default value	Notes
BlockSize	131072(128KB)	Must be between 4096(4KB) to 4194304(4MB) inclusive.

Installer property	Description
	The default block size is 128KB The maximum block size is 4MB Multicast environments can only use the default block size. If you define a larger value for multicast environments, Nomad automatically resets it to the default. Clients use the block size defined in the registry and ignore the values from the LSZ
	The Dynamic Block Size (DBS) feature increases block size on high-bandwidth links to get maximum efficiency, and reduces it on low-bandwidth links to reduce the impact. Using DBS, Nomad is able to automatically decide the appropriate block size for a given link bandwidth and also adjust it as needed during the download if the link conditions change. As a result, Nomad is far more efficient and faster on all types of connection bandwidths while retaining its minimal impact on other link traffic. **Note** DBS is enabled or disabled by configuring Bit 25 in the CompatibilityFlags registry. Setting Bit 25 disables DBS and clearing Bit 25 enables DBS. In Nomad 7.0 onwards, the DBS feature is turned off by default for new installations, and not changed for upgrades. Prior to v6.3 the default value of BlockSize registry setting was 32KB (0x8000). From v6.3 onwards the default is 128KB (0x20000). The installer automatically sets this to 128KB for both fresh installs and upgrades from previous versions. The only exceptions to this are: It will use the specified value if the BLOCKSIZE property is used in the installation command line or in a MST transform, when doing a fresh install or upgrade It will retain the previous value of BLOCKSIZE if it was set to anything other than 32KB (the older default), when doing an upgrade.
MODULE.NOMAD.CACHECLEANCYCLEHRS	Determines the number of hours between automatically running the Nomad cache cleaner. Click here to expand...

Installer property	Description

Determines the number of hours between automatically running the Nomad cache cleaner.

Registry value	Default value	Notes
CacheCleanCycleHrs	0 (turned off)	The first automatic cache clean runs randomly between 10 to 60 mins of service start up. Subsequent cache clean cycles run after the number of hours specified. 0 means feature turned off. No cache cleaning cycle would run. Changing this registry entry performs an internal restart. The minimum value is 4. The maximum value is 168 (Once a week) Please refer to Cache management for details about other cache management settings.

MODULE.NOMAD.CACHECLEANSUBNETLOOKUP

If enabled, sets the cache clean subnet lookup.

Click here to expand...

If enabled, sets the cache clean subnet lookup.

Registry value	Type	Default value	Notes
CacheCleanSubnetLookup	REG_DWORD	1	Before deleting content, Nomad checks if it is on any other client in the same subnet, and will only delete local content if the same is present on at least one other client on the same subnet.

Installer property	Description
	To disable subnet lookup, set the value to 0. Its value can be 0 or 1. The default value is 1, subnet lookup is enabled. New setting introduced in 8.0. Please refer to Cache management for details about other cache management settings.
MODULE.NOMAD.CACHEPATH	Determines the value of : NomadBranch\LocalCachePath - the location of local Nomad package cache Click here to expand LocalCachePath... The location of local Nomad package cache.

Registry value	Default value	Notes
LocalCachePath	%ALLUSERSPROFILE%\1E\NomadBranch\	There are two registry values called LocalCachePath that are used by Nomad. The LocalCachePath REG_SZ registry value under the HKLM\Software\1E\NomadBranch key sets the path to the local Nomad package cache. The LocalCachePath REG_SZ registry value under the HKLM\Software\1E\NomadBranch\NMDS key sets the path to the PBA package cache.

Installer property	Description
	The path is created if it does not exist. If the drive letter does not exist, and it is not possible to create the specified path, *%TEMP%* is used. Default values are dependent on OS. **Known issue fixed in latest accumulated hotfix** The value for the installer property CACHEPATH requires a trailing backslash \. When Nomad is installed on a DP this location is also used for the LSZFiles vDir folder. If LocalCachePath does not contain a trailing backslash, then: the LSZFILES folder is incorrectly created (LocalCachePathLSZFILES instead of LocalCachePath\LSZFILES) IIS vDIR points to wrong folder (LocalCachePathLSZFILES instead of LocalCachePath\LSZFILES) LSZGEN fails because it is attempting to store LSZ files to non-existent path (LocalCachePath\LSZFILES) PBA cache is also derived from the same installer property MODULE.NOMAD.CACHEPATH, but it is stored in the registry value> CachePath in the NomadBranch\NMDS registry key.

Installer property	Description
	NomadBranch\NMDS\CachePath - the location of the base peer backup assistant (PBS) share where user data is copied to Click here to expand CachePath... This value holds the location of the base peer backup assistant (PBS) share where user data is copied to. Registry value: CachePath Default value: <NomadCachePath>\NMDS Notes: This REG_SZ registry value is found under the PBA registry key NomadBranch\NMDS. This parameter relies on the folder it points to as being configured as a share. In normal circumstances, this should not be modified from the default value. The MODULE.NOMAD.CACHEPATH installer property also used to configure the location of the Nomad cache, which is stored in the registry value LocalCachePath. The location of the PBA cache is derived from the MODULE.NOMAD.CACHEPATH property, and is stored in the registry value CachePath in the NomadBranch\NMDS registry key.
MODULE.NOMAD.CACHESTATESYNCINTERVALMINUTES	Ensures the cache state of a device held on ContentDistribution is in sync with locally held data. This setting controls the **Content Registration Sync Cycle** feature.

Installer property	Description

Registry value	Default value	Notes
CacheStateSyncIntervalMinutes	1440 (1day)	Range: from 60 to 525600 (1Year).

The **Content Registration Sync Cycle** is available in the following versions of 1E Client, where the Nomad client registers pending and failed content registrations with ActiveEfficiency or Tachyon Platform. Please refer to Single Site Download: Improved resilience of content registration.

Nomad 8.0 in 1E Client 5.2 - uses Content Distribution in Tachyon Platform

Nomad 7.1 in 1E Client 5.2 - uses Content Distribution in Tachyon Platform

Nomad 7.0.200 in 1E Client 5.1 - uses ActiveEfficiency

Nomad 7.0.100 in 1E Client 5.0 - uses ActiveEfficiency

Nomad 7.0 in 1E Client 4.1 - uses ActiveEfficiency

MODULE.NOMAD.CERTISSUER

Defines one or more certificate issuers that Nomad will use to select the appropriate PKI certificate for the:

Configuration Manager (CM) client authentication certificate - used when downloading over HTTPS from Distribution Points and when communicating with Management Points during pre-caching

Nomad Server Authentication certificate - used to share content between peers over HTTPS

Client Authentication certificate - used for certificate-based client authentication when sharing content between peers over HTTPS.

In most cases Nomad will be able to identify a suitable certificate in the Local Computer Personal certificate store without needing to specify CertIssuer (refer to Peer copy over HTTP or HTTPS: Certificate Selection for more details). You should use CertIssuer if the CM client is not using PKI certificates and there are multiple Client Authentication certificates issued by different Certificate Authorities in the store, and if there is a chance some of those certificates may not be trusted by other peers or CM site systems.

Click here to expand...

Installer property	Description

Defines one or more certificate issuers that Nomad will use to select the appropriate PKI certificate for the:

Configuration Manager (CM) client authentication certificate - used when downloading over HTTPS from Distribution Points and when communicating with Management Points during pre-caching

Nomad Server Authentication certificate - used to share content between peers over HTTPS

Client Authentication certificate - used for certificate-based client authentication when sharing content between peers over HTTPS.

In most cases Nomad will be able to identify a suitable certificate in the Local Computer Personal certificate store without needing to specify CertIssuer (refer to Peer copy over HTTP or HTTPS: Certificate Selection for more details). You should use CertIssuer if the CM client is not using PKI certificates and there are multiple Client Authentication certificates issued by different Certificate Authorities in the store, and if there is a chance some of those certificates may not be trusted by other peers or CM site systems.

Registry value	Default value	Notes
CertIssuer	" "	Set this value to the name of the certificate issuer (Certificate Authority (CA)) that Nomad should use to select the appropriate PKI certificate. A case-insensitive substring-within-a-string match is performed. If you have multiple CAs you can specify a: Common sub-string (e.g. "CORPCA" would work for certificates issued by CORPCA1 or CORPCA2) Comma-separated list of certificate issuers (both exact names or substrings are acceptable values). For example, "DigiCert,Thawte,Verisign" would work for certificates issued by DigiCert, DigiCert EV, Thawte or Verisign. If you are only using HTTPS for downloading from an HTTPS DP (That is, not using HTTPS for peer-to-peer

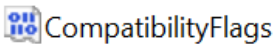
Installer property	Description
	data transfer) you can leave this blank and set CertSubject instead.
MODULE.NOMAD.CERTSUBJECT	Defines one or more certificate subject names that Nomad uses to select the appropriate PKI certificate for authentication with Configuration Manager (CM) site systems configured to use HTTPS. It does not affect certificate selection for client authentication certificates used for peer-to-peer authentication or for selection of server authentication certificates. In most cases Nomad will be able to identify a suitable certificate in the Local Computer Personal certificate store without the need to specify CertSubject (refer to Peer copy over HTTP or HTTPS: Certificate Selection for more details). Click here to expand... Defines one or more certificate subject names that Nomad uses to select the appropriate PKI certificate for authentication with Configuration Manager (CM) site systems configured to use HTTPS. It does not affect certificate selection for client authentication certificates used for peer-to-peer authentication or for selection of server authentication certificates. In most cases Nomad will be able to identify a suitable certificate in the Local Computer Personal certificate store without the need to specify CertSubject (refer to Peer copy over HTTP or HTTPS: Certificate Selection for more details).

Registry value	Default value	Notes
CertSubject	" "	For downloads over HTTPS from the Distribution Point, set either the CertIssuer or CertSubject registry values. Set this value to the subject name of the certificate that Nomad should use to select the appropriate PKI certificate. The match has the following properties: case-insensitive a substring search is done, so if the text is set to ACME it will return certificates where ACME appears anywhere in the certificate's subject.

Installer property	Description
	If you have multiple valid subject names you can specify a: Common sub-string, for example "contoso.com" would work for certificates that have contoso.com anywhere in the subject name Comma-separated list of subject names or sub-strings, for example, you can specify multiple subject domain suffixes, for example "contoso.com,abc.in". For the installer property, configure either MODULE.NOMAD.CERTISSUER or MODULE.NOMAD.CERTSUBJECTinstaller properties for HTTPS downloads.
MODULE.NOMAD.COMPATIBILITYFLAGS	Determines different compatibility settings which relate to specific customer related functionality and should not generally be changed from the default value under normal conditions, unless advised.The installer property must be set to sum of the integer values for the required bits. For example, to disable hash value checking (1) and DelegatedLSZ checks and errors (131072), run *`msiexec /i 1E.Client-x64.msi MODULE.NOMAD.COMPATIBILITYFLAGS=131073 [other properties] /qn`* on the installer command-line. Click here to expand... Determines different compatibility settings which relate to specific customer related functionality and should not generally be changed from the default value under normal conditions, unless advised.

Registry value	Default value	Notes
CompatibilityFlags	0x1E18000A (504889354)	For Nomad in full OS, the registry value is set to the sum of the values for the required bits. CompatibilityFlags REG

Installer property	Description
	The default value combines the following settings: *Bit 1 - 0x00000002* - Enable longer values for hashes *Bit 3 - 0x00000008* - Fix wrong IPs in election messages *Bit 19 - 0x00080000* - Enable full hash generation for SIS content on DPs *Bit 20 - 0x00100000* - Abort download on the Nomad client if an LsZ has mismatch is detected *Bit 25 - 0x02000000* - Turn off Dynamic Block Size *Bit 26 - 0x04000000* - Enable download of Windows 10 Express File Updates *Bit 27 - 0x08000000* - Enable download of Software Updates (including Windows 10 feature updates) from Microsoft Update - see note *Bit 28 - 0x10000000* - Enable support for byte-range downloads (e.g. Office 365 or delta content for updates) from Microsoft Update - see note First bit is bit 0. The default in binary is: 0001 1110 0001 1000 0000 0000 0000 1010 **Support for downloading updates from Microsoft Update** Setting bits 27 and/or 28 will enable Nomad to download content from Microsoft Update if the update has been deployed with Configuration Manager and the option

Installer property	Description
	If software updates are not available on distribution point in current, neighbor or site boundary, download content from Microsoft Update has been enabled on the Download Settings tab of the deployment. Nomad will not be used to download updates from Microsoft Update if the update is requested outside of a Configuration Manager Software Update Deployment (e.g. when using Windows Update for Business). **Note** Prior to 1E Client 4.1 (Nomad 7.0) the default was 0x00180000 (1572864): *Bit 19 - 0x00080000* - Enable full hash generation for SIS content on DPs *Bit 20 - 0x00100000* - Abort download on the Nomad client if an LsZ has mismatch is detected
0x00100002 (1048578)	For the task sequence action **Install and configure Nomad in Windows PE**, the registry value is set to the sum of the values for the required bits.  The default value combines the following settings:

Installer property	Description
	Bit 1 - 0x00000002 - Enable longer values for hashes *Bit 20 - 0x00100000* - Abort download on the Nomad client if an LsZ has mismatch is detected **Note** *Bit 1 - 0x00000002* (Enable longer values for hashes) is mandatory. The installer property must be set to sum of the values for the required bits, and given in decimal notation. For example, the following installer command-line uses: *Default- 0x1E18000A* *Bit 0 - 0x00000001* - Never check hashes of downloaded content *Bit 17 - 0x00020000* - Disable DelegatedLSZ checks and errors *Sum - 0x1E1A000B* (505020427) `> msiexec /i 1E.Client-x64.msi MODULE.NOMAD.COMPATIBILITY`

Installer property	Description

```
FLAGS=505020427 [ot
her properties] /qn
```

Bit	Hex	Decimal	Description
0	*0x0001*	1	Never check hashes of downloaded content.
1	*0x0002*	2	Enable longer values for hashes. This value is auto-enabled when the Configuration Manager client is detected. You must manually configure this setting on any DP that does not have the Configuration Manager client installed. **Note** Prior to 1E Client 4.1 (Nomad 7.0) this was disabled (0) by default.
2	*0x0004*	4	Calculate CRCs as files are downloading.
3	*0x0008*	8	Fix wrong IPs in election messages. On multi-homed machines sometimes the IP from a wrong adapter can get sent in the election messages resulting in peers failing to connect to the master. Enabling this flag causes Nomad to correct such IPs at the time when messages are received and thus prevent master connectivity issues.
4	*0x0010*	16	Determines compatibility with Nomad v3.x caches. Set this option once all Nomad v3.x installations have been upgraded.
5	*0x0020*	32	Disable all RDC data generation.

Installer property	Description			
	6	*0x0040*	64	Keep Packages that failed the CRC test during P2P or download from DP.
	7	*0x0080*	128	Prevent computers using wireless connections from becoming fill-in multicast masters.
	8	*0x0100*	256	Include LinkLocal IPv4 addresses.
	9	*0x0200*	512	Include LinkLocal IPv6 addresses.
	11	*0x0800*	2048	RESERVED
	12	*0x1000*	4096	Do not automatically jump from HTTP to HTTPS during download from DP.
	13	*0x2000*	8192	Always use HTTPS. (Use this setting when Configuration Manager is configured to use HTTPS-only communication for downloading content from Distribution Points)
	14	*0x4000*	16384	RESERVED
	15	*0x8000*	32768	RESERVED
	16	*0x00010000*	65536	RESERVED (this flag is no longer used; previously this flag disabled a workaround for the issue described in Nomad post-installation tasks: IIS request filtering)
	17	*0x00020000*	131072	Disable DelegatedLSZ checks and errors.
	18	*0x00040000*	262144	Disable partial download when App-V streaming, i.e. download entire application.
	19	*0x00080000*	524288	Enable full hash generation for SIS content when an LsZ file is generated on a DP. If this is not enabled, SIS content is trusted,

Installer property	Description			
				and corrupted content may be downloaded. Enabled by default.
	20	*0x00100000*	1048576	Abort download on the Nomad client if an LsZ hash mismatch is detected. If this is not set, when a Nomad client detects a hash mismatch it will re-request LsZ generation on the DP then try again, and get stuck in a loop if the SIS content is corrupt. Must be set on clients if Bit 19 is set on DPs. Enabled by default.
	25	*0x02000000*	33554432	Turn off Dynamic Block Size. This flag is set by default, which means Dynamic Block Size is disabled by default. **Note** Prior to 1E Client 4.1 (Nomad 7.0) this bit was off, meaning **Dynamic Block Size** was enabled by default.
	26	*0x04000000*	67108864	Enable download of Windows 10 Express update files. Enabled by default. **Note** This is a new setting in 1E Client 4.1 (Nomad 7.0) and Q20144 for NomadBranch 6.3.201.
	27	*0x08000000*	134217728	Enable download of full file software updates from Microsoft Update when deployed through Configuration Manager. Enabled by default. **Note** This is a new setting in 1E Client 4.1 (Nomad 7.0) and Q20246 for NomadBranch 6.3.201.
	28	*0x10000000*	268435456	Enable download of byte-range software updates (e.g. Express updates, O365

Installer property	Description			
				updates) from Microsoft Update when deployed through Configuration Manager. Enabled by default. **Note** This is a new setting in 1E Client 4.1 (Nomad 7.0) and Q20246 for NomadBranch 6.3.201.
	30	*0x40000000*	1073741824	Enable SoftwareUpdate metadata validation. This is not enabled by default. It can be used to resolve rare issues related to SoftwareUpdates where the contents could be updated without any change in its ID or version. Please refer to Resolving SoftwareUpdate metadata validation for more details. **Note** This is a new setting in 1E Client 5.1 (Nomad 7.0.200).
MODULE.NOMAD.CONTENTPROVIDERONWIFI	Determines whether a device on a WLAN can become content provider. By default, only devices connected to a LAN can become content providers when using Single Site Download (SSD). **Note** This setting is only applicable to SSD and has no effect on P2P content transfers on the local subnet. Click here to expand... Determines whether a device on a WLAN can become content provider. By default, only devices connected to a LAN can become content providers when using Single Site Download (SSD). **Note** This setting is only applicable to SSD and has no effect on P2P content transfers on the local subnet.			

Installer property	Description

Registry value	Default value	Notes
ContentProviderOnWifi	0	Values are: 0 – Only devices connected to a LAN can be content providers 1 – Devices connected to any network (including WLANs) can be content providers

MODULE.NOMAD.CONTENTREGISTRATION

Determines if content in Nomad's cache (packages, applications, software updates, boot images, etc.) is registered with Content Distribution. Content registration is necessary if a host is to be available as a Single Site Download (SSD) provider or can be woken up if a Nomad peer requires the content locally.

Click here to expand...

Determines if content in Nomad's cache (packages, applications, software updates, boot images, etc.) is registered with Content Distribution. Content registration is necessary if a host is to be available as a Single Site Download (SSD) provider or can be woken up if a Nomad peer requires the content locally.

Registry value	Default value	Notes
Platform\ContentRegistration	0	To enable content registration, update the value to 1 – it is found under the Platform\ContentDistribution To enable SSD when you install Nomad, you must specify the MODULE.NOMAD.SSDENABLED installer property and ensure the Tachyon client is enabled by specifying SWITCH and BACKGROUNDCHANNELURL installer properties. If MODULE.NOMAD.SSDENABLED is specified during installation, the

Installer property	Description
	registry value of ContentRegistration is automatically set to 1. If you want to enable SSD as a provider after installation, then you also need to configure the registry values for SSDEnabled and ContentRegistration, in addition to enabling the Tachyon client. The ContentDistribution registry setting is found under the Platform key. Nomad app provides visibility of content distribution activity Single Site Download (SSD) Single Site Peer Backup Assistant (SSPBA) High Availability Peer Backup Assistant (HAPBA) Get Migration Settings task sequence action used to manage computer associations Nomad Pre-caching Nomad Download Pause. In legacy versions of Nomad, Platform features were provided using ActiveEfficiency. This required the PlatformURL setting to be configured. This is no longer required. You will see that the PlatformURL registry is used, but this is configured automatically by Nomad on startup by querying the value that the Tachyon client is using (stored in the 1EClient.conf file).

Installer property	Description
MODULE.NOMAD.DEBUG	The level of messages logged in the Nomad logs for debugging purposes. The installer property must be set to sum of the integer values for the required bits. For example, to set all three supported debug levels, run: *`msiexec /i 1E.Client-x64.msi MODULE.NOMAD.DEBUG=25 [other properties] /qn`* on the installer command-line. Click here to expand... The level of messages logged in the Nomad logs for debugging purposes.

Registry value	Default value	Notes
Debug	0x09 (9)	See the table below for customer supported values. The default is a combination of *`0x01`* (Minimal logging) and *`0x08`* (Registry changes). For example, to set maximum debugging, set bit 0, 3 and 4, which is a value of 0x19 hexadecimal or 25 decimal. Values on the installer command-line must be provided in decimal. So to set maximum debugging you would use the following installer command-line: `> msiexec /i 1E.Client-x64.msi DEBUG=25 [other properties] /qn`

Bit	Hex	Decimal	Description
0	0x01	1	Minimal logging.
1	0x02	2	RESERVED
2	0x04	4	RESERVED
3	0x08	8	Registry changes.
4	0x10	16	Additional debugging (should only be used if requested by 1E support).

Installer property	Description
MODULE.NOMAD.DOREPORTINGENABLED	Enables Delivery Optimization monitoring and reporting if ContentRegistration is enabled. Click here to expand... Enables Delivery Optimization monitoring and reporting if ContentRegistration is enabled. Registry value: DeliveryOptimizationReportingEnabled Default value: 0 Notes: Enables monitoring of Delivery Optimization downloads and reporting them to Tachyon Platform (ContentDistribution). Delivery Optimization monitoring and reporting is only supported in versions of Windows Server 2019 and Windows 10 Version 1909 onwards. When it is enabled, DO download events get written to .etl files in the Nomad cache folder, for example: NomadDo-20210325-182415.etl. And aggregated information about the downloads gets writtern to sqlite files **Do.db** and **DoDownloadMonitor.db** in LocalDb folder inside Nomad cache folder.

Installer property	Description
MODULE.NOMAD.DOWNLOADTIMEOUT	Sets the timeout in seconds after which a job will be cancelled if the download has not been successful. Click here to expand... Sets the timeout in seconds after which a job will be cancelled if the download has not been successful. Registry value: DownloadTimeout Default value: 0 Notes: This parameter is associated with the distribution point resilience feature and is used in conjunction with the *RecycleDPDelay* registry value. If a value greater than zero is set, the download timeout will either use this or the Configuration Manager setting depending on which is the smaller value. When the timeout is reached, the job package download is cancelled and a success is sent to the Configuration Manager client with the *ERROR_MAXDURATION* timeout error sent as the package status message. The default is to use the Configuration Manager setting (28 days by default).
MODULE.NOMAD.DPCACHECLEANUPENABLED	Delete all obsolete LSZ files on the DP where the associated content is no longer present in ContentLib. Click here to expand... Delete all obsolete LSZ files on the DP where the associated content is no longer present in ContentLib.

Installer property	Description

Registry value	Default value	Notes
DpCacheCleanupEnabled	0 (turned off)	This entry controls the cached LSZ files cleaning feature. When turned on, this feature deletes all LSZ files in a Distribution Point (DP) cache where the associated content is not present in ContentLib. The following table describes the values this entry may be set to: Value: 0 — The feature is turned off. This is the default. Value: 1 (or greater) — The feature is turned on. Please refer to Cache management for details about other cache management settings.

MODULE.NOMAD.DPNOTAVAILABLECODES

Determines which error codes will cause Nomad to retry a download using an alternative distribution point.

For example, the following would set Nomad to the default value on the 1E Client installer command-line:`> msiexec /i 1E.Client-x64.msi MODULE.NOMAD.DPNOTAVAILABLECODES="0x205A,0x205D" [other properties] /qn`

Click here to expand...

Determines which error codes will cause Nomad to retry a download using an alternative distribution point.

Installer property	Description			
	Registry value	Default value	Notes	
	DPNotAvailableCodes	0x205A, 0x205D	This registry entry contains a comma-separated list of return codes, see Nomad return codes for a list of the possible ones. If Nomad encounters one of these during download it will attempt a retry from an alternative DP. It gets the list of possible DPs from Configuration Manager. The two return codes set as default are the only ones that are applicable to DP availability: 0x205A – in valid special package path (set using *--pp*) 0x205D – DP path not found Under normal circumstances, you would not change this from the default value. You may want to not allow failover to an alternative DP altogether, in which case you would set the value to " " in the registry. Or you may only want to failover if the DP path was not found, in which case you would set the value to 0x205D only. This installer property should be set to a string containing the comma-separated hex values. For example the following sets Nomad to failover to the next DP only when the DP path was not found: *> msiexec /i 1E.Client-x64.msi DPNOTAVAILABLECODES="0x205D" [other properties] /qn*	
MODULE.NOMAD.ENFORCEQUOTAS	Determines whether Windows Disk Quotas (if configured) are enforced on the PBA share defined inCachePath. Click here to expand...			

Installer property	Description

Determines whether Windows Disk Quotas (if configured) are enforced on the PBA share defined in CachePath.

Registry value	Default value	Notes
EnforceQuotas	0x0 (0)	Enables quotas to be enforced but requires Windows Disk Quotas to be configured. If the size specified in the NMDS_POLL request causes the quota to be exceeded, the request fails and you get disk full error. This registry value is found under the PBA registry key NomadBranch\NMDS.

MODULE.NOMAD.GENERATEWEREVENTS

Determines whether Windows Error Reporting memory dumps should be sent to Microsoft Winqual.

Click here to expand...

Determines whether Windows Error Reporting memory dumps should be sent to Microsoft Winqual.

Registry value	Default value	Notes
GenerateWEREvents	1	If enabled and if Nomad experiences an unexpected failure, a dialog is displayed prompting the user to send the debug information to Winqual which is forwarded to 1E for continued quality improvements. Values are: 0 disables this feature 1 enables this feature

MODULE.NOMAD.HAACKTIMEOUTMINS

The time-out period in minutes for the Peer Backup Assistant - High Availability (deprecated) (PBA-HA) task sequence action. If a machine running this action does not receive an acknowledgement message within this period from the PBA host performing the additional backups, the action will fail.

Click here to expand...

Installer property	Description

The time-out period in minutes for the Peer Backup Assistant - High Availability (deprecated) (PBA-HA) task sequence action. If a machine running this action does not receive an acknowledgement message within this period from the PBA host performing the additional backups, the action will fail.

Registry value	Default value	Notes
HAACKTimeoutMins	20	Applies to synchronized backups only. The PBA tost sends the acknowledgement messages back to the machine running the task sequence approximately every 5% of the synchronized copy. This registry value is found under the PBA registry key NomadBranch\NMDS.

MODULE.NOMAD.LOCALSSDSTAGGER

Sets the site SSD query stagger duration (seconds).

Click here to expand...

Sets the site SSD query stagger duration (seconds).

Deployments to large numbers of clients (30,000 or more) generate significant network traffic from 1E Client to Content Distribution that may result in IIS 503 Overload errors on the server, causing content registrations and SSD requests to fail. LocalSsdStagger allows an elected subnet master to wait for a random configurable time before making a local SSD request. All peers in the subnet participating in the election would also synchronize and wait for the same time before copying from master machine.

Registry value	Type	Default value	Notes
LocalSsdStagger	REG_DWORD	5	Sets the local SSD query stagger duration in seconds. The stagger is 0 (disabled) by default. The maximum value that can configured is 600 seconds (10 minutes).

Installer property	Description
	There is no SSD staggering in WinPE. Local SSD happens when only when network broadcast is disabled. **Note** Please consult 1E before changing this value. This setting works in conjunction with SiteSsdStagger.
MODULE.NOMAD.LOGNAME	Name of the Nomad log file. This value is preserved upon upgrade. This property is combined with MODULE.NOMAD.LOGPATH to create registry value LogFileName. The default value is *NomadBranch.log*
MODULE.NOMAD.LOGPATH	Location of the Nomad log file. The path will be created if it does not exist. This value is preserved upon upgrade. Default values are dependent on OS. This property is combined with MODULE.NOMAD.LOGNAME to create the registry value LogFileName. The default location is: *%ALLUSERSPROFILE%\1E\NomadBranch\LogFiles*
MODULE.NOMAD.MADCAPSCOPE	The MADCAP scope for multicast. Click here to expand... The MADCAP scope for multicast. **Warning** The Multicast feature is not supported in the Tachyon 5.2 release. This feature is under consideration for re-design and may be available in future versions of Nomad.

Registry value	Default value	Notes
MultiCastMADCAPScope	SMSNomad	Values may be set using either of the formats in the table below.

Installer property	Description

Format	Description
<ScopeName>	*<ScopeName>* is the name of a scope defined in the DHCP (if you are using the Microsoft implementation of MADCAP). Use this format if you have multiple MADCAP servers. This method uses the time to live settings for the scope.
<MADCAP_ServerIP> *<MADCAP_Scope_IP>* *<TTL>*	*<MADCAP_ServerIP>* is the IP address of a specific MADCAP server *<MADCAP_ScopeIP>* is the starting IP address for a MADCAP scope defined in the DHCP (if you are using the Microsoft implementation of MADCAP) *<TTL>* is the time to live for the multicast packets **Note** Using a TTL greater than 1 is not recommended unless you have ensured that multicast traffic cannot leak back upstream through any intervening routers. The valid range for TTL is a number between 1 and 255 Nomad is also capable of performing control multicast without a MADCAP server installation on the network. In order to use this feature, the *<MADCAP_ServerIP>* must be set to *0.0.0.0*. For example, the following supports MADCAP server not being present, with a scope of *239.0.9.0* and a time to live of *3*. `0.0.0.0,239.0.9.0,3`

MODULE.NOMAD.MAXALLOCREQUEST	Sets the maximum amount of space in MB that can be requested by each PBA client. Click here to expand...

Installer property	Description

Sets the maximum amount of space in MB that can be requested by each PBA client.

Registry value	Default value	Notes
MaxAllocRequest	0xC8 (200)	Located under the PBA registry key NomadBranch\NMDS.

MODULE.NOMAD.MAXCACHEDAYS

When the Nomad cache cleaner runs, delete any application or package content that last triggered Nomad elections before the specified number of days ago.

Click here to expand...

When the Nomad cache cleaner runs, delete any application or package content that last triggered Nomad elections before the specified number of days ago.

Registry value	Default value	Notes
MaxCacheDays	0 (turned off)	Set to delete application or package content that last triggered Nomad elections before the specified number of days from the date the cache cleaner runs. This ensures that only application or package content that have triggered elections recently will be kept in the cache. 0 means that application and package content will not be deleted automatically when the cache cleaner runs. Please refer to Cache management for details about other cache management settings.

MODULE.NOMAD.MAXCA

This is the maximum number of days content is present on a client.

Click here to expand...

<table>
<tr><th>Installer property</th><th>Description</th></tr>
<tr><td>CHEDAYSTHRESHOLD</td><td>This is the maximum number of days content is present on a client.
<table>
<tr><th>Registry value</th><th>Type</th><th>Default value</th><th>Notes</th></tr>
<tr><td>MaxCacheDaysThreshold</td><td>REG_DWORD</td><td>0</td><td>This is the maximum number of days content is present on a client. If it's not zero, then content will be deleted without any other checks once it reaches the threshold. If the threshold has a value greater than zero and less than 30, Nomad uses the threshold of 30 days and creates an associated log.

Default value is 0.

New setting introduced in 8.0.

Please refer to Cache management for details about other cache management settings.</td></tr>
</table></td></tr>
<tr><td>MODULE.NOMAD.MAXCACHESIZEMB</td><td>Provided for backward compatibility only – use PercentAvailableDisk instead. The value (in bytes) for the maximum size the cache is allowed to grow to, before automatic cache cleaning takes place.

Click here to expand...

Provided for backward compatibility only – use PercentAvailableDisk instead. The value (in bytes) for the maximum size the cache is allowed to grow to, before automatic cache cleaning takes place.</td></tr>
</table>

Installer property	Description

Registry value	Default value	Notes
MaxCacheSizeMB	0	There is no maximum value for this property. This method for determining the maximum size of the cache is an alternative to PercentAvailableDisk: If PercentAvailableDisk has a value greater than zero set its method will be used to control the cache size. If MaxCacheSizeMB is set to a value greater than zero and PercentAvailableDisk is set to zero thenMaxCacheSizeMB will be used as the method for determining the maximum size of the Nomad cache.

MODULE.NOMAD.MAXCONCURRENCY

Sets the maximum number of concurrent PBA sessions that may be in use on the host.

Click here to expand...

Sets the maximum number of concurrent PBA sessions that may be in use on the host.

Registry value	Default value	Notes
MaxConcurrency	0x3 (3)	Located under the PBA registry key NomadBranch\NMDS.

MODULE.NOMAD.MAXDEVICESFROMAE

The maximum number of devices with the content that Nomad can retrieve from Content Distribution in one call.

Click here to expand...

The maximum number of devices with the content that Nomad can retrieve from Content Distribution in one call.

Installer property	Description

Registry value	Default value	Notes
MaxDevicesFromAE	10	The maximum number of devices (i.e. machines) with the content (package, application or software update) that Nomad can retrieve from Content Distribution in one call. The maximum value is 20.

MODULE.NOMAD.MAXELECTIONRESPONSELOGGING

Defines the number of election responses Nomad will write to the log for a given election.

Click here to expand...

Defines the number of election responses Nomad will write to the log for a given election.

Registry value	Default value	Notes
MaxElectionResponseLogging	By default this REG_DWORD value is not present and all election responses are logged.	Add this REG_DWORD value and set it to the number of responses that Nomad should log for any given election. Setting the value to 0 effectively turns off logging of any election responses.

Note

The value of MaxElectionResponseLogging specifies the number of election replies to be logged per election request. As an example, if MaxElectionResponseLogging = 5 and there are two election requests for the same package at different times, a maximum of 5 election responses will be logged for each elections (up to 10 election replies in total). If there are two concurrent election requests for the same package, the number of maximum election replies logged may vary from 5 to 10. In general, if MaxElectionResponseLogging = *n* and if there are *m* concurrent election requests for the same package, the number of maximum election replies logged may vary from *n* to *m***n*.

Installer property	Description
MODULE.NOMAD.MAXIMUMMEGABYTE	The maximum amount of space (in MB) that can be used for all the PBA shares combined on the host. Click here to expand... The maximum amount of space (in MB) that can be used for all the PBA shares combined on the host. Registry value: MaximumMegaByte Default value: 0 Notes: A non-zero value enables PBA share. This registry value is located under the PBA registry key NomadBranch\NMDS.
MODULE.NOMAD.MAXLOGSIZE	The maximum size (in bytes) of the Nomad log file. Default is 5MB. Click here to expand... The maximum size (in bytes) of the Nomad log file. Default is 5MB. Registry value: MaxLogFileSize Default value: 5242880 Notes: When the log file reaches this size, it is renamed with a *.LO_* extension and a new *.LOG* file is created. The *.LO* file is overwritten each time. **Note** The default has been increased from 1048576 (1MB) to 5242880 (5MB) for Nomad 7.0 onwards (1E Client 4.1). **Note** The installer property name is different to the registry name.
MODULE.NOMAD.MAXPACKAGEFAST	The maximum size (in bytes) of a package that Nomad attempts to cache on a Fast LAN (>500 kbps) connection. Click here to expand...

Installer property	Description
	The maximum size (in bytes) of a package that Nomad attempts to cache on a Fast LAN (>500 kbps) connection. Registry value: MaxPackageSizeFastLAN Default value: 0 Notes: Works in conjunction with the RunUncachedPermittedFastLAN registry value. **Note** The installer property name is different to the registry name.
MODULE.NOMAD.MAXPACKAGERAS	The maximum size (in bytes) of a package that Nomad will attempt to cache on a RAS (<55 kbps) connection. Click here to expand... The maximum size (in bytes) of a package that Nomad will attempt to cache on a RAS (<55 kbps) connection. Registry value: MaxPackageSizeRAS Default value: 0 Notes: **Note** The installer property name is different to the registry name.
MODULE.NOMAD.MAXPACKAGESLOW	Maximum size (in bytes) of a package that Nomad attempts to cache on a Slow LAN (55-500 kbps) connection. Click here to expand... Maximum size (in bytes) of a package that Nomad attempts to cache on a Slow LAN (55-500 kbps) connection.

Installer property	Description

Registry value	Default value	Notes
MaxPackageSizeSlowLAN	0	**Note** The installer property name is different to the registry name.

MODULE.NOMAD.MAXPACKETSPERSECOND

The maximum rate at which multicast packets are sent.

Click here to expand...

The maximum rate at which multicast packets are sent.

Warning

The Multicast feature is not supported in the Tachyon 5.2 release. This feature is under consideration for re-design and may be available in future versions of Nomad.

Registry value	Default value	Notes
MaxPacketsPerSecond	800	Modify this value with caution. If packets are sent too fast, machines will drop packets and multicast will not be effective - too slow and multicast works, but slowly. The default value is indicative of how this should be set.

MODULE.NOMAD.MAXPRECACHEDAYS

When the Nomad cache cleaner runs, delete any pre-cached content that last triggered Nomad elections before the specified number of days ago.

Click here to expand...

When the Nomad cache cleaner runs, delete any pre-cached content that last triggered Nomad elections before the specified number of days ago.

Installer property	Description

Registry value	Default value	Notes
MaxPreCacheDays	0 (turned off)	Set to delete pre-cached content that last triggered Nomad elections before the specified number of days from the date the cache cleaner runs. This ensures that only pre-cached content that has triggered elections recently will be kept in the cache. 0 means that pre-cached content will not be deleted automatically when the cache cleaner runs. Please refer to Cache management for details about other cache management settings.

MODULE.NOMAD.MAXSTATUSFREQUENCY

he minimum interval (in seconds) between sending transfer progress status messages, thereby governing the overall maximum frequency for sending the messages.

Click here to expand...

he minimum interval (in seconds) between sending transfer progress status messages, thereby governing the overall maximum frequency for sending the messages.

Registry value	Default value	Notes
MaxStatusFrequency	3600	Works in conjunction with the ++sm setting on the Nomad properties tab and the StatusMsgEvents registry values.

MODULE.NOMAD.MAXSTUCKCOUNT

Registry value to hold an integer determining the number of times Nomad attempts to copy content and gets stuck before aborting.

Click here to expand...

Installer property	Description

Registry value to hold an integer determining the number of times Nomad attempts to copy content and gets stuck before aborting.

If you update the registry, you must restart the Nomad service for you changes to take effect. We recommend backing up your registry before you do this.

Registry value	Default value	Notes
MaxStuckCount	100	The number of times Nomad attempts to copy content after failure (such as network outages, incomplete LSZ files, hash mismatches, election issues, connecting with peers) before it aborts the operation. The range is 3 to 1000, but if the value is less than 3 or greater than 1000, it sets to the default of 100. **Warning** The MaxStuckCount value is an internal NomadBranch registry value. You should not change this value unless advised by 1E.

Do not use unless advised by 1E.

MODULE.NOMAD.MAXSUCACHEDAYS

When the Nomad cache cleaner runs, delete any software updates that last triggered Nomad elections before the specified number of days ago.

Click here to expand...

When the Nomad cache cleaner runs, delete any software updates that last triggered Nomad elections before the specified number of days ago.

Registry value	Default value	Notes
MaxSUCacheDays	0 (turned off)	Set to delete software updates that last triggered Nomad elections before the

Installer property	Description
	specified number of days from the date the cache cleaner runs. This ensures that only software updates that have triggered elections recently will be kept in the cache. 0 means that software updates will not be deleted automatically when the cache cleaner runs. Please refer to Cache management for details about other cache management settings.
MODULE.NOMAD.MULTICASTSUPPORT	The behavior of local multicast. Click here to expand... The behavior of local multicast. **Warning** The Multicast feature is not supported in the Tachyon 5.2 release. This feature is under consideration for re-design and may be available in future versions of Nomad.

Registry value	Default value	Notes
MulticastSupport	0x0 (0)	All machines in a single branch must be configured using the same value for this parameter. If you are not using multicast, deploy the Nomad branch agent with the MULTICASTSUPPORT property set to 0 to reduce the noise in Nomad logs. Prior to Nomad 7.0 multicast was enabled (0x1) by default. Now it is disabled (0x0) by default.

Installer property	Description

Bit	Hex	Decimal	Description
	0x0	0	**No Multicast**– disables the feature.
0	0x1	1	**Data Only Multicast** – choose this for a standard Nomad multicast. Data refers to the content of the downloaded package. Nomad control communications are broadcast as normal on the local subnet. Select this option for standard functionality.
1	0x2	2	**Control Only Multicast** – control information refers to the communications between Nomad enabled machines, especially for elections. This may be used if there is more than one subnet in a single location to enable a single Nomad master to be elected for all the subnets.
	0x3	3	**Control and Data Multicast** – data and control information is multicast. Select this option if a branch has multiple subnets connected by high speed routers.

MODULE.NOMAD.NOHARDLINK

Determines whether hard links are used between the Nomad cache and the Configuration Manager cache.

Click here to expand...

Determines whether hard links are used between the Nomad cache and the Configuration Manager cache.

Registry value	Default value	Notes
NoHardlink	0	Values are:

Installer property	Description
	0 – hard links are used. The Nomad cache will link to the Configuration Manager cache so only a single copy of a package is held locally. 1 – hard links are not used and results in the content being double-cached For more detail about the Nomad Cache please refer to Nomad cache.
MODULE.NOMAD.NOMADINHIBITEDADSITES	Prevents Nomad from calling an election when it is connected to a specified AD site, meaning that each Nomad client on the listed AD sites will automatically become a Nomad master. This prevents P2P sharing, as each master downloads its own copy of the content. Click here to expand... Prevents Nomad from calling an election when it is connected to a specified AD site, meaning that each Nomad client on the listed AD sites will automatically become a Nomad master. This prevents P2P sharing, as each master downloads its own copy of the content.

Registry value	Default value	Notes
NomadInhibitedADSites	(empty)	A comma-separated list for each AD site to be inhibited. Useful for sites with: a local DP a VPN without isolation For example, to inhibit three AD sites called site1, site2 and site3: `site1,site2,site3` Please refer to Design Considerations: Inhibiting subnets and sites.

Installer property	Description
MODULE.NOMAD.NOMAD	Prevents Nomad from calling an election when it is connected to a specified IP subnet, meaning that each Nomad client on the IP subnet automatically

Installer property	Description
INHIBITEDSUBNETS	becomes a Nomad master. This prevents P2P sharing, as each master downloads its own copy of the content. Click here to expand... Prevents Nomad from calling an election when it is connected to a specified IP subnet, meaning that each Nomad client on the IP subnet automatically becomes a Nomad master. This prevents P2P sharing, as each master downloads its own copy of the content. Registry value: NomadInhibitedSubnets Default value: (empty) Notes: A comma-separated list of each subnet to be inhibited in CIDR notation. Useful for sites with either of the following: a local DP a VPN without isolation For example, to isolate two subnets: `10.2.0.0/16,192.168.9.0/24` Please refer to Design Considerations: Inhibiting subnets and sites.
MODULE.NOMAD.P2PDISQUALIFYMAXNUMPEERS	Defines the max number of devices which a device will disqualify during a peer-to-peer copy. Click here to expand... Defines the max number of devices which a device will disqualify during a peer-to-peer copy. If you update the registry, you must restart the Nomad service for you changes to take effect. We recommend backing up your registry before you do this. Registry value: P2PDisqualifyMaxNumPeers Default value: 5 Notes: A device does not further disqualify a peer if it has disqualified

Installer property	Description
	P2PDisqualifyMaxNumPeers number of peers within last P2PDisqualifyMaxWindowMins minutes. **Warning** The P2PDisqualifyMaxNumPeers value is an internal NomadBranch registry value. You should not change this value unless advised by 1E. Do not use unless advised by 1E.
MODULE.NOMAD.P2PDISQUALIFYMAXWINDOWMINS	Defines the max number of minutes within which a device will disqualify a peer during a peer-to-peer copy. Click here to expand... Defines the max number of minutes within which a device will disqualify a peer during a peer-to-peer copy. If you update the registry, you must restart the Nomad service for you changes to take effect. We recommend backing up your registry before you do this.

Registry value	Default value	Notes
P2PDisqualifyMaxWindowMins	60	A device does not further disqualify a peer if it has disqualified P2PDisqualifyMaxNumPeers number of peers within last P2PDisqualifyMaxWindowMins minutes. **Warning** The P2PDisqualifyMaxWindowMins value is an internal NomadBranch registry value. You should not

Installer property	Description
	change this value unless advised by 1E. Do not use unless advised by 1E.
MODULE.NOMAD.P2PENABLED	Determines how the Nomad cache is accessed. Please refer to Nomad cache for more details. The installer property must be set to sum of the integer values for the required bits. For example, the following would set Nomad to use connectionless P2P on the 1E Client installer command-line: *> msiexec /i 1E.Client-x64.msi MODULE.NOMAD.P2PENABLED=6 [other properties] /qn* Click here to expand... Determines how the Nomad cache is accessed. Please refer to Nomad cache for more details.

Registry value	Default value	Notes
P2PEnabled	9	The default (Hex 0x0009) configures P2P to use SMB and Net Literal Names. You can set more than one option at the same time by combining the bit values. See the table below for details. **Note** We recommend restarting the Nomad Branch service when you modify this parameter.

Bit	Hex	Decimal	Notes
0	0x0001	1	(Default) Use the SMB protocol to share its own cache, and create the NomadSHR file share upon the start of the Nomad service, unless the CustomShare option has been enabled in SpecialNetShare. When

Installer property	Description			
				P2PEnabled is set in addition to Bit 5 (use HTTP) or Bit 6 (use HTTPS), Nomad will attempt to use HTTPS/HTTP and will fall-back to SMB if HTTPS/HTTP is unavailable on other peers. To disable SMB P2P, set this bit to 0.
		1	0x0002	2	Enable connectionless P2P server.
		2	0x0004	4	Enable connectionless P2P client.
		3	0x0008	8	(Default) Use Net Literal Names when connecting to P2P shares. This causes Nomad to use the Nomad master's IP address when connecting to the share and is recommended when running wirelessly.
		4	0x0010	16	Use FQDN when connecting to P2P shares. Recommended when using a multi-forest environment where computers from different forests may be present in the same subnet. This requires that reverse lookup for IP addresses is correctly configured and running. If this is not available Nomad will revert to using the IP address for connecting to the P2P shares.
		5	0x0020	32	Use the HTTP protocol to share its own cache and access other caches.
		6	0x0040	64	Use the HTTPS protocol to share its own cache and access other caches.
MODULE.NOMAD.P2PHTTPPORT	The HTTP port to use for peer copy. Click here to expand... The HTTP port to use for peer copy.				

Installer property	Description

Registry value	Default value	Notes
P2PHttpPort	5080	Default HTTP port to use for peer copy. If you are using a custom port, ensure that all agents use the same custom port.

MODULE.NOMAD.P2PHTTPSPORT

The HTTPS port to use for peer copy.

Click here to expand...

Registry value	Default value	Notes
P2PHttpsPort	5443	Default HTTPS port to use for peer copy. If you are using a custom port, ensure that all agents use the same custom port.

MODULE.NOMAD.P2PPORT

Port used to broadcast election messages, for connectionless cache access and package status broadcasts.

Click here to expand...

Port used to broadcast election messages, for connectionless cache access and package status broadcasts.

Registry value	Default value	Notes
P2P_Port	1779	

MODULE.NOMAD.P2PSSLSETTINGS

Defines server and client authentication options when using HTTPS for P2P content transfer (i.e. P2PEnabled 0x60 option is set).

Click here to expand...

Defines server and client authentication options when using HTTPS for P2P content transfer (i.e. P2PEnabled 0x60 option is set).

Installer property	Description

Registry value	Default value	Notes
P2PSslSettings	0	The default value (0) configures Nomad to use a self-signed certificate for server authentication and disables certificate-based client authentication. P2PSslSettings is a numeric value where, when represented in binary, each bit represents a configurable option as defined in the table below. You can combine these options to derive the required value, for example setting P2PSslSettings to 3 (0x1 + 0x2) configures Nomad to use a PKI certificate for server authentication and also enables certificate-based authentication. These options are only applicable if the HTTPS protocol has been enabled in the P2PEnabled setting. If you are using PKI certificates you must deploy the certificates to all clients before enabling this option. Refer to Peer copy over HTTP or HTTPS for further details on using HTTPS and associated authentication.

Bit	Hex	Decimal	Notes
0	0x0001	1	If not set (0), use self-signed certificate for server (Master) authentication If set (1), use PKI certificate for server (Master) authentication
1	0x0002	2	Enables certificate-based client authentication (Requires a PKI client authentication certificate)

Note

Installer property	Description
	If this option is enabled and the Configuration Manager client is using self-signed client authentication certificates (or Nomad is being used outside of CM), you should specify CertIssuer to ensure Nomad uses the intended certificate.
MODULE.NOMAD.PERCENTAVAILABLEDISK	The limit on the Nomad cache. Specified as a percentage of the available disk space, it controls the automatic cache cleaning to ensure that the cache does not grow to a size whereby the percentage of available disk space is less than this value. Click here to expand... The limit on the Nomad cache. Specified as a percentage of the available disk space, it controls the automatic cache cleaning to ensure that the cache does not grow to a size whereby the percentage of available disk space is less than this value.

Registry value	Default value	Notes
PercentAvailableDisk	10	By default, the cache will not grow such that less that #UUID146b7586a8d378aba88bc74a4d10ae9110 % of total disk space is available. The maximum value is 80. The cache will not grow beyond 20% of the total available disk space. This method for determining the maximum size of the cache is provided as an alternative to MaxCacheSizeMB: If PercentAvailableDisk is greater than zero, its method is used to control the cache size IfMaxCacheSizeMB is greater than zero and PercentAvailableDisk is zero, then MaxCacheSizeMB is used as the method for determining the maximum size of the Nomad cache.

Installer property	Description
MODULE.NOMAD.PERMITTEDLSZSHARES	Restricts Nomad LSZ file generation requests to a list of permitted package source locations. Click here to expand... Restricts Nomad LSZ file generation requests to a list of permitted package source locations.

Registry value	Default value	Notes
PermittedLSZShares	SMSPKG*$ SMS_DP_SMSPKG*$	A list of comma-separated package source locations. Enables increased security and is only used by the Nomad client installed on a distribution point. Nomad LSZ file generation requests will only be completed if the content location is listed. If you are using additional package source locations, you must manually add these to this registry value. *PermittedLSZShares* can incorporate wildcard characters to provide flexible naming convention support. If you leave the registry value blank, security checks on package source locations are not carried out. **Note** When Configuration Manager (specifically Distribution Point servers) is configured to use HTTPS only, you must also add *NOCERT_SMS_DP_SMSPKG*$* and CCMTOKENAUTH_SMS_DP_SMSPKG*$ to the PermittedLSZShares registry value.

Installer property	Description
MODULE.NOMAD.PERMITUNCACHED	Determines where the download package is run from under certain conditions. Click here to expand... Determines where the download package is run from under certain conditions.

Registry value	Default value	Notes
RunUncachedPermittedFastLAN	0	Works in conjunction with MaxPackageSizeFastLAN (which needs to contain a value value greater than zero). Values are: 0 – do not run package from the distribution point. 1 – run package directly from the distribution point if there is either insufficient disk space to create the cache, or the maximum package threshold is exceeded but the connection is fast (>500kbps). To ensure that the un-cached mode works correctly, set the Program Environment Properties to include the Drive mode/Require drive letter option.

MODULE.NOMAD.PLATFORMURL	The URL of the Tachyon Platform, specifically the Tachyon Background Channel, which provides a reverse proxy for the Content Distribution component of Tachyon Platform. Usually of the form *https://<BackgroundChannelServer>:<BackgroundChannelPort>/Background/* Click here to expand... **Note**

Installer property	Description

Platform features are now enabled by using the BackgroundChannelUrl instead of PlatformURL.

The URL of the Tachyon Platform, specifically the Tachyon Background Channel, which provides a reverse proxy for the Content Distribution component of Tachyon Platform. Usually of the form *https://<BackgroundChannelServer>:<BackgroundChannelPort>/Background/*

Registry value	Default value	Notes
PlatformURL	(empty)	Located under the following registry keys, depending on the component. For *NomadBranch*, it is found under *HKLM\Software\1E\NomadBranch\Platform* For *NomadBranchAdminUIExt* on 64-bit machines, it is found under *HKLM\Software\Wow6432Node\1E\NomadAdminUI\Platform* For *NomadBranchAdminUIExt* on 32-bit machines, it is found under *HKLM\Software\1E\NomadAdminUI\Platform* **Warning** Do not configure this registry setting, it is automatically configured on service startup. To enable SSD when you install Nomad, you must specify the MODULE.NOMAD.SSDENABLED installer property and ensure the Tachyon client is enabled by specifying SWITCH and BACKGROUNDCHANNELURL installer properties. If MODULE.NOMAD.SSDENABLED is specified during installation, the registry value of ContentRegistration is automatically set to 1. If you want to enable SSD as a provider after installation, then you also need to configure the registry values for SSDEnabled and ContentRegistration, in addition to enabling the Tachyon client. The

Installer property	Description
	ContentDistribution registry setting is found under the Platform key. Nomad app provides visibility of content distribution activity Single Site Download (SSD) Single Site Peer Backup Assistant (SSPBA) High Availability Peer Backup Assistant (HAPBA) Get Migration Settings task sequence action used to manage computer associations Nomad Pre-caching Nomad Download Pause. In legacy versions of Nomad, Platform features were provided using ActiveEfficiency. This required the PlatformURL setting to be configured. This is no longer required. You will see that the PlatformURL registry is used, but this is configured automatically by Nomad on startup by querying the value that the Tachyon client is using (stored in the 1EClient.conf file).
MODULE.NOMAD.POSTCOMPLETETIMEOUTHOURS	The duration (in hours) after which the PBA share is deleted from the host. Click here to expand... The duration (in hours) after which the PBA share is deleted from the host.

Registry value	Default value	Notes
PostCompleteTimeoutHours	0xA8 (168)	Only applies to a PBA share after the NMDS_COMPLETE command has been run for it, otherwise the PreCompleteTimeoutHours value will apply. The intention is that an incomplete share will only be available for a short period of time,

Installer property	Description
	defined in PreCompleteTimeoutHours. Once the NMDS_COMPLETE command is sent, it will be fixed for this longer time. When the share is deleted the folder and associated user will be removed. This registry value is found under the PBA registry key NomadBranch\NMDS.
MODULE.NOMAD.PRECACHEPOLLBATCHSIZE	The number of notifications a client processes in one pre-cache poll cycle. Click here to expand... The number of notifications a client processes in one pre-cache poll cycle. Registry value: PrecachePollBatchSize Default value: 20 Notes: Range is 1 to 500. If the value is greater than 500, it defaults to 500. If you set the value to 0, it defaults to 20.
MODULE.NOMAD.PRECACHEPOLLMINUTES	The interval (in minutes) between Nomad polling Content Distribution for new pre-cache jobs. Click here to expand... The interval (in minutes) between Nomad polling Content Distribution for new pre-cache jobs. Registry value: PrecachePollMinutes Default value: 0x5A0 (1440) Notes: Nomad clients normally start their polling cycle when the service starts-up, with a random delay to minimize the possibility of concurrent polls from different clients.

Installer property	Description
	The range is 60 - 525600 (1 year). 0 disables polling
MODULE.NOMAD.PRECOMPLETETIMEOUTHOURS	The duration (in hours) after which PBA share is deleted from the host. Click here to expand... The duration (in hours) after which PBA share is deleted from the host.

Registry value	Default value	Notes
PreCompleteTimeoutHours	0x3 (3)	Located under the PBA registry key NomadBranch\NMDS, it only applies to a PBA share after the NMDS_POLL command has been run, but not the NMDS_COMPLETE command. The intention is that an incomplete share will only be available for a short period of time. When the share is deleted the folder and associated user is removed.

Installer property	Description
MODULE.NOMAD.RECYCLEDPDELAY	The delay (in seconds) before restarting retries from the first DP after the whole list of available DPs have been tried. Click here to expand... The delay (in seconds) before restarting retries from the first DP after the whole list of available DPs have been tried.

Registry value	Default value	Notes
RecycleDPDelay	600	It is associated with the distribution point resilience feature and is used in conjunction with DownloadTimeout. The default equates to 10 minutes.

Installer property	Description
MODULE.NOMAD.RANDOMIZEREMOTEPATHS	Allows you to enable and disable the remote paths randomization for CM and pre-cache jobs. Click here to expand... Allows you to enable and disable the remote paths randomization for CM and pre-cache jobs. When Nomad begins content download, its content is pulled from the same distribution point by every client. For example, If a site has four Distribution Points (DP), the first one in the list is always used for downloading. In a very large environment, this can put an unnecessary load on a single DP. Using**RandomizeRemotePaths**Nomad can randomize the content location list.

Registry value	Type	Default value	Notes
RandomizeRemotePaths	REG_DWORD	0	By default, RandomizeRemotePaths is not present in the Nomad registry hive. To change the value, you need to create it and set your desired value. You can enable and disable the remote paths randomization for either Configuration Manager (CM) or pre-cache jobs using the following bits:

Bit	Hex	Decimal	Notes
0	0x0001	1	Enable remote paths randomization for CM jobs.

Installer property	Description				
		1	0x0002	2	Enable remote paths randomization for Pre-cache jobs.

MODULE.NOMAD.SIGSFOLDER

The path to the Configuration Manager signature files.

Click here to expand...

The path to the Configuration Manager signature files.

Registry value	Default value	Notes
SigsFolder	C:\SMSSIG$	Relates to RDC integration and must point to the folder where the signature files are held for Configuration Manager. Wildcards are not allowed. For example: `E:\SMSSIG$` When it is not set, Nomad assumes that signature files location as *`C:\SMSSIG$`*, if it exists.

MODULE.NOMAD.SITESSDSTAGGER

Sets the site SSD query stagger duration (seconds).

Click here to expand...

Sets the site SSD query stagger duration (seconds).

Deployments to large numbers of clients (30,000 or more) generate significant network traffic from 1E Clients to ContentDistribution that may result in IIS 503 Overload errors on the server, causing content registrations and SSD requests to fail. SiteSsdStagger allows an elected subnet master to wait for a random configurable time before making a site SSD request. All peers in the subnet participating in the election would also synchronize and wait for the same time before copying from master machine.

Installer property	Description

Registry value	Type	Default value	Notes
SiteSsdStagger	REG_DWORD	0	Sets the site SSD query stagger duration in seconds. The stagger is 0 (disabled) by default. The maximum value that can configured is 300 seconds (5 minutes). There is no SSD staggering in WinPE. Site SSD happens when broadcast is enabled or if local SSD is enabled and it does not return any devices from ActiveEfficiency. **Note** Please consult 1E before changing this value. This setting works in conjunction with LocalSsdStagger.

MODULE.NOMAD.SITESSDMINPACKAGESIZEKB

Allows you to configure a minimum content size before making an SSD request.

Click here to expand...

Allows you to configure a minimum content size before making an SSD request.

Registry value	Type	Default value	Notes
SiteSSDMinPackageSizeKB	REG_DWORD	0	The default value is 0 which can be changed after installation when it will be an installer property. There is no lower limit for this key, upper limit

Installer property	Description
	is 10240. If the registry value is greater than 10240, the agent will only consider 10240 and will log a warning. Size of content is first taken from Job data, if that's not available it's taken from the LST file, if it's not present there, this key is ignored and an SSD request is made irrespective of size. **Note** This check is for site SSD, not for local SSD.
MODULE.NOMAD.SPECIALNETSHARE	Sets various special feature options related to the Nomad share. The installer property must be set to sum of the integer values for the required bits. For example, to use the computer$ account for access to the Nomad share, and have custom share permissions, you would set the value for the SpecialNetShare registry entry to 129 (0x81 hex). This is shown in the following 1E Client installer command-line: `> msiexec /i 1E.Client-x64.msi MODULE.NOMAD.SPECIALNETSHARE=129 [other properties] /qn` Click here to expand... Sets various special feature options related to the Nomad share.

Registry value	Default value	Notes
SpecialNetShare	0x2060 (8288)	You can set more than one option at the same time by combining the bit values. For example, to have custom share permissions and use the machine account for access to the Nomad share,

Installer property	Description
	set the value for SpecialNetShare to 129 (decimal value 1+128 or 0x0081 hex). See The Nomad share for more detail on configuration and security. The default value in different versions has changed, based on feedback. Upgrading does not change the value unless explicitly set. **Nomad version** / **Default in MSI** Nomad 8.0 (1E Client 8.0): 0x2060 (8288) Bit 5: Disables broadcast of download statistics Bit 6: Enable Nomad FanOut Bit 13: Use HTTP/S or SMB Nomad 7.1 (1E Client 5.2) Nomad 7.0 (1E Client 4.1 to 5.1): 0x2020 (8224) Bit 5: Disables broadcast of download statistics Bit 13: Use HTTP/S or SMB Nomad 6.x: 0x0000 (0) No special features enabled. The default used in all versions of Client Deployment Assistant (and earlier Endpoint Agent Installer) is 0x2070 (8304): Bit 4: Enable Nomad hidden share as NomadSHR$ Bit 5: Disables broadcast of download statistics

Installer property	Description

Bit 6: Enable Nomad FanOut

Bit 13: Use HTTP/S or SMB

Bit	Hex	Decimal	Description
	0x0000	0	No special features enabled.
0	0x0001	1	Custom Share Permissions: Administrators configure and manage custom share permissions. The service doesn't create the *NomadSHR* share on start-up, leaving the administrator to manually create it and set the permissions. It is also not deleted when the service stops and therefore existing share permissions are preserved.
1	0x0002	2	Enables support for IPv6: If the network supports both IPv6 and IPv4, enable support for both – set bit 1 but not bit 2.
2	0x0004	4	Disables support for IPv4: If the network supports only IPv6, disable IPv4 and set both bit 1 and bit 2.
3	0x0008	8	RESERVED
4	0x0010	16	The Nomad share is hidden and named *NomadSHR$*. When using a hidden share, all Nomad installations must be configured to use this option. See The Nomad share for more detail on configuration and security.
5	0x0020	32	Disables broadcast of download statistics. By default, this is disabled. If enabled, Nomad broadcasts download statistics to all peers when a download is complete.

Note

Installer property	Description			
				Prior to 1E Client 4.1 (Nomad 7.0) this was enabled (0) by default, now it is disabled (1) by default.
	6	0x0040	64	Enables Nomad FanOut.
	7	0x0080	128	The machine account is used when connecting to a peer client. The SMSNomadP2P& account is not created. Please refer to The Nomad share: Use Machine Account. **Note** Will not work if peers exist in untrusted domains or workgroups.
	8	0x0100	256	RESERVED
	9	0x0200	512	RESERVED
	10	0x0400	1024	RESERVED
	11	0x0800	2048	RESERVED
	12	0x1000	4096	RESERVED (deprecated)
	13	0x2000	8192	Use HTTP/S or SMB. Ensure that this is set if Nomad integration is used by Tachyon. HTTP/S is automatically used if CM client is detected. **Note** Prior to 1E Client 4.1 (Nomad 7.0) this was disabled (0) by default, now it is enabled (1) by default. This setting should be enabled in baseline or other policies.
	14	0x4000	16384	Web LSZ generation: enables the Nomad client on Configuration Manager standalone DPs to handle LSZ file generation requests coming from HTTP/HTTPS enabled clients.

Installer property	Description			
				Used when Nomad clients are configured with either of the following enabled: Bit13 (0x2000) – Use HTTP/S or SMB Bit 15 (0x8000) – Use HTTP/S only, not SMB When enabled, the Nomad distribution point client creates a virtual folder called *LSZFILES*. The permissions for this are copied from the Configuration Manager *SMS_DP_SMSPKGX$* share. By default, access to the LSZFILES folder requires SSL to be enabled. This is the case for Internet facing scenarios where local client access certificates will ensure authentication. If you are using HTTP instead of HTTPS, manually disable SSL on the LSZFILES web folder in order for the Nomad LSZ file generation process to work. Only needs to be enabled when using HTTP or HTTPS on standalone DPs; it is not required on site server DPs because Nomad automatically configures Web LSZ generation on them.
	15	0x8000	32768	Use HTTP/S only, not SMB: enables the Nomad client to download content using HTTPS or HTTP depending on the content location provided by Configuration Manager or Tachyon. The Nomad client will not use SMB to download content when this is enabled.
MODULE.NOMAD.SSDENABLED	Enables Single Site Download (SSD). The installer property must be set to sum of the integer values for the required bits. For example, the following will turn the complete SSD functionality on. `> msiexec /i 1E.Client-x64.msi MODULE.NOMAD.SSDENABLED=3 [other properties] /qn` Click here to expand... Enables Single Site Download (SSD).			

Installer property	Description		
	Registry value	Default value	Notes
	SSDEnabled	0	You can set more than one option at the same time by combining the bit values. For example, to enable clients to fetch downloads using SSD and provide them to peers, set the value to 3 (decimal value 1+2 or 0x3). To enable clients to fetch downloads using site and local SSD and provide them to peers, set the value to 7. To enable SSD when you install Nomad, you must specify the MODULE.NOMAD.SSDENABLED installer property and ensure the Tachyon client is enabled by specifying SWITCH and BACKGROUNDCHANNELURL installer properties. If MODULE.NOMAD.SSDENABLED is specified during installation, the registry value of ContentRegistration is automatically set to 1. If you want to enable SSD as a provider after installation, then you also need to configure the registry values for SSDEnabled and ContentRegistration, in addition to enabling the Tachyon client. The ContentDistribution registry setting is found under the Platform key. Nomad app provides visibility of content distribution activity Single Site Download (SSD) Single Site Peer Backup Assistant (SSPBA) High Availability Peer Backup Assistant (HAPBA) Get Migration Settings task sequence action used to manage computer associations Nomad Pre-caching Nomad Download Pause.

Installer property	Description
	In legacy versions of Nomad, Platform features were provided using ActiveEfficiency. This required the PlatformURL setting to be configured. This is no longer required. You will see that the PlatformURL registry is used, but this is configured automatically by Nomad on startup by querying the value that the Tachyon client is using (stored in the 1EClient.conf file). If your network is running over a WLAN or have devices on a wireless network you want to be content providers, set ContentProviderOnWifi=1.

Bit	Hex	Decimal	Description
	0x0	0	SSD is disabled, the Nomad client takes no part in the SSD on the site.
0	0x1	1	SSD is enabled and the Nomad client fetches downloads using SSD. This setting on its own (without provider mode set) should be used with sensitive server weighting. Provider mode is where a peer gets content from another peer but cannot serve it (it cannot act as a master).
1	0x2	2	SSD is enabled and the Nomad client provides downloads to peers. Enabling this bit causes Nomad to register content with Content Distribution. In practice, this is unlikely to be used on its own. This is automatically disabled for WinPE installations (because cached content is only temporary).
2	0x4	4	Local SSD is enabled and the Nomad client fetches downloads from a local client (also known as a subnet peer master - the term used for local devices which have content but cannot be located during the normal election process because network broadcasts have been disabled) within the subnet.

Installer property	Description
	The local SSD feature was introduced to supplement site SSD for clients on networks such as wireless where broadcasts are disabled, to prevent each client becoming its own master and downloading direct from the DP. In a SSD enabled environment, a master queries Content Distribution to get a list of devices on other subnets within the site that have content. With local SSD enabled, the master also queries for devices having content within local subnet. If any local peers with content are available, then the master downloads from them, otherwise it attempts to download from Site peers (other subnets in the site), and if the master still cannot find any peers, it downloads the content direct from the DP. In version 7.0 and later, a master skips using local SSD if it sees broadcast messages from peers. This means clients in mixed network environments can be configured with the same SSDEnabled setting (with Local SSD enabled) and clients can move seamlessly between networks. When on a wireless network (where broadcasts are typically disabled) local SSD can be used. On LAN networks (where broadcasts are typically allowed) local SSD would be skipped because a master is elected and sees broadcast activity from peers. This setting should only be used if networks have broadcasts being disabled (for example wireless networks) and clients are forced to download from the DP as they can't participate in an election. Local SSD requires that a peer on the local subnet be configured to provide downloads to peers, that is at least one client on the subnet must be configured with Bit 1 enabled. To maintain consistency with typical Nomad peer sharing behavior where local SSD is not required, configure all clients with *SSDEnabled=7*. You'll also want to set ContentProviderOnWifi=1. When enabled, the elected master:

Installer property	Description
	Queries Content Distribution to get a list of local devices having the content. Queries each of those devices to check if they are available and have the content. The list is ordered by percentage of content the device holds. Repeats the same process for devices on other subnets (existing SSD feature). Stores a list of subnets as well as site devices in memory. Cycles through the list in the following order: Subnet peer master (fetched from list of local devices from Content Distribution) Site master DP. To distinguish between a master derived from Content Distribution and an election, the log records: *`Connection::SetDownloadSource = SubnetPeer`* (an elected peer) instead of *`Connection::SetDownloadSource = Peer`* (an SSD peer master).
MODULE.NOMAD.SSPBAENABLED	Enables the use of Single Site functionality for PBA data stores. See Single Site peer backup assistant for more details. Click here to expand... Enables the use of Single Site functionality for PBA data stores. See Single Site peer backup assistant for more details.

Registry value	Default value	Notes
SSPBAEnabled	0	Has a dependency on the Tachyon Platform PlatformURL. Values are:

Installer property	Description
	0 – disables single-site integration with ContentDistribution 1 – enables single-site integration with ContentDistribution
MODULE.NOMAD.STATUSMSGEVENTS	Determines which Nomad events are reported using Configuration Manager status messages. Click here to expand... Determines which Nomad events are reported using Configuration Manager status messages. Registry value: StatusMsgEvents Default value: 0x0 Notes: Nomad can send status messages through Configuration Manager based on specific download events which appear in its deployment status. They are provided mainly for advanced troubleshooting purposes, or for custom reporting solutions. From v7.1 onwards, they are no longer required for the Nomad Dashboard which now gets its status events directly via the Platform Content Distribution feature. However, you may have custom reporting in Configuration Manger that also use these messages, and you can configure this setting accordingly for this purpose. These messages are controlled by the StatusMsgEvents registry value. This is a *REG_SZ* string data type and the format of the parameter must be a 64-bit value. Status messages are only sent when there is an active deployment. **Warning** Status message events should be used with caution as they could impact your Configuration Manager environment

Installer property	Description
	when scaled up to tens of thousands of machines. For example, to set the request started, request completed, started copy and master changed events, update the StatusMsgEvents registry value to *0x80002060*. 0x0000000001 – SNO_EVT_START 0x0000000002 – SNO_EVT_STOP 0x0000000004 – SNO_EVT_ERROR 0x0000000008 – SNO_EVT_PAUSED 0x0000000010 – SNO_EVT_RESUMED 0x0000000020 – SNO_EVT_REQUEST_STARTED 0x0000000040 – SNO_EVT_REQUEST_COMPLETED 0x0000000080 – SNO_EVT_SERVICE_RESET 0x0000000100 – SNO_EVT_STARTED_CACHE_MANAGEMENT 0x0000000200 – SNO_EVT_FINISHED_CACHE_MANAGEMENT 0x0000000400 – SNO_EVT_STARTED_HASHCHECK 0x0000000800 – SNO_EVT_FINISHED_HASHCHECK 0x0000001000 – SNO_EVT_ELECTION_REQUEST 0x0000002000 – SNO_EVT_MASTER_CHANGED 0x0000004000 – SNO_EVT_FILLIN_MASTER_CHANGED 0x0000008000 – SNO_EVT_MCAST_CENTRALSCHED

Installer property	Description
	0x0000010000 – SNO_EVT_MCAST_ERROR 0x0000020000 – SNO_EVT_MCAST_COMPLETE 0x0000040000 – SNO_EVT_SCHEDULER 0x0000080000 – SNO_EVT_STARTED_TX_CENTRALMCAST 0x0000100000 – SNO_EVT_STOPPED_TX_CENTRALMCAST 0x0000200000 – SNO_EVT_STARTED_TX_ACTIVEMCAST 0x0000400000 – SNO_EVT_STOPPED_TX_ACTIVEMCAST 0x0000800000 – SNO_EVT_STARTED_TX_FILLINMCAST 0x0001000000 – SNO_EVT_STOPPED_TX_FILLINMCAST 0x0002000000 – SNO_EVT_STARTED_RX_CENTRALMCAST 0x0004000000 – SNO_EVT_STOPPED_RX_CENTRALMCAST 0x0008000000 – SNO_EVT_STARTED_RX_ACTIVEMCAST 0x0010000000 – SNO_EVT_STOPPED_RX_ACTIVEMCAST 0x0020000000 – SNO_EVT_STARTED_RX_FILLINMCAST 0x0040000000 – SNO_EVT_STOPPED_RX_FILLINMCAST 0x0080000000 – SNO_EVT_STARTED_COPY 0x0100000000 – SNO_EVT_STOPPED_COPY

Installer property	Description
	0x0200000000 – SNO_EVT_WORKRATE_CHANGED 0x0400000000 – SNO_EVT_WRONG_PKG_VERSION 0x0800000000 – SNO_EVT_INFORMATIONAL 0x1000000000 – SNO_EVT_FINALSTATS (see notes below) 0x2000000000 – SNO_EVT_WAIT 0x4000000000 – SNO_EVT_MAX_EVENTID **SNO_EVT_FINALSTATS notes** For success reporting, this message provides feedback on the status of the download. For example, it can show how much data was received using multicast as opposed to peer-to-peer copying. Turning this message on creates an extra status message per machine for each deployment. The format of the status message is: `Evt_FinalStats MD100067 1 170 59195038 170 59195038 0 59195038 0 0` Configuration Manager status messages are made up of insertion strings. The strings for the final stats event are: InstrStr0 – Nomad event string (internal reference) – N/A InstrStr1 – Package Id and Package version – MD100067 1 InstrStr2 – Total number of files in package – 170

Installer property	Description			
		InstrStr3	Total number of package bytes	59195038
		InstrStr4	Number of files which are cached	170
		InstrStr5	Bytes which are cached	59195038
		InstrStr6	Bytes coped from a peer agent (P2P)	0
		InstrStr7	Bytes copied from the DP	59195038
		InstrStr8	Bytes received via local multicast	0
		InstrStr9	Bytes received from a central multicast	0
	If the package is already cached and is re-deployed with an unchanged package version, the final stats message will not be re-sent.			
MODULE.NOMAD.SUCCESSCODES	A list of Nomad return codes that are translated as success to the Content Transfer Manager (CTM) component of the Configuration Manager client. Click here to expand... A list of Nomad return codes that are translated as success to the Content Transfer Manager (CTM) component of the Configuration Manager client.			

Registry value	Default	Notes
SuccessCodes	0x206b, 0x2077, 0x103, 0xffffffff, 0x1,	This REG_SZ value contains a comma-delimited list of possible Nomad return codes that should be treated as a success and thereby prevent Configuration Manager from

Installer property	Description		
		0x70, 0x2050, 0x2051, 0x2052, 0x2053, 0x2054,0x2055, 0x2056, 0x2057, 0x2058, 0x205a, 0x205b, 0x205c, 0x205d, 0x205e, 0x2060, 0x2061,0x2062, 0x2063, 0x2064, 0x2065, 0x2066, 0x2067, 0x2068, 0x2069, 0x209A	attempting to download the content itself or use another Alternate Content Provider (ACP). Any code returned by Nomad that is not on the list will be treated as a failure and trigger the Configuration Manager client to attempt to download the content using alternate means. Nomad also sends a status message to the Configuration Manager site containing its return code. Strictly speaking the Nomad return codes are actually internal status codes, Nomad will only ever return success or failure to the Content Transfer Manager (CTM) component of the Configuration Manager client. When CTM receives a success it passes control to the ExecMgr component of the Configuration Manager client, which attempts to execute the deployment. ExecMgr will fail if Nomad did not download the content and make it available in the Configuration Manager cache. In this case, ExecMgr sends a status message (e.g. failed deployment) back to the Configuration Manager site. If Nomad generates a return code that is not in the list, it passes a fail to the CTM component which causes the Configuration Manager client to try downloading the content itself using BITS, or use another Alternate Content Provider (ACP). This process may itself succeed or fail depending on the conditions that resulted in the original Nomad return code, and may have an undesirable impact on the network. **Note** The special code 0x9999 can be added to the list, or used on its own, to cause Nomad to always return a success to CTM. As a

Installer property	Description

consequence this code is also known as "prevent failover to BITS".

Note

The SuccessCodes list need not be modified under normal circumstances, other than to add or remove the 0x9999 code.

The following table shows the possible Nomad return codes that can be set in the list:

Note

This list is subject to change with each release of Nomad, and provided for reference only.

Return Code	Description	
-1	0xFFFFFFFF	Reserved.
1	0x0001	Reserved.
112	0x0070	Insufficient disk space to create the cache.
259	0x0103	Reserved.
8272	0x2050	The download has been suspended by APM.
8273	0x2051	The user has cancelled this download.
8274	0x2052	Invalid command line.

Installer property	Description			
		8275	0x2053	Command-line execution failure.
		8276	0x2054	Internal Error.
		8277	0x2055	The package exceeds the threshold for a RAS connection.
		8278	0x2056	The package exceeds the threshold for a Slow LAN connection.
		8279	0x2057	The package exceeds the threshold for a Fast LAN connection.
		8280	0x2058	Reserved.
		8281	0x2059	Unknown transport. Returned when an attempt is made to download a Software Update from an Internet location (like Microsoft Updates).
		8282	0x205A	Invalid special package path (set using --pp).
		8283	0x205B	Incorrect file hash.
		8284	0x205C	Exited due to a kill request.
		8285	0x205D	DP path not found.
		8286	0x205E	The MaxBusyBackOff consecutive event

Installer property	Description			
				threshold has been exceeded.
		8287	0x205F	The service has stopped.
		8288	0x2060	The advertisement has expired.
		8289	0x2061	Reserved.
		8290	0x2062	This is an unlicensed version of Nomad.
		8291	0x2063	Invalid alternate cache path (set using --cp).
		8292	0x2064	No Configuration Manager job data found in WMI.
		8293	0x2065	Incorrect package hash.
		8294	0x2066	MaxDuration or execution runtime for this program has been exceeded.
		8295	0x2067	Reserved.
		8296	0x2068	Incorrect package version.
		8297	0x2069	Obsolete package version.

Installer property	Description			
		8298	0x206A	The BlockSize has been changed during download.
		8299	0x206B	The "no progress" re-check threshold has been exceeded.
		8300	0x206C	The parent process has terminated.
		8301	0x206D	Duplicate download for the package.
		8302	0x206E	The service was reset. This will occur if certain configuration parameters are changed during a download e.g. NomadInhibitedSubnets
		8303	0x206F	Nomad inhibited.
		8311	0x2077	Internal error LST incomplete.
		8346	0x209A	Client certificate missing. Nomad is configured to use certificate-based client authentication but was unable to find an appropriate certificate.

Installer property	Description
MODULE.NOMAD.SUPPORTWPAD	Provides support for Web Proxy Auto-Discovery Protocol (WPAD). Click here to expand... Provides support for Web Proxy Auto-Discovery Protocol (WPAD). Nomad always uses System level proxy if it has been set, irrespective of what SupportWPAD has been set to. SupportWPAD was introduced in v7.1 and when disabled it does not change the default behavior, which is: If system level proxy is set then use it, otherwise access directly without proxy. When SupportWPAD is enabled in Nomad, the behavior is: If system level proxy is set then use it and do not try WPAD If system level proxy is not set then fetch automatic proxy using WPAD and use it If system level proxy is not set and failed to get automatic proxy using WPAD then try access directly without proxy. **How to know if a system level proxy has been set** `netsh winhttp show proxy` Registry value: SupportWPAD Default value: 0 Notes: By default, the WPAD feature is disabled. To enable WPAD in Nomad, add registry key 'SupportWPAD' and set it to 1 at registry path HKLM/Software/1E/NomadBranch To enable or disable the WPAD feature in Nomad: Disable WPAD set SupportWPAD = 0 Enable WPAD set SupportWPAD= 1 (or non-zero value).
MODULE.NOMAD.USEFIPS	This installer property sets the Nomad EncryptionType registry entry.

Installer property	Description
	Determines the type of encryption used by Nomad to encrypt its communications between Nomad peers. Click here to expand... Determines the type of encryption used by Nomad to encrypt its communications between Nomad peers. Registry value: EncryptionType Default value: 0x0 (0) Notes: Value are: 0 – standard Nomad encryption 1 – FIPS encryption
MODULE.NOMAD.WAKEUPBATCHSIZE	The maximum number of machines to wake up in a single call. Click here to expand... The maximum number of machines to wake up in a single call. **Warning** Nomad integration with WakeUp enables Nomad to share content from its devices that are holding particular content, even if those devices are offline. One reason why peers in the local subnet may not respond to the request even though they have content in their caches is that they are offline (shutdown, in hibernate or sleep mode). However, if WakeUp is integrated, the Nomad client would know which offline device has the content and can wake it up when it queried Content Distribution. The wake-up list is maintained by Content Distribution and is the same list that Single Site Download (SSD) uses. Separate lists of peers are returned for the subnet and site. This feature requires Nomad SSD to be enabled, Content Distribution, and a NightWatchman infrastructure. The feature is enabled during the installation of the NightWatchman Management Center. Please refer to Introducing Nomad for requirements.

Installer property	Description

Registry value	Default value	Notes
WakeUpBatchSize	10	Sets the maximum number of machines to wake up in one call, for subnet and site separately. (So up to twice this number of requests is sent in total if WakeUp is enabled for both subnet and site.) The next batch is launched, if necessary, after a re-election (usually a periodic election). The value cannot be greater than MaxDevicesFromAE, and hence itself cannot be more than 20.

MODULE.NOMAD.WAKEUPENABLED

Enables WakeUp integration, see Integrating Nomad with WakeUp for more details.

Click here to expand...

Enables WakeUp integration, see Integrating Nomad with WakeUp for more details.

Warning

Nomad integration with WakeUp enables Nomad to share content from its devices that are holding particular content, even if those devices are offline. One reason why peers in the local subnet may not respond to the request even though they have content in their caches is that they are offline (shutdown, in hibernate or sleep mode). However, if WakeUp is integrated, the Nomad client would know which offline device has the content and can wake it up when it queried Content Distribution.

The wake-up list is maintained by Content Distribution and is the same list that Single Site Download (SSD) uses. Separate lists of peers are returned for the subnet and site. This feature requires Nomad SSD to be enabled, Content Distribution, and a NightWatchman infrastructure. The feature is enabled during the installation of the NightWatchman Management Center. Please refer toIntroducing Nomad for requirements.

Installer property	Description

Registry value	Default value	Notes
WakeUpEnabled	0	Determines the status of the WakeUp integration. If configured by the installer, it is disabled (0) by default. If integration is enabled, Nomad attempts to wake up dormant hosts that are known to have the requested content in their caches. The integration has a dependency on the PlatformURL. To enable integration post-installation, for normal usage, set both bits 0 and 1 (0x3)

Bit	Hex	Decimal	Description
	0x0	0	Disables WakeUp integration.
0	0x1	1	Enables WakeUp integration only for the local subnet.
1	0x2	2	Enables WakeUp integration only for the site.
	0x3	3	Enables WakeUp integration for the site and the local subnet.

MODULE.NOMAD.WAKEUPMINPACKAGESIZEMB

The minimum size of content (in megabytes) that will cause a request for a wakeup. See Integrating Nomad with WakeUp for more details.

Click here to expand...

The minimum size of content (in megabytes) that will cause a request for a wakeup. See Integrating Nomad with WakeUp for more details.

Warning

Nomad integration with WakeUp enables Nomad to share content from its devices that are holding particular content, even if those devices are offline. One reason why peers in the local subnet may not respond to the request even though they have content in their caches is that they are offline (shutdown, in hibernate or sleep mode).

Installer property	Description

However, if WakeUp is integrated, the Nomad client would know which offline device has the content and can wake it up when it queried Content Distribution.

The wake-up list is maintained by Content Distribution and is the same list that Single Site Download (SSD) uses. Separate lists of peers are returned for the subnet and site. This feature requires Nomad SSD to be enabled, Content Distribution, and a NightWatchman infrastructure. The feature is enabled during the installation of the NightWatchman Management Center. Please refer toIntroducing Nomad for requirements.

Registry value	Default value	Notes
WakeUpMinPackageSizeMB	1024	Any content below this size is downloaded from the DP as downloads from the DP for files this size will likely complete before any wakeups will have had a chance to finish. The value can be 0, in which case wakeups will always be attempted. For example, if it is set to 512 and size of the content downloaded is 500 MB, a wake-up request (to site or subnet) is not be sent. Similarly, if size of the content is 600 MB, then wake-up requests (to site and subnet, determined by WakeupEnabled) is be sent. **Note** For standalone downloads (using SMSNomad.exe) and under WinPE, there has no effect as the size of the content cannot easily be determined. Wake-up requests are always sent in these instances.

Installer property	Description
MODULE.NOMAD.WLANBLIPSECS	The duration for temporarily disabling a wireless connection when a wired LAN connection becomes available, to provide time for the OS and Nomad to switch to the LAN connection. This is useful for OS versions and drivers that do not automatically switch to a preferred wired connection. Click here to expand... The duration for temporarily disabling a wireless connection when a wired LAN connection becomes available, to provide time for the OS and Nomad to switch to the LAN connection. This is useful for OS versions and drivers that do not automatically switch to a preferred wired connection. Registry value: WLanBlipSecs Default value: 0 Notes: The value must be 20 seconds or more. Nomad provides extra stability by managing a machine's network connections as they move between a wireless and a wired LAN. Depending on the OS version or other factors, once an SMB or HTTP session is running on a wireless connection, it will remain on wireless even when a wired LAN becomes available. Nomad uses **WLanBlipSecs** to temporarily drop a wireless connection when it detects a wired LAN connection, to give time for the OS and Nomad to automatically switch to the LAN connection. For example, if a Nomad master was initiated when a machine was on a wireless connection and a wired connection subsequently became available, Nomad disables the wireless adapter for a long enough period to enable a switchover to the wired connection. As a result of this, the IP address and the share path will change and peers will log error messages until each peer re-establishes its connection to the master and the new share location. This feature is turned off by default. **Note** Other applications may be affected when switching from wireless to wired connection. Irrespective of the **WLanBlipSecs** setting, you can also control which service set identifier (SSID) Nomad connects to by managing a list. To do this, update the NomadBranch WLanProfileList registry value with a comma-delimited list of SSIDs or use the wildcard (*) character for any SSID. Examples:

Installer property	Description
	`WLanProfileList REG_SZ WIFIGAP,GUEST` `WLanProfileList REG_SZ *`
MODULE.NOMAD.WLANPROFILELIST	A list of wireless SSIDs to enable switching from wireless to wired LAN connections. Click here to expand... A list of wireless SSIDs to enable switching from wireless to wired LAN connections. Registry value: WLanProfileList; Default value: ; Notes: A comma-delimited list of wireless SSIDs (* for any all) which enables Nomad to switch form wireless to a wired LAN connection when it becomes available.

9.6.12 Nomad registry values

The two Nomad components that have registry values are NomadBranch and NomadBranchAdminUIExt, grouped below under feature headings.

9.6.12.1 NomadBranch registry values

The NomadBranch registry values can be changed to alter some of the default installation values for Nomad. Before you make any registry updates, ensure you make a backup of the registry. The following headings show the Nomad registry entries related to a particular functional area.

Clicking on a registry value's link will take you to its definition page, which has more details including its Windows installer property.

Note

Registry values for NomadBranch are located in *HKLM\Software\1E\NomadBranch*

9.6.12.1.1 Basic Nomad configuration

CompatibilityFlags, Debug, GenerateWEREvents, InstallationDirectory, LogFileName, MaxLogFileSize, MaxStuckCount, P2PDisqualifyMaxNumPeers, P2PDisqualifyMaxWindowMins, P2PElectionWeight, P2Penabled, P2P_Port, SpecialNetShare, SuccessCodes

9.6.12.1.2 Peer Backup Assistant (PBA)

CachePath, EnforceQuotas, HAACKTimeoutMins, MaxAllocRequest, MaxConcurrency, MaximumMegaByte, PostCompleteTimeoutHours, PreCompleteTimeoutHours, SSPBAEnabled

9.6.12.1.3 Connection and downloads

DownloadTimeout, MaxAllowedLinkSpeed, MaxBusyBackOffSecs, MaxPackageSizeFastLAN, MaxPackageSizeRAS, MaxPackageSizeSlowLAN, MaxWorkRates, NomadNeverUseSubnets, RunUncachedPermittedFastLAN, WLanBlipSecs, WLanProfilesList

9.6.12.1.4 Nomad cache

AuthenticatedUsers, CacheCleanCycleHrs, MaxCacheDays, MaxCacheSizeMB, MaxPreCacheDays, MaxSUCacheDays, NoHardlink, NomadInhibitedADSites, NomadInhibitedSubnets, PercentAvailableDisk

9.6.12.1.5 Certificates, HTTPS and Internet-facing clients

CertIssuer, CertSubject

9.6.12.1.6 Distribution Point server related

DPNotAvailableCodes, PermittedLSZShares, RecycleDPDelay, SigsFolder

9.6.12.1.7 Status messages

MaxStatusFrequency, StatusMsgEvents

9.6.12.1.8 FanOut

ExtraReplyDelayMs, SpecialNetShare

9.6.12.1.9 Single Site Download (SSD)

ActiveEfficiency\PlatformURL, ContentRegSyncBatchSz, ContentRegSyncCycleHrs, ContentRegSyncReqDelay, LocalSsdStagger, NoSsdReqOnInhibitedSubnets, PercentDelayedContentReg, SiteSsdStagger, SSDEnabled, SSPBAEnabled, CacheStateSyncIntervalMinutes

9.6.12.1.10 Multicast

CentralMCastExtraDelayMins, MaxPacketsPerSecond, MultiCastMADCAPScope, MulticastSupport

9.6.12.1.11 WakeUp

MaxDevicesFromAE, WakeUpBatchSize, WakeUpEnabled, WakeUpMinPackageSizeMB

> **Note**
>
> If you make changes to the registry values, we recommend you restart the Nomad service – changes to P2P_Port, P2PEnabled, NomadInhibitedSubnets and NomadInhibitedADSites will not take effect until the service is restarted.

9.6.12.2 NomadBranchAdminUIExt registry categories

For 64-bit machines running the Configuration Manager console, the registry values for NomadBranchAdminUIExt are under: *HKLM\Software\Wow6432Node\1E\NomadAdminUI\Platform*

For 32-bit machines running the Configuration Manager console, the registry values for NomadBranchAdminUIExt are under: *HKLM\Software\1E\NomadAdminUI\Platform*

9.6.12.2.1 Nomad pre-caching

There is only one value that is of use in the NomadBranchAdminUIExt registry that defines the location of Content Distribution Server for use with the Nomad Pre-caching feature: PlatformURL

9.6.12.3 Alphabetic NomadBranch registry values

The following table shows the supported NomadBranch registry value and any associated installer properties. Installer properties must be upper-case and those that use numeric values must be set using decimal integers on the command-line.

Registry value	Description
Platform\PlatformURL	The URL of the Tachyon Platform, specifically the Tachyon Background Channel, which provides a reverse proxy for the Content Distribution component of Tachyon Platform. Usually of the form *https://<BackgroundChannelServer>:<BackgroundChannelPort>/Background/*
Platform\ContentRegistration	Determines if content in Nomad's cache (packages, applications, software updates, boot images, etc.) is registered with Content Distribution. Content registration is necessary if a host is to be available as a Single Site Download (SSD) provider or can be woken up if a Nomad peer requires the content locally.
Platform\ContentProviderOnWifi	Determines whether a device on a WLAN can become content provider. By default, only devices connected to a LAN can become content providers when using Single Site Download (SSD). **Note** This setting is only applicable to SSD and has no effect on P2P content transfers on the local subnet.
AssumedLinkSpeed	**Warning** AssumedLinkSpeed is obsolete. Its value may exist in the Nomad registry but it is not used. Instead Nomad now

Registry value	Description
	relies on the actual content being downloaded to gauge link speed.
AuthenticatedUsers	Determines which of the built-in security groups is granted read-only permissions to the Nomad cache.
BlockSize	Value (in bytes) for the minimum size of each block of data Nomad copies from the package source folder.
CacheCleanCycleHrs	Determines the number of hours between automatically running the Nomad cache cleaner.
CacheCleanSubnetLookup	If enabled, sets the cache clean subnet lookup.
CentralMCastExtraDelayMins	An integer value that sets the delay for receiving Central Multicast. Normally you would not need to set this value.
CertIssuer	Defines one or more certificate issuers that Nomad will use to select the appropriate PKI certificate for the: Configuration Manager (CM) client authentication certificate - used when downloading over HTTPS from Distribution Points and when communicating with Management Points during pre-caching Nomad Server Authentication certificate - used to share content between peers over HTTPS Client Authentication certificate - used for certificate-based client authentication when sharing content between peers over HTTPS. In most cases Nomad will be able to identify a suitable certificate in the Local Computer Personal certificate store without needing to specify CertIssuer (refer to Peer copy over HTTP or HTTPS: Certificate Selection for more details). You should use CertIssuer if the CM client is not using PKI certificates and there are multiple Client Authentication certificates issued by different Certificate Authorities in the store, and if there is a chance some of those certificates may not be trusted by other peers or CM site systems.
CertSubject	Defines one or more certificate subject names that Nomad uses to select the appropriate PKI certificate for authentication with Configuration Manager (CM) site systems configured to use HTTPS. It does not affect certificate selection for client

Registry value	Description
	authentication certificates used for peer-to-peer authentication or for selection of server authentication certificates. In most cases Nomad will be able to identify a suitable certificate in the Local Computer Personal certificate store without the need to specify CertSubject (refer to Peer copy over HTTP or HTTPS: Certificate Selection for more details).
CompatibilityFlags	Determines different compatibility settings which relate to specific customer related functionality and should not generally be changed from the default value under normal conditions, unless advised.
ContentRegSyncCycleHrs	**Warning** ContentRegSyncCycleHrs is obsolete. Its value may exist in the Nomad registry, but it is not used. Instead, please refer to CacheStateSyncIntervalMinutes.
ContentRegSyncReqDelay	**Warning** ContentRegSyncReqDelay is obsolete. Its value may exist in the Nomad registry, but it is not used. Instead, please refer to CacheStateSyncIntervalMinutes.
ContentRegSyncBatchSz	**Warning** ContentRegSyncBatchSz is obsolete. Its value may exist in the Nomad registry, but it is not used. Instead, please refer to CacheStateSyncIntervalMinutes.
Debug	The level of messages logged in the Nomad logs for debugging purposes.
DebugDynamicBlock	The level of messages related to the Dynamic Block Size (DBS) feature logged in the Nomad logs for debugging purposes.
DeliveryOptimizationReportingEnabled	Enables Delivery Optimization monitoring and reporting if ContentRegistration is enabled.
DownloadTimeout	Sets the timeout in seconds after which a job will be cancelled if the download has not been successful.

Registry value	Description
DPNotAvailableCodes	Determines which error codes will cause Nomad to retry a download using an alternative distribution point.
DpCacheCleanupEnabled	Delete all obsolete LSZ files on the DP where the associated content is no longer present in ContentLib.
ContentProviderOnWifi	Determines whether a device on a WLAN can become content provider. By default, only devices connected to a LAN can become content providers when using Single Site Download (SSD). **Note** This setting is only applicable to SSD and has no effect on P2P content transfers on the local subnet.
EncryptionType	Determines the type of encryption used by Nomad to encrypt its communications between Nomad peers.
GenerateWEREvents	Determines whether Windows Error Reporting memory dumps should be sent to Microsoft Winqual.
InstallationDirectory	The installation directory for Nomad.
LocalCachePath	The location of local Nomad package cache.
LogFileName	The path and filename of the Nomad log file.
MaxAllowedLinkSpeed	(Optional setting) If set, defines the maximum possible link speed in bits per second.
MaxBusyBackOffSecs	The maximum duration (in seconds) that Nomad backs-off between blocks of data.
MaxCacheDays	When the Nomad cache cleaner runs, delete any application or package content that last triggered Nomad elections before the specified number of days ago.
MaxCacheDaysThreshold	This is the maximum number of days content is present on a client.

Registry value	Description
MaxCacheSizeMB	Provided for backward compatibility only – use PercentAvailableDisk instead. The value (in bytes) for the maximum size the cache is allowed to grow to, before automatic cache cleaning takes place.
MaxDevicesFromAE	The maximum number of devices with the content that Nomad can retrieve from Content Distribution in one call.
MaxElectionResponseLogging	Defines the number of election responses Nomad will write to the log for a given election.
MaxLogFileSize	The maximum size (in bytes) of the Nomad log file. Default is 5MB.
MaxPackageSizeFastLAN	The maximum size (in bytes) of a package that Nomad attempts to cache on a Fast LAN (>500 kbps) connection.
MaxPackageSizeRAS	The maximum size (in bytes) of a package that Nomad will attempt to cache on a RAS (<55 kbps) connection.
MaxPackageSizeSlowLAN	Maximum size (in bytes) of a package that Nomad attempts to cache on a Slow LAN (55-500 kbps) connection.
MaxPacketsPerSecond	The maximum rate at which multicast packets are sent.
MaxPreCacheDays	When the Nomad cache cleaner runs, delete any pre-cached content that last triggered Nomad elections before the specified number of days ago.
MaxStatusFrequency	he minimum interval (in seconds) between sending transfer progress status messages, thereby governing the overall maximum frequency for sending the messages.
MaxStuckCount	Registry value to hold an integer determining the number of times Nomad attempts to copy content and gets stuck before aborting.
MaxSUCacheDays	When the Nomad cache cleaner runs, delete any software updates that last triggered Nomad elections before the specified number of days ago.

Registry value	Description
MaxWorkRates	MaxWorkRates is a registry key, that must be created, to hold registry values for each day of the week (Day0 to Day6) where the hourly maximums for the variable work rates are set.
MultiCastMADCAPScope	The MADCAP scope for multicast.
MulticastSupport	The behavior of local multicast.
NMDS\CachePath	This value holds the location of the base peer backup assistant (PBS) share where user data is copied to.
NMDS\EnforceQuotas	Determines whether Windows Disk Quotas (if configured) are enforced on the PBA share defined in CachePath.
NMDS\ExtraReplyDelayMs	Time by which PBA peer reply window should be extended to avoid network spikes.
NMDS\HAACKTimeoutMins	The time-out period in minutes for the Peer Backup Assistant - High Availability (PBA-HA) task sequence action. If a machine running this action does not receive an acknowledgement message within this period from the PBA host performing the additional backups, the action will fail.
NMDS\MaxAllocRequest	Sets the maximum amount of space in MB that can be requested by each PBA client.
NMDS\MaxConcurrency	Sets the maximum number of concurrent PBA sessions that may be in use on the host.
NMDS\MaximumMegaByte	The maximum amount of space (in MB) that can be used for all the PBA shares combined on the host.
NMDS\PostCompleteTimeoutHours	The duration (in hours) after which the PBA share is deleted from the host.
NMDS\PreCompleteTimeoutHours	The duration (in hours) after which PBA share is deleted from the host.
NoHardlink	Determines whether hard links are used between the Nomad cache and the Configuration Manager cache.

Registry value	Description
NomadInhibitedADSites	Prevents Nomad from calling an election when it is connected to a specified AD site, meaning that each Nomad client on the listed AD sites will automatically become a Nomad master. This prevents P2P sharing, as each master downloads its own copy of the content.
NomadInhibitedSubnets	Prevents Nomad from calling an election when it is connected to a specified IP subnet, meaning that each Nomad client on the IP subnet automatically becomes a Nomad master. This prevents P2P sharing, as each master downloads its own copy of the content.
NomadNeverUseSubnets	Prevents Nomad from using specific network adaptors based on the IP subnet. For example, this can be used to exclude Server backup subnets.
P2PClientCertWaitPeriodMins	Defines the number of minutes that Nomad waits from the start time of the download job for a valid client authentication certificate before failing the download job.
P2PDisqualifyMaxNumPeers	Defines the max number of devices which a device will disqualify during a peer-to-peer copy.
P2PDisqualifyMaxWindowMins	Defines the max number of minutes within which a device will disqualify a peer during a peer-to-peer copy.
P2PElectionWeight	Determines the outcome of Nomad elections.
P2PEnabled	Determines how the Nomad cache is accessed. Please refer to Nomad cache for more details.
P2PHttpPort	The HTTP port to use for peer copy.
P2PHttpsPort	The HTTPS port to use for peer copy.
P2P_Port	Port used to broadcast election messages, for connectionless cache access and package status broadcasts.
P2PSslSettings	Defines server and client authentication options when using HTTPS for P2P content transfer (i.e. P2PEnabled 0x60 option is set).

Registry value	Description
PercentAvailableDisk	The limit on the Nomad cache. Specified as a percentage of the available disk space, it controls the automatic cache cleaning to ensure that the cache does not grow to a size whereby the percentage of available disk space is less than this value.
PercentDelayedContentReg	**Warning** PercentDelayedContentReg is obsolete. Its value may exist in the Nomad registry, but it is not used. Instead, **Content Registration Sync Cycle** is now used, please refer to CacheStateSyncIntervalMinutes.
PermittedLSZShares	Restricts Nomad LSZ file generation requests to a list of permitted package source locations.
PrecachePollBatchSize	The number of notifications a client processes in one pre-cache poll cycle.
PrecachePollMinutes	The interval (in minutes) between Nomad polling Content Distribution for new pre-cache jobs.
RecycleDPDelay	The delay (in seconds) before restarting retries from the first DP after the whole list of available DPs have been tried.
RunUncachedPermittedFastLAN	Determines where the download package is run from under certain conditions.
SigsFolder	The path to the Configuration Manager signature files.
SpecialNetShare	Sets various special feature options related to the Nomad share.
SSDEnabled	Enables Single Site Download (SSD).
SSPBAEnabled	Enables the use of Single Site functionality for PBA data stores. See Single Site peer backup assistant for more details.
StatusMsgEvents	Determines which Nomad events are reported using Configuration Manager status messages.

Registry value	Description
SuccessCodes	A list of Nomad return codes that are translated as success to the Content Transfer Manager (CTM) component of the Configuration Manager client.
SupportWPAD	Provides support for Web Proxy Auto-Discovery Protocol (WPAD).
WakeUpBatchSize	The maximum number of machines to wake up in a single call.
WakeUpEnabled	Enables WakeUp integration, see Integrating Nomad with WakeUp for more details.
WakeUpMinPackageSizeMB	The minimum size of content (in megabytes) that will cause a request for a wakeup. See Integrating Nomad with WakeUp for more details.
WLanBlipSecs	The duration for temporarily disabling a wireless connection when a wired LAN connection becomes available, to provide time for the OS and Nomad to switch to the LAN connection. This is useful for OS versions and drivers that do not automatically switch to a preferred wired connection.
WLanProfileList	A list of wireless SSIDs to enable switching from wireless to wired LAN connections.

9.6.12.3.1 AssumedLinkSpeed

Warning

AssumedLinkSpeed is obsolete. Its value may exist in the Nomad registry but it is not used. Instead Nomad now relies on the actual content being downloaded to gauge link speed.

Value (in bits per second) to for the link speed calculations at the beginning of a download. This value should only be modified if requested by 1E support.

Registry value	Default value	Notes	Installer property
AssumedLinkSpeed	100	If set to 0, an unreliable IPv4 ping test is performed to gauge the bandwidth of the WAN link before starting a download. By default, the value is set to	n/a

Registry value	Default value	Notes	Installer property
		100 so as to disable the ICMP test and calculate the end-to-end bandwidth based on actual data blocks	

9.6.12.3.2 AuthenticatedUsers

Determines which of the built-in security groups is granted read-only permissions to the Nomad cache.

Registry value	Default value	Notes	Installer property
AuthenticatedUsers	1	Grants read-only access to the Nomad cache as follows: 0 – Everyone built-in security group and the *SMSNomadP2P&* Nomad share account. This is the least restrictive option and is not valid with HTTP or HTTPS protocol and is treated as 2 (only the *SMSNomadP2P&* Nomad share account) 1 – Authenticated Users built-in security group and the *SMSNomadP2P&* Nomad share account 2 – Only the *SMSNomadP2P&* Nomad share account. This account has also been added to NTFS permission settings. Unauthorised HTTP requests to access the	MODULE.NOMAD.AUTHENTICATEDUSERS

Registry value	Default value	Notes	Installer property
		caches are met with a 403 status code. The Nomad share has more information about share permissions and NTFS security. The difference between Authenticated Users and Everyone depends on the OS version, but in general Everyone includes Authenticated Users plus Guest.	

9.6.12.3.3 BlockSize

Value (in bytes) for the minimum size of each block of data Nomad copies from the package source folder.

Note

Any change to this value requires a manual service restart before it can take effect.

Registry value	Default value	Notes	Installer property
BlockSize	131072(128KB)	Must be between 4096(4KB) to 4194304(4MB) inclusive. The default block size is 128KB The maximum block size is 4MB Multicast environments can only use the default block size. If you define a larger value for multicast environments, Nomad automatically resets it to the default. Clients use the block size defined in the registry and ignore the values from the LSZ	MODULE.NOMAD.BLOCKSIZE

The Dynamic Block Size (DBS) feature increases block size on high-bandwidth links to get maximum efficiency, and reduces it on low-bandwidth links to reduce the impact. Using DBS, Nomad is able to automatically decide the appropriate block size for a given link bandwidth and also adjust it as needed during the download if the link conditions change. As a result, Nomad is far more efficient and faster on all types of connection bandwidths while retaining its minimal impact on other link traffic.

Note

DBS is enabled or disabled by configuring Bit 25 in the CompatibilityFlags registry. Setting Bit 25 disables DBS and clearing Bit 25 enables DBS.

In Nomad 7.0 onwards, the DBS feature is turned off by default for new installations, and not changed for upgrades.

Prior to v6.3 the default value of BlockSize registry setting was 32KB (0x8000). From v6.3 onwards the default is 128KB (0x20000).

The installer automatically sets this to 128KB for both fresh installs and upgrades from previous versions. The only exceptions to this are:

It will use the specified value if the BLOCKSIZE property is used in the installation command line or in a MST transform, when doing a fresh install or upgrade

It will retain the previous value of BLOCKSIZE if it was set to anything other than 32KB (the older default), when doing an upgrade.

9.6.12.3.4 CacheCleanCycleHrs

Determines the number of hours between automatically running the Nomad cache cleaner.

Registry value	Default value	Notes	Installer property
CacheCleanCycleHrs	0 (turned off)	The first automatic cache clean runs randomly between 10 to 60 mins of service start up. Subsequent cache clean cycles run after the number of hours specified. 0 means feature turned off. No cache cleaning cycle would run. Changing this registry entry performs an internal restart.	MODULE.NOMAD.CACHECLEANCYCLEHRS

Registry value	Default value	Notes	Installer property
		The minimum value is 4. The maximum value is 168 (Once a week) Please refer to Cache management for details about other cache management settings.	

9.6.12.3.5 CacheCleanSubnetLookup

If enabled, sets the cache clean subnet lookup.

Registry value	Type	Default value	Notes	Installer property
CacheCleanSubnetLookup	REG_DWORD	1	Before deleting content, Nomad checks if it is on any other client in the same subnet, and will only delete local content if the same is present on at least one other client on the same subnet.	MODULE.NOMAD.CACHECLEANSUBNETLOOKUP

Registry value	Type	Default value	Notes	Installer property
			To disable subnet lookup, set the value to 0. Its value can be 0 or 1. The default value is 1, subnet lookup is enabled. New setting introduced in 8.0. Please refer to Cache management for details about other cache management settings.	

9.6.12.3.6 CachePath

This value holds the location of the base peer backup assistant (PBS) share where user data is copied to.

Registry value	Default value	Notes	Installer property
NMDS\CachePath	<NomadCachePath>\NMDS	This REG_SZ registry value is found under the PBA registry key NomadBranch\NMDS. This parameter relies on the folder it points to as being configured as a share. In normal circumstances, this should not be modified from the default value. The MODULE.NOMAD.CACHEPATH installer property also used to configure the location of the Nomad cache, which is stored in the registry value LocalCachePath. The location of the PBA cache is derived from the MODULE.NOMAD.CACHEPATH property, and is stored in the registry value CachePath in the NomadBranch\NMDS registry key.	MODULE.NOMAD.CACHEPATH

9.6.12.3.7 CacheStateSyncIntervalMinutes

Ensures the cache state of a device held on ContentDistribution is in sync with locally held data. This setting controls the **Content Registration Sync Cycle** feature.

Registry value	Default value	Notes	Installer property
CacheStateSyncIntervalMinutes	1440 (1day)	Range: from 60 to 525600	MODULE.NOMAD.CACHESTATESYNCINTERVALMINUTES

Registry value	Default value	Notes	Installer property
		(1Year).	

The **Content Registration Sync Cycle** is available in the following versions of 1E Client, where the Nomad client registers pending and failed content registrations with ActiveEfficiency or Tachyon Platform. Please refer to Single Site Download: Improved resilience of content registration.

Nomad 8.0 in 1E Client 5.2 - uses Content Distribution in Tachyon Platform

Nomad 7.1 in 1E Client 5.2 - uses Content Distribution in Tachyon Platform

Nomad 7.0.200 in 1E Client 5.1 - uses ActiveEfficiency

Nomad 7.0.100 in 1E Client 5.0 - uses ActiveEfficiency

Nomad 7.0 in 1E Client 4.1 - uses ActiveEfficiency

9.6.12.3.8 CentralMCastExtraDelayMins

An integer value that sets the delay for receiving Central Multicast. Normally you would not need to set this value.

> **Warning**
>
> The Multicast feature is not supported in the Tachyon 5.2 release. This feature is under consideration for re-design and may be available in future versions of Nomad.

Registry value	Default value	Notes	Installer property
CentralMCastExtraDelayMins	n\a	This registry value does not exist until a successful central multicast has run. If problems occur during the multicast and the message and you get a Too late for Central Multicast message in the local Nomad client logs, increase the value.	None

9.6.12.3.9 CertIssuer

Defines one or more certificate issuers that Nomad will use to select the appropriate PKI certificate for the:

Configuration Manager (CM) client authentication certificate - used when downloading over HTTPS from Distribution Points and when communicating with Management Points during pre-caching

Nomad Server Authentication certificate - used to share content between peers over HTTPS

Client Authentication certificate - used for certificate-based client authentication when sharing content between peers over HTTPS.

In most cases Nomad will be able to identify a suitable certificate in the Local Computer Personal certificate store without needing to specify CertIssuer (refer to Peer copy over HTTP or HTTPS: Certificate Selection for more details). You should use CertIssuer if the CM client is not using PKI certificates and there are multiple Client Authentication certificates issued by different Certificate Authorities in the store, and if there is a chance some of those certificates may not be trusted by other peers or CM site systems.

Registry value	Default value	Notes	Installer property
CertIssuer	" "	Set this value to the name of the certificate issuer (Certificate Authority (CA)) that Nomad should use to select the appropriate PKI certificate. A case-insensitive substring-within-a-string match is performed. If you have multiple CAs you can specify a: Common sub-string (e.g. "CORPCA" would work for certificates issued by CORPCA1 or CORPCA2) Comma-separated list of certificate issuers (both exact names or substrings are acceptable values). For example, "DigiCert,Thawte,Verisign" would work for certificates issued by DigiCert, DigiCert EV, Thawte or Verisign. If you are only using HTTPS for downloading from an HTTPS DP (That is, not using HTTPS for peer-to-peer data transfer) you can leave this blank and set CertSubject instead.	MODULE.NOMAD.CERTISSUER

9.6.12.3.10 CertSubject

Defines one or more certificate subject names that Nomad uses to select the appropriate PKI certificate for authentication with Configuration Manager (CM) site systems configured to use HTTPS. It does not affect certificate selection for client authentication certificates used for peer-to-peer authentication or for selection of server authentication certificates.

In most cases Nomad will be able to identify a suitable certificate in the Local Computer Personal certificate store without the need to specify CertSubject (refer to Peer copy over HTTP or HTTPS: Certificate Selection for more details).

Registry value	Default value	Notes	Installer property
CertSubject	" "	For downloads over HTTPS from the Distribution Point, set either the CertIssuer or CertSubject registry values. Set this value to the subject name of the certificate that Nomad should use to select the appropriate PKI certificate. The match has the following properties: case-insensitive a substring search is done, so if the text is set to ACME it will return certificates where ACME appears anywhere in the certificate's subject. If you have multiple valid subject names you can specify a: Common sub-string, for example "contoso.com" would work for certificates that have contoso.com anywhere in the subject name Comma-separated list of subject names or sub-strings, for example, you can specify multiple subject domain suffixes, for example "contoso.com,abc.in". For the installer property, configure either MODULE.NOMAD.CERTISSUER or MODULE.NOMAD.CERTSUBJECTinstaller properties for HTTPS downloads.	MODULE.NOMAD.CERTSUBJECT

9.6.12.3.11 CompatibilityFlags

Determines different compatibility settings which relate to specific customer related functionality and should not generally be changed from the default value under normal conditions, unless advised.

Registry value	Default value	Notes	Installer property
CompatibilityFlags	0x1E18000A (504889354)	For Nomad in full OS, the REG_DWORD registry value is set to the sum of the values for the required bits. The default value combines the following settings: *Bit 1 - 0x00000002* - Enable longer values for hashes *Bit 3 - 0x00000008* - Fix wrong IPs in election messages *Bit 19 - 0x00080000* - Enable full hash generation for SIS content on DPs *Bit 20 - 0x00100000* - Abort download on the Nomad client if an LsZ has mismatch is detected *Bit 25 - 0x02000000* - Turn off Dynamic Block Size *Bit 26 - 0x04000000* - Enable download of Windows 10 Express File Updates *Bit 27 - 0x08000000* - Enable download of Software Updates (including Windows 10 feature updates) from Microsoft Update - see note *Bit 28 - 0x10000000* - Enable support for byte-range downloads (e.g. Office 365 or delta content for updates) from Microsoft Update - see note First bit is bit 0. The default in binary is: 0001 1110 0001 1000 0000 0000 0000 1010 **Support for downloading updates from Microsoft Update** Setting bits 27 and/or 28 will enable Nomad to download content from Microsoft Update if the update has been deployed with Configuration Manager and the option **If software updates are not available on distribution point in current, neighbor or site boundary, download content from Microsoft Update** has been enabled on the	MODULE.NOMAD.COMPATIBILITYFLAGS

Registry value	Default value	Notes	Installer property
		Download Settings tab of the deployment. Nomad will not be used to download updates from Microsoft Update if the update is requested outside of a Configuration Manager Software Update Deployment (e.g. when using Windows Update for Business). **Note** Prior to 1E Client 4.1 (Nomad 7.0) the default was 0x00180000 (1572864): *Bit 19 - 0x00080000* - Enable full hash generation for SIS content on DPs *Bit 20 - 0x00100000* - Abort download on the Nomad client if an LsZ has mismatch is detected	
0x00100002 (1048578)	For the task sequence action **Install and configure Nomad in Windows PE**, the registry value is set to the sum of the values for the required bits. The default value combines the following settings: *Bit 1 - 0x00000002* - Enable longer values for hashes *Bit 20 - 0x00100000* -		

Registry value	Default value	Notes	Installer property
	Abort download on the Nomad client if an LsZ has mismatch is detected **Note** *Bit 1 - 0x00000002* (Enable longer values for hashes) is mandatory. The installer property must be set to sum of the values for the required bits, and given in decimal notation. For example, the following installer command-line uses: *Default- 0x1E18000A* *Bit 0 - 0x00000001* -		

Registry value	Default value	Notes	Installer property
	Never check hashes of downloaded content *Bit 17 - 0x00020000* - Disable DelegatedLSZ checks and errors *Sum - 0x1E1A000B* (505020427) `> msiexec /i 1E.Client-x64.msi MODULE.NOMAD.COMPATIBILITYFLAGS=505020427 [other properties] /qn`		

Bit	Hex	Decimal	Description
0	*0x0001*	1	Never check hashes of downloaded content.
1	*0x0002*	2	Enable longer values for hashes. This value is auto-enabled when the Configuration Manager client is detected. You must manually configure this setting on any DP that does not have the Configuration Manager client installed. **Note** Prior to 1E Client 4.1 (Nomad 7.0) this was disabled (0) by default.
2	*0x0004*	4	Calculate CRCs as files are downloading.

Bit	Hex	Decimal	Description
3	*0x0008*	8	Fix wrong IPs in election messages. On multi-homed machines sometimes the IP from a wrong adapter can get sent in the election messages resulting in peers failing to connect to the master. Enabling this flag causes Nomad to correct such IPs at the time when messages are received and thus prevent master connectivity issues.
4	*0x0010*	16	Determines compatibility with Nomad v3.x caches. Set this option once all Nomad v3.x installations have been upgraded.
5	*0x0020*	32	Disable all RDC data generation.
6	*0x0040*	64	Keep Packages that failed the CRC test during P2P or download from DP.
7	*0x0080*	128	Prevent computers using wireless connections from becoming fill-in multicast masters.
8	*0x0100*	256	Include LinkLocal IPv4 addresses.
9	*0x0200*	512	Include LinkLocal IPv6 addresses.
11	*0x0800*	2048	RESERVED
12	*0x1000*	4096	Do not automatically jump from HTTP to HTTPS during download from DP.
13	*0x2000*	8192	Always use HTTPS. (Use this setting when Configuration Manager is configured to use HTTPS-only communication for downloading content from Distribution Points)
14	*0x4000*	16384	RESERVED
15	*0x8000*	32768	RESERVED
16	*0x00010000*	65536	RESERVED (this flag is no longer used; previously this flag disabled a workaround for the issue described in Nomad post-installation tasks: IIS request filtering)

Bit	Hex	Decimal	Description
17	*0x00020000*	131072	Disable DelegatedLSZ checks and errors.
18	*0x00040000*	262144	Disable partial download when App-V streaming, i.e. download entire application.
19	*0x00080000*	524288	Enable full hash generation for SIS content when an LsZ file is generated on a DP. If this is not enabled, SIS content is trusted, and corrupted content may be downloaded. Enabled by default.
20	*0x00100000*	1048576	Abort download on the Nomad client if an LsZ hash mismatch is detected. If this is not set, when a Nomad client detects a hash mismatch it will re-request LsZ generation on the DP then try again, and get stuck in a loop if the SIS content is corrupt. Must be set on clients if Bit 19 is set on DPs. Enabled by default.
25	*0x02000000*	33554432	Turn off Dynamic Block Size. This flag is set by default, which means Dynamic Block Size is disabled by default. **Note** Prior to 1E Client 4.1 (Nomad 7.0) this bit was off, meaning **Dynamic Block Size** was enabled by default.
26	*0x04000000*	67108864	Enable download of Windows 10 Express update files. Enabled by default. **Note** This is a new setting in 1E Client 4.1 (Nomad 7.0) and Q20144 for NomadBranch 6.3.201.
27	*0x08000000*	134217728	Enable download of full file software updates from Microsoft Update when deployed through Configuration Manager (see Support for downloading updates from Microsoft Update). Enabled by default. **Note** This is a new setting in 1E Client 4.1 (Nomad 7.0) and Q20246 for NomadBranch 6.3.201.

Bit	Hex	Decimal	Description
28	*0x10000000*	268435456	Enable download of byte-range software updates (e.g. Express updates, O365 updates) from Microsoft Update when deployed through Configuration Manager >(see Support for downloading updates from Microsoft Update). Enabled by default. **Note** This is a new setting in 1E Client 4.1 (Nomad 7.0) and Q20246 for NomadBranch 6.3.201.
30	*0x40000000*	1073741824	Enable SoftwareUpdate metadata validation. This is not enabled by default. It can be used to resolve rare issues related to SoftwareUpdates where the contents could be updated without any change in its ID or version. Please refer to Resolving SoftwareUpdate metadata validation for more details. **Note** This is a new setting in 1E Client 5.1 (Nomad 7.0.200).

9.6.12.3.12 ContentProviderOnWifi

Determines whether a device on a WLAN can become content provider. By default, only devices connected to a LAN can become content providers when using Single Site Download (SSD).

Note

This setting is only applicable to SSD and has no effect on P2P content transfers on the local subnet.

Registry value	Default value	Notes	Installer property
Platform\ ContentProviderOnWifi	0	Values are: 0 – Only devices connected to a LAN can be content providers 1 – Devices connected to any network (including	MODULE.NOMAD.CONTENTPROVIDERONWIFI

Registry value	Default value	Notes	Installer property
		WLANs) can be content providers	

9.6.12.3.13 ContentRegistration

Determines if content in Nomad's cache (packages, applications, software updates, boot images, etc.) is registered with Content Distribution. Content registration is necessary if a host is to be available as a Single Site Download (SSD) provider or can be woken up if a Nomad peer requires the content locally.

Registry value	Default value	Notes	Installer property
Platform\ ContentRegistration	0	To enable content registration, update the value to 1 – it is found under the Platform\ContentDistribution To enable SSD when you install Nomad, you must specify the MODULE.NOMAD.SSDENABLED installer property and ensure the Tachyon client is enabled by specifying SWITCH and BACKGROUNDCHANNELURL installer properties. If MODULE.NOMAD.SSDENABLED is specified during installation, the registry value of ContentRegistration is automatically set to 1. If you want to enable SSD as a provider after installation, then you also need to configure the registry values for	MODULE.NOMAD.CONTENTREGISTRATION

Registry value	Default value	Notes	Installer property
		SSDEnabled and ContentRegistration, in addition to enabling the Tachyon client. The ContentDistribution registry setting is found under the Platform key. Nomad app provides visibility of content distribution activity Single Site Download (SSD) Single Site Peer Backup Assistant (SSPBA) High Availability Peer Backup Assistant (HAPBA) Get Migration Settings task sequence action used to manage computer associations Nomad Pre-caching Nomad Download Pause. In legacy versions of Nomad, Platform features were provided using ActiveEfficiency. This required the PlatformURL setting to be configured. This is no longer required. You will see that the PlatformURL registry is used, but this is configured automatically by Nomad on startup by querying the value that the Tachyon	

Registry value	Default value	Notes	Installer property
		client is using (stored in the 1EClient.conf file).	

9.6.12.3.14 ContentRegSyncBatchSz

Warning

ContentRegSyncBatchSz is obsolete. Its value may exist in the Nomad registry, but it is not used. Instead, please refer to CacheStateSyncIntervalMinutes.

The **Content Registration Sync Cycle** is available in Nomad 7.0 (1E Client 4.1) which registers pending and failed content registrations with ActiveEfficiency. Please refer to Single-site download: Improved resilience of content registration.

Registry value	Type	Default value	Notes	Installer property
ContentRegSyncBatchSz	REG_DWORD	30	Number of content registrations that will be attempted in each content registration cycle. Range: from 5 to 100 registrations per run.	none

9.6.12.3.15 ContentRegSyncCycleHrs

Warning

ContentRegSyncCycleHrs is obsolete. Its value may exist in the Nomad registry, but it is not used. Instead, please refer to CacheStateSyncIntervalMinutes.

The **Content Registration Sync Cycle** is available in Nomad 7.0 (1E Client 4.1) which registers pending and failed content registrations with Content Distribution. Please refer to Single Site Download: Improved resilience of content registration.

Registry value	Type	Default value	Notes	Installer property
ContentRegSyncCycleHrs	REG_DWORD	24	A periodic cycle that does pending content registrations.The value specifies	none

Registry value	Type	Default value	Notes	Installer property
			the periodic run of the cycle in HOURS. Setting it to 0 means the feature is turned off and Nomad will not run the content registration sync cycle. Range: from 4 hours to 168 hours (1 week). When this registry value is set to **non-zero** the feature is enabled, and Nomad sets the following two registry values: ContentRegSyncReqDelay is set to 1000 millisecs ContentRegSyncBatchSz is set to 30	

9.6.12.3.16 ContentRegSyncReqDelay

Warning

ContentRegSyncReqDelay is obsolete. Its value may exist in the Nomad registry, but it is not used. Instead, please refer to CacheStateSyncIntervalMinutes.

The **Content Registration Sync Cycle** is available in Nomad 7.0 (1E Client 4.1) which registers pending and failed content registrations with Content Distribution. Please refer to Single Site Download: Improved resilience of content registration.

Registry value	Type	Default value	Notes	Installer property
ContentRegSyncReqDelay	REG_DWORD	1000	Delay, in milliseconds, between successive content registration API calls to Content Distribution. Range: from 100 milliseconds to 60000 milliseconds (1 minute).	none

9.6.12.3.17 Debug

The level of messages logged in the Nomad logs for debugging purposes.

Registry value	Default value	Notes	Installer property
Debug	0x09 (9)	See the table below for customer supported values. The default is a combination of *0x01* (Minimal logging) and *0x08* (Registry changes). For example, to set maximum debugging, set bit 0, 3 and 4, which is a value of 0x19 hexadecimal or 25 decimal. Values on the installer command-line must be provided in decimal. So to set maximum debugging you would use the following installer command-line: `> msiexec /i 1E.Client-x64.msi DEBUG=25 [other properties] /qn` Bit / Hex / Decimal / Description 0 / 0x01 / 1 / Minimal logging. 1 / 0x02 / 2 / RESERVED 2 / 0x04 / 4 / RESERVED 3 / 0x08 / 8 / Registry changes. 4 / 0x10 / 16 / Additional debugging (should only be used if requested by 1E support).	MODULE.NOMAD.DEBUG

9.6.12.3.18 DebugDynamicBlock

The level of messages related to the Dynamic Block Size (DBS) feature logged in the Nomad logs for debugging purposes.

> **Note**
>
> This DWORD registry value does not exist by default and must be created under HKLM\SOFTWARE\1E\NomadBranch if you want to enable debugging for the DBS feature.

<table>
<tr><th>Registry value</th><th>Default value</th><th>Notes</th><th>Installer property</th></tr>
<tr><td>DebugDynamicBlock</td><td>The value does not exist by default. This is the equivalent of 0x0 where DBS logging is off.</td><td>This may take one of the following values:
<table><tr><th>Bit</th><th>Hex</th><th>Decimal</th><th>Description</th></tr><tr><td></td><td>0x0</td><td>0</td><td>Turns DBS logging off. This is also the default where the DebugDynamicBlock value does not exist.
Note
To maximize performance DebugDynamicBlock should not be created or if it exists it should be set to 0. You only need to change this setting if you are actively debugging the use of the DBS feature.</td></tr><tr><td>0</td><td>0x01</td><td>1</td><td>Normal log level where changes in block size as DBS ramps up and down are logged.</td></tr><tr><td>1</td><td>0x02</td><td>2</td><td>Verbose log level where various DBS parameters are logged such as: the time taken to download a block, speed and delta.</td></tr></table></td><td>None</td></tr>
</table>

9.6.12.3.19 DeliveryOptimizationReportingEnabled

Enables Delivery Optimization monitoring and reporting if ContentRegistration is enabled.

Registry value	Default value	Notes	Installer property
DeliveryOptimizationReportingEnabled	0	Enables monitoring of Delivery Optimization downloads and reporting them to Tachyon Platform (ContentDistribution). Delivery Optimization monitoring and reporting is only supported in versions of Windows Server 2019 and Windows 10 Version 1909 onwards. When it is enabled, DO download events get written to .etl files in the Nomad cache folder, for example: NomadDo-20210325-182415.etl. And aggregated information about the downloads gets writtern to sqlite files **Do.db** and **DoDownloadMonitor.db** in LocalDb folder inside Nomad cache folder.	MODULE.NOMAD.DOREPORTINGENABLED

9.6.12.3.20 DownloadTimeout

Sets the timeout in seconds after which a job will be cancelled if the download has not been successful.

Registry value	Default value	Notes	Installer property
DownloadTimeout	0	This parameter is associated with the distribution point resilience feature and is used in conjunction with the *RecycleDPDelay* registry value. If a value greater than zero is set, the download timeout will either use this or the Configuration Manager setting depending on which is the smaller value. When the timeout is reached, the job package download is cancelled and a success is sent to the Configuration Manager client with the *ERROR_MAXDURATION* timeout error sent as the package status message. The default is to use the Configuration Manager setting (28 days by default).	MODULE.NOMAD.DOWNLOADTIMEOUT

9.6.12.3.21 DpCacheCleanupEnabled

Delete all obsolete LSZ files on the DP where the associated content is no longer present in ContentLib.

<table>
<tr><th>Registry value</th><th>Default value</th><th>Notes</th><th>Installer property</th></tr>
<tr><td>DpCacheCleanupEnabled</td><td>0 (turned off)</td><td>This entry controls the cached LSZ files cleaning feature. When turned on, this feature deletes all LSZ files in a Distribution Point (DP) cache where the associated content is not present in ContentLib.

The following table describes the values this entry may be set to:

<table><tr><th>Value</th><th>Description</th></tr><tr><td>0</td><td>The feature is turned off. This is the default.</td></tr><tr><td>1 (or greater)</td><td>The feature is turned on.</td></tr></table>
Please refer to Cache management for details about other cache management settings.</td><td>MODULE.NOMAD.DPCACHECLEANUPENABLED</td></tr>
</table>

9.6.12.3.22 DPNotAvailableCodes

Determines which error codes will cause Nomad to retry a download using an alternative distribution point.

Registry value	Default value	Notes	Installer property
DPNotAvailableCodes	0x205A, 0x205D	This registry entry contains a comma-separated list of return codes, see Nomad return codes for a list of the possible ones. If Nomad encounters one of these during download it will attempt a retry from an alternative DP. It gets the list of possible DPs from Configuration Manager. The two return codes set as default are the only ones that are applicable to DP availability: 0x205A – in valid special package path (set using *--pp*) 0x205D – DP path not found Under normal circumstances, you would not change this from the default value. You may want to not allow failover to an alternative DP altogether, in which case you would set the value to " " in the registry. Or you may only want to failover if the DP path was not found, in which case you would set the value to 0x205D only. This installer property should be set to a string containing the comma-separated hex values. For example the following sets Nomad to failover to the next DP only	MODULE.NOMAD.DPNOTAVAILABLECODES

Registry value	Default value	Notes	Installer property
		when the DP path was not found: `> msiexec /i 1E.Client-x64.msi DPNOTAVAILABLECODES="0x205D" [other properties] /qn`	

9.6.12.3.23 EncryptionType

Determines the type of encryption used by Nomad to encrypt its communications between Nomad peers.

Registry value	Default value	Notes	Installer property
EncryptionType	0x0 (0)	Value are: 0 – standard Nomad encryption 1 – FIPS encryption	MODULE.NOMAD.USEFIPS

9.6.12.3.24 EnforceQuotas

Determines whether Windows Disk Quotas (if configured) are enforced on the PBA share defined inCachePath.

Registry value	Default value	Notes	Installer property
NMDS\ EnforceQuotas	0x0 (0)	Enables quotas to be enforced but requires Windows Disk Quotas to be configured. If the size specified in the NMDS_POLL request causes the quota to be exceeded, the request fails and you get disk full error. This registry value is found under the PBA registry key NomadBranch\NMDS.	MODULE.NOMAD.ENFORCEQUOTAS

9.6.12.3.25 ExtraReplyDelayMs

Time by which PBA peer reply window should be extended to avoid network spikes.

When a machine sends a PBA message like POLL all peers do not reply at the same time. They spread their replies out across a time window. This is done to avoid network spikes such as ARP or UDP storms. The default reply window size of 100ms is mostly enough, but sometimes proves inadequate especially in large subnets. In such cases the window can be extended by the number of milliseconds specified in this registry setting.

Registry value	Default value	Notes	Installer property
NMDS\ ExtraReplyDelayMs	0x0 (0)	Located under the PBA registry key NomadBranch\NMDS. Maximum allowed value is 5000	None

9.6.12.3.26 GenerateWEREvents

Determines whether Windows Error Reporting memory dumps should be sent to Microsoft Winqual.

Registry value	Default value	Notes	Installer property
GenerateWEREvents	1	If enabled and if Nomad experiences an unexpected failure, a dialog is displayed prompting the user to send the debug information to Winqual which is forwarded to 1E for continued quality improvements. Values are: 0 disables this feature 1 enables this feature	MODULE.NOMAD.GENERATEWEREVENTS

9.6.12.3.27 HAACKTimeoutMins

The time-out period in minutes for the Peer Backup Assistant - High Availability (PBA-HA) task sequence action. If a machine running this action does not receive an acknowledgement message within this period from the PBA host performing the additional backups, the action will fail.

Registry value	Default value	Notes	Installer property
NMDS\ HAACKTimeoutMins	20	Applies to synchronized backups only. The PBA tost sends the acknowledgement messages back to the machine running the task sequence approximately every 5% of the synchronized copy. This registry value is found under the PBA registry key NomadBranch\NMDS.	MODULE.NOMAD.HAACKTIMEOUTMINS

9.6.12.3.28 InstallationDirectory

The installation directory for Nomad.

Registry value	Default value	Notes	Installer property
InstallationDirectory	%PROGRAMFILES%\1E\Client\Extensibility\NomadBranch	This registry value must not be modified. It records the locations of Nomad client executables, and is derived from the installation location of the 1E Client.	1E Client settings: INSTALLDIR

9.6.12.3.29 KnownMobileDevices

Note

This feature is retired. We are currently working on a new feature to replace this which will be made available in a future release.

Mobile device connections known to Nomad. When a device running the Nomad client uses a mobile connection whose identifier appears on this list, it will only receive packages that have the --mobok command-line switch set.

Registry value	Default value	Notes	Installer property
KnownMobileDevices	VNClite*,Vodafone*	A list of mobile devices restricting the delivery of packages to only those that contain the *--mobok* command-line switch.	MODULE.NOMAD.KNOWNMOBILEDEVICES

9.6.12.3.30 LocalCachePath

The location of local Nomad package cache.

Registry value	Default value	Notes	Installer property
LocalCachePath	%ALLUSERSPROFILE%\1E\NomadBranch\	There are two registry values called LocalCachePath that are used by Nomad. The LocalCachePath REG_SZ registry value under the HKLM\Software\1E\NomadBranch key sets the path to the local Nomad package cache.	MODULE.NOMAD.CACHEPATH

Registry value	Default value	Notes	Installer property
		The LocalCachePath REG_SZ registry value under the HKLM\Software\1E\NomadBranch\NMDS key sets the path to the PBA package cache. The path is created if it does not exist. If the drive letter does not exist, and it is not possible to create the specified path, *%TEMP%* is used. Default values are dependent on OS. **Known issue fixed in latest accumulated hotfix** The value for the installer property CACHEPATH requires a trailing backslash \. When Nomad is installed on a DP this location is also used for the LSZFiles vDir folder. If LocalCachePath does not contain a trailing backslash, then: the LSZFILES folder is incorrectly created (LocalCachePathLSZFILES instead of LocalCachePath\LSZFILES) IIS vDIR points to wrong folder (LocalCachePathLSZFILES instead of LocalCachePath\LSZFILES) LSZGEN fails because it is attempting to store LSZ files to non-existent path (LocalCachePath\LSZFILES)	

Registry value	Default value	Notes	Installer property
		PBA cache is also derived from the same installer property MODULE.NOMAD.CACHEPATH, but it is stored in the registry value> CachePath in the NomadBranch\NMDS registry key.	

9.6.12.3.31 LocalSsdStagger

Sets the site SSD query stagger duration (seconds).

Deployments to large numbers of clients (30,000 or more) generate significant network traffic from 1E Client to Content Distribution that may result in IIS 503 Overload errors on the server, causing content registrations and SSD requests to fail. LocalSsdStagger allows an elected subnet master to wait for a random configurable time before making a local SSD request. All peers in the subnet participating in the election would also synchronize and wait for the same time before copying from master machine.

Registry value	Type	Default value	Notes	Installer property
LocalSsdStagger	REG_DWORD	5	Sets the local SSD query stagger duration in seconds. The stagger is 0 (disabled) by default. The maximum value that can configured is 600 seconds (10 minutes). There is no SSD staggering in WinPE. Local SSD happens when only when network	MODULE.NOMAD.LOCALSSDSTAGGER

Registry value	Type	Default value	Notes	Installer property
			broadcast is disabled. **Note** Please consult 1E before changing this value. This setting works in conjunction with SiteSsdStagger.	

9.6.12.3.32 LogFileName

The path and filename of the Nomad log file.

For details of log files for 1E Client and other Nomad features, please refer to Log files.

Registry value	Default value	Notes	Installer property
LogFileName	%ALLUSERSPROFILE%\1E\NomadBranch\LogFiles\NomadBranch.log	The location and name of the Nomad log and preserved when you upgrade Nomad. **Note** If Nomad is installed using 1E Client Deployment Assistant (CDA) (previously 1E Endpoint Agent Installation Solution Accelerator (EAISA) and Endpoint Agent Installer (EAI)).	Based on a combination of the MODULE.NOMAD.LOGPATH and MODULE.NOMAD.LOGNAME installer properties.

Registry value	Default value	Notes	Installer property
		You might find the log file in: *C:\WINDOWS\CCM\Logs\NomadBranch.Log*	

9.6.12.3.33 MaxAllocRequest

Sets the maximum amount of space in MB that can be requested by each PBA client.

Registry value	Default value	Notes	Installer property
NMDS\MaxAllocRequest	0xC8 (200)	Located under the PBA registry key NomadBranch\NMDS.	MODULE.NOMAD.MAXALLOCREQUEST

9.6.12.3.34 MaxAllowedLinkSpeed

(Optional setting) If set, defines the maximum possible link speed in bits per second.

Registry value	Default value	Notes	Installer property
MaxAllowedLinkSpeed	0	If greater than 0, a fixed cap method is implemented where Nomad's bandwidth usage cannot exceed the set value. This is useful for lines that have burst mode which affects the initial automatic bandwidth calculations. The minimum value is 0 which sets Nomad to use its calculated bandwidth value. The maximum effective value is the total capacity of the link in question.	None

9.6.12.3.35 MaxBusyBackOffSecs

The maximum duration (in seconds) that Nomad backs-off between blocks of data.

Registry value	Default value	Notes	Installer property
MaxBusyBackOffSecs	20	Governs Nomad's multicast and peer-to-peer behaviour.	None

9.6.12.3.36 MaxCacheDays

When the Nomad cache cleaner runs, delete any application or package content that last triggered Nomad elections before the specified number of days ago.

Registry value	Default value	Notes	Installer property
MaxCacheDays	0 (turned off)	Set to delete application or package content that last triggered Nomad elections before the specified number of days from the date the cache cleaner runs. This ensures that only application or package content that have triggered elections recently will be kept in the cache. 0 means that application and package content will not be deleted automatically when the cache cleaner runs. Please refer to Cache management for details about other cache management settings.	MODULE.NOMAD.MAXCACHEDAYS

9.6.12.3.37 MaxCacheDaysThreshold

This is the maximum number of days content is present on a client.

Registry value	Type	Default value	Notes	Installer property
MaxCacheDaysThreshold	REG_DWORD	0	This is the maximum number of	MODULE.NOMAD.MAXCACHEDAYSTHRESHOLD

Registry value	Type	Default value	Notes	Installer property
			days content is present on a client. If it's not zero, then content will be deleted without any other checks once it reaches the threshold. If the threshold has a value greater than zero and less than 30, Nomad uses the threshold of 30 days and creates an associated log. Default value is 0. New setting introduced in 8.0.	

Registry value	Type	Default value	Notes	Installer property
			Please refer to Cache management for details about other cache management settings.	

9.6.12.3.38 MaxCacheSizeMB

Provided for backward compatibility only – use PercentAvailableDisk instead. The value (in bytes) for the maximum size the cache is allowed to grow to, before automatic cache cleaning takes place.

Registry value	Default value	Notes	Installer property
MaxCacheSizeMB	0	There is no maximum value for this property. This method for determining the maximum size of the cache is an alternative to PercentAvailableDisk: If PercentAvailableDisk has a value greater than zero set its method will be used to control the cache size. If *MaxCacheSizeMB* is set to a value greater than zero and PercentAvailableDisk is set to zero then *MaxCacheSizeMB* will be used as the method for determining the maximum size of the Nomad cache.	MODULE.NOMAD.MAXCACHESIZEMB

9.6.12.3.39 MaxConcurrency

Sets the maximum number of concurrent PBA sessions that may be in use on the host.

Registry value	Default value	Notes	Installer property
NMDS\ MaxConcurrency	0x3 (3)	Located under the PBA registry key NomadBranch\NMDS.	MODULE.NOMAD.MAXCONCURRENCY

9.6.12.3.40 MaxDevicesFromAE

The maximum number of devices with the content that Nomad can retrieve from Content Distribution in one call.

Registry value	Default value	Notes	Installer property
MaxDevicesFromAE	10	The maximum number of devices (i.e. machines) with the content (package, application or software update) that Nomad can retrieve from Content Distribution in one call. The maximum value is 20.	MODULE.NOMAD.MAXDEVICESFROMAE

9.6.12.3.41 MaxElectionResponseLogging

Defines the number of election responses Nomad will write to the log for a given election.

Registry value	Default value	Notes	Installer Property
MaxElectionResponseLogging	By default this REG_DWORD value is not present and all election responses are logged.	Add this REG_DWORD value and set it to the number of responses that Nomad should log for any	MODULE.NOMAD.MAXELECTIONRESPONSELOGGING

Registry value	Default value	Notes	Installer Property
		given election. Setting the value to 0 effectively turns off logging of any election responses.	

Note

The value of MaxElectionResponseLogging specifies the number of election replies to be logged per election request. As an example, if MaxElectionResponseLogging = 5 and there are two election requests for the same package at different times, a maximum of 5 election responses will be logged for each elections (up to 10 election replies in total). If there are two concurrent election requests for the same package, the number of maximum election replies logged may vary from 5 to 10. In general, if MaxElectionResponseLogging = *n* and if there are *m* concurrent election requests for the same package, the number of maximum election replies logged may vary from *n* to *m***n*.

9.6.12.3.42 MaximumMegaByte

The maximum amount of space (in MB) that can be used for all the PBA shares combined on the host.

Registry value	Default value	Notes	Installer property
NMDS\MaximumMegaByte	0	A non-zero value enables PBA share. This registry value is located under the PBA registry key NomadBranch\NMDS.	MODULE.NOMAD.MAXIMUMMEGABYTE

9.6.12.3.43 MaxLogFileSize

The maximum size (in bytes) of the Nomad log file. Default is 5MB.

Registry value	Default value	Notes	Installer property
MaxLogFileSize	5242880	When the log file reaches this size, it is renamed with a *.LO_* extension and a new *.LOG* file is created. The *.LO* file is overwritten each time. **Note** The default has been increased from 1048576 (1MB) to 5242880 (5MB) for Nomad 7.0 onwards (1E Client 4.1). **Note** The installer property name is different to the registry name.	MODULE.NOMAD.MAXLOGSIZE

9.6.12.3.44 MaxPackageSizeFastLAN

The maximum size (in bytes) of a package that Nomad attempts to cache on a Fast LAN (>500 kbps) connection.

Registry value	Default value	Notes	Installer property
MaxPackageSizeFastLAN	0	Works in conjunction with the RunUncachedPermittedFastLAN registry value. **Note** The installer property name is different to the registry name.	MODULE.NOMAD.MAXPACKAGEFAST

9.6.12.3.45 MaxPackageSizeRAS

The maximum size (in bytes) of a package that Nomad will attempt to cache on a RAS (<55 kbps) connection.

Registry value	Default value	Notes	Installer property
MaxPackageSizeRAS	0	**Note** The installer property name is different to the registry name.	MODULE.NOMAD.MAXPACKAGERAS

9.6.12.3.46 MaxPackageSizeSlowLAN

Maximum size (in bytes) of a package that Nomad attempts to cache on a Slow LAN (55-500 kbps) connection.

Registry value	Default value	Notes	Installer property
MaxPackageSizeSlowLAN	0	**Note** The installer property name is different to the registry name.	MODULE.NOMAD.MAXPACKAGESLOW

9.6.12.3.47 MaxPacketsPerSecond

The maximum rate at which multicast packets are sent.

> **Warning**
>
> The Multicast feature is not supported in the Tachyon 5.2 release. This feature is under consideration for re-design and may be available in future versions of Nomad.

Registry value	Default value	Notes	Installer property
MaxPacketsPerSecond	800	Modify this value with caution. If packets are sent too fast, machines will drop packets and multicast will not be effective - too slow and multicast	MODULE.NOMAD.MAXPACKETSPERSECOND

Registry value	Default value	Notes	Installer property
		works, but slowly. The default value is indicative of how this should be set.	

9.6.12.3.48 MaxPreCacheDays

When the Nomad cache cleaner runs, delete any pre-cached content that last triggered Nomad elections before the specified number of days ago.

Registry value	Default value	Notes	Installer property
MaxPreCacheDays	0 (turned off)	Set to delete pre-cached content that last triggered Nomad elections before the specified number of days from the date the cache cleaner runs. This ensures that only pre-cached content that has triggered elections recently will be kept in the cache. 0 means that pre-cached content will not be deleted automatically when the cache cleaner runs. Please refer to Cache management for details about other cache management settings.	MODULE.NOMAD.MAXPRECACHEDAYS

9.6.12.3.49 MaxStatusFrequency

he minimum interval (in seconds) between sending transfer progress status messages, thereby governing the overall maximum frequency for sending the messages.

Registry value	Default value	Notes	Installer property
MaxStatusFrequency	3600	Works in conjunction with the ++sm setting on the Nomad properties tab and the StatusMsgEvents registry values.	MAXSTATUSFREQUENCY

9.6.12.3.50 MaxStuckCount

Registry value to hold an integer determining the number of times Nomad attempts to copy content and gets stuck before aborting.

If you update the registry, you must restart the Nomad service for you changes to take effect. We recommend backing up your registry before you do this.

Registry value	Default value	Notes	Installer property
MaxStuckCount	100	The number of times Nomad attempts to copy content after failure (such as network outages, incomplete LSZ files, hash mismatches, election issues, connecting with peers) before it aborts the operation. The range is 3 to 1000, but if the value is less than 3 or greater than 1000, it sets to the default of 100. **Warning** The MaxStuckCount value is an internal NomadBranch registry value. You should not change this value unless advised by 1E.	MODULE.NOMAD.MAXSTUCKCOUNT

9.6.12.3.51 MaxSUCacheDays

When the Nomad cache cleaner runs, delete any software updates that last triggered Nomad elections before the specified number of days ago.

Registry value	Default value	Notes	Installer property
MaxSUCacheDays	0 (turned off)	Set to delete software updates that last triggered Nomad elections before the specified number of days from the date the cache cleaner runs. This ensures that only software updates that have triggered elections recently will be kept in the cache. 0 means that software updates will not be deleted automatically when the cache cleaner runs. Please refer to Cache management for details about other cache management settings.	MODULE.NOMAD.MAXSUCACHEDAYS

9.6.12.3.52 MaxWorkRates

MaxWorkRates is a registry key, that must be created, to hold registry values for each day of the week (Day0 to Day6) where the hourly maximums for the variable work rates are set.

Registry values	Default value	Notes	Installer property
MaxWorkRates\Day#		Hourly variable workmates can be set throughout the day. The days of the week are labelled: **Day0** to **Day6** where **Day0** = Sunday, **Day1** = Monday etc. Each day value is REG_SZ string set as a comma separated list of 24 hourly work rates for that day. Each value can be set from 1-100. The following is an example for setting for the Day# values where on Sunday, a maximum work rate of 20% will be used. On Monday, the max	None.

Registry values	Default value	Notes	Installer property

		work rate between 0:00-05:59 is 80%, between 06:00-17:59 is 20% and between 18:00-23:59 is it 80% again. For the rest of the week, the work rate specified on the command-line is used. If neither work rate is specified, the default is 80%.
		
		`Windows Registry Editor Version 5.00`
		
		`[HKEY_LOCAL_MACHINE\SOFTWARE\1E\NomadBranch\MaxWorkRates]`
		`"Day0"="20,20,20,20,20,20,20,20,20,20,20,20,20,20,20,20,20,20,20,20,20,20,20,20"`
		`"Day1"="80,80,80,80,80,80,20,20,20,20,20,20,20,20,20,20,80,80,80,80,80,80"`
		`"Day2"=""`
		`"Day3"=""`
		`"Day4"=""`
		`"Day5"=""`
		`"Day6"=""`	

Nomad allows hourly variable work rates to be set throughout the day enabling organizations to use different maximum percentage of available bandwidth during the working day and in the evenings. Intra-day work rates are set on the client using the *MaxWorkRates* registry value. If the intra-day work rate is less than that defined on the command-line, it will override the command-line value. If the intra-day work rate is higher than that defined on command-line, the command-line value is used in preference.

Note

Work rates only apply to transfers from a DP not to P2P transfers within a LAN.

Work rate override arguments

The intra-day work rates can be overridden using the --wro and --wr Nomad command-line arguments.

If these two arguments are combined, the value for the --wr switch is used in preference to the intra-day work rate set in the registry

If only the --wro argument is used, any intra-day value is overridden with a default maximum of 80%

If using intra-day work rates and the --wr argument only, the lower of the two values is used.

9.6.12.3.53 MultiCastMADCAPScope

The MADCAP scope for multicast.

Warning

The Multicast feature is not supported in the Tachyon 5.2 release. This feature is under consideration for re-design and may be available in future versions of Nomad.

Registry value	Default value	Notes	Installer property
MultiCastMADCAPScope	SMSNomad	Values may be set using either of the formats in the table below.	MODULE.NOMAD.MADCAPSCOPE

Format	Description
<ScopeName>	*<ScopeName>* is the name of a scope defined in the DHCP (if you are using the Microsoft implementation of MADCAP). Use this format if you have multiple MADCAP servers. This method uses the time to live settings for the scope.
<MADCAP_ServerIP>	*<MADCAP_ServerIP>* is the IP address of a specific MADCAP server
<MADCAP_Scope_IP> *<TTL>*	*<MADCAP_ScopeIP>* is the starting IP address for a MADCAP scope defined in the DHCP (if you are using the Microsoft implementation of MADCAP) *<TTL>* is the time to live for the multicast packets **Note** Using a TTL greater than 1 is not recommended unless you have ensured that multicast traffic cannot leak back upstream through any intervening routers. The valid range for TTL is a number between 1 and 255 Nomad is also capable of performing control multicast without a MADCAP server installation on the network. In order to use this feature, the *<MADCAP_ServerIP>* must be set to *0.0.0.0*. For example, the following supports MADCAP server not being present, with a scope of *239.0.9.0* and a time to live of *3*. `0.0.0.0,239.0.9.0,3`

9.6.12.3.54 MulticastSupport

The behavior of local multicast.

Warning

The Multicast feature is not supported in the Tachyon 5.2 release. This feature is under consideration for re-design and may be available in future versions of Nomad.

Registry value	Default value	Notes	Installer property
MulticastSupport	0x0 (0)	All machines in a single branch must be configured using the same value for this parameter. If you are not using multicast, deploy the Nomad branch agent with theMODULE.NOMAD.MULTICASTSUPPORT property set to 0 to reduce the noise in Nomad logs. Prior to Nomad 7.0 multicast was enabled (0x1) by default. Now it is disabled (0x0) by default.	MODULE.NOMAD.MULTICASTSUPPORT

Bit	Hex	Decimal	Description
	0x0	0	**No Multicast**– disables the feature.
0	0x1	1	**Data Only Multicast** – choose this for a standard Nomad multicast. Data refers to the content of the downloaded package. Nomad control communications are broadcast as normal on the local subnet. Select this option for standard functionality.
1	0x2	2	**Control Only Multicast** – control information refers to the communications between Nomad enabled machines, especially for elections. This may be used if there is more than one subnet in a single location to enable a single Nomad master to be elected for all the subnets.
	0x3	3	**Control and Data Multicast** – data and control information is multicast.

Bit	Hex	Decimal	Description
			Select this option if a branch has multiple subnets connected by high speed routers.

9.6.12.3.55 NoHardlink

Determines whether hard links are used between the Nomad cache and the Configuration Manager cache.

Registry value	Default value	Notes	Installer property
NoHardlink	0	Values are: 0 – hard links are used. The Nomad cache will link to the Configuration Manager cache so only a single copy of a package is held locally. 1 – hard links are not used and results in the content being double-cached For more detail about the Nomad Cache please refer to Nomad cache.	MODULE.NOMAD.NOHARDLINK

9.6.12.3.56 NomadInhibitedADSites

Prevents Nomad from calling an election when it is connected to a specified AD site, meaning that each Nomad client on the listed AD sites will automatically become a Nomad master. This prevents P2P sharing, as each master downloads its own copy of the content.

Registry value	Default value	Notes	Installer property
NomadInhibitedADSites	(empty)	A comma-separated list for each AD site to be inhibited. Useful for sites with: a local DP a VPN without isolation	MODULE.NOMAD.NOMADINHIBITEDADSITES

Registry value	Default value	Notes	Installer property
		For example, to inhibit three AD sites called site1, site2 and site3: `site1,site2,site3` Please refer to Design Considerations: Inhibiting subnets and sites.	

9.6.12.3.57 NomadInhibitedSubnets

Prevents Nomad from calling an election when it is connected to a specified IP subnet, meaning that each Nomad client on the IP subnet automatically becomes a Nomad master. This prevents P2P sharing, as each master downloads its own copy of the content.

Registry value	Default value	Notes	Installer property
NomadInhibitedSubnets	(empty)	A comma-separated list of each subnet to be inhibited in CIDR notation. Useful for sites with either of the following: a local DP a VPN without isolation For example, to isolate two subnets: `10.2.0.0/16,192.168.9.0/24`	MODULE.NOMAD.NOMADINHIBITEDSUBNETS

Registry value	Default value	Notes	Installer property
		Please refer to Design Considerations: Inhibiting subnets and sites.	

9.6.12.3.58 NomadNeverUseSubnets

Prevents Nomad from using specific network adaptors based on the IP subnet. For example, this can be used to exclude Server backup subnets.

Registry value	Default value	Notes	Installer property
NomadNeverUseSubnets	" "	A comma-separated list of each subnet to be inhibited in CIDR notation. When Nomad is excluded from using a subnet, it attempts other cards available to that machine. If no other cards are available, Nomad will wait until one comes available. For example, 192.168.100.0/24	None.

9.6.12.3.59 NoSsdReqOnInhibitedSubnets

Determines whether local and site SSD requests are disabled from elected masters located in NomadInhibitedSubnet.

Registry value	Type	Default value	Notes	Installer property
NoSsdReqOnInhibitedSubnets	REG_DWORD	0	Possible values are 0 or 1. If the value is set to 1 thenthe Nomad client will not send local or site SSD requests to ContentDistribut	MODULE.NOMAD.NOSSDREQONINHIBITEDSUBNETS

Registry value	Type	Default value	Notes	Installer property
			ion if both of the following are true: the Nomad client is an elected master the *connected* adapter's IP address subnet is present in the Nomad registry NomadInhibited Subnet registry	

9.6.12.3.60 P2P_Port

Port used to broadcast election messages, for connectionless cache access and package status broadcasts.

Registry value	Default value	Notes	Installer property
P2P_Port	1779		MODULE.NOMAD.P2PPORT

9.6.12.3.61 P2PClientCertWaitPeriodMins

Defines the number of minutes that Nomad waits from the start time of the download job for a valid client authentication certificate before failing the download job.

Registry Value	Default value	Notes	Installer Property
P2PClientCertWaitPeriodMins	1440	Number of minutes (0 to 4294967295 (MAXDWORD)).	None

9.6.12.3.62 P2PDisqualifyMaxNumPeers

Defines the max number of devices which a device will disqualify during a peer-to-peer copy.

If you update the registry, you must restart the Nomad service for you changes to take effect. We recommend backing up your registry before you do this.

Registry value	Default value	Notes	Installer property
P2PDisqualifyMaxNumPeers	5	A device does not further disqualify a peer if it has disqualified P2PDisqualifyMaxNumPeers number of peers within last P2PDisqualifyMaxWindowMins minutes. **Warning** The P2PDisqualifyMaxNumPeers value is an internal NomadBranch registry value. You should not change this value unless advised by 1E.	MODULE.NOMAD.P2PDISQUALIFYMAXNUMPEERS

9.6.12.3.63 P2PDisqualifyMaxWindowMins

Defines the max number of minutes within which a device will disqualify a peer during a peer-to-peer copy.

If you update the registry, you must restart the Nomad service for you changes to take effect. We recommend backing up your registry before you do this.

Registry value	Default value	Notes	Installer property
P2PDisqualifyMaxWindowMins	60	A device does not further disqualify a peer if it has disqualified P2PDisqualifyMaxNumPeersn umber of peers within last	MODULE.NOMAD.P2PDISQUALIFYMAXWINDOWMINS

Registry value	Default value	Notes	Installer property
		P2PDisqualifyMaxWindowMins minutes. **Warning** The P2PDisqualifyMaxWindowMins value is an internal NomadBranch registry value. You should not change this value unless advised by 1E.	

9.6.12.3.64 P2PElectionWeight

Determines the outcome of Nomad elections.

Registry value	Default value	Notes	Installer property
P2PElectionWeight	The registry value does not exist, and dynamic election weighting is used.	Nomad performs automatic weighting depending on its situation, according to the criteria listed below, and stores the value in memory (not registry). The higher the value, the greater the probability of winning the election. 61 – the agent is running on a server OS and it is not a domain controller (DC) 40 – the agent is running on a laptop 30 – the agent is running on a wireless network 10 – the agent is running on WinPE 50 – default	None

Registry value	Default value	Notes	Installer property
		If necessary, you can use the P2PElectionWeight registry setting to increase or decrease a Nomad client's probability of being elected a master. The range for this registry value must be between 0 and 99 inclusive. If not set, Nomad uses the values listed above. The registry key is located at: *HKLM\software\1e\NomadBranch\P2PElectionWeight* To take effect after setting the registry value, the client sevice must be restarted. This method is not recommended because Nomad is already quite efficient in the way it elects a master and needs very little intervention in this process. However, you may want to reduce the chance of computers with low processing power, or prevent critical servers, becoming a master. You should also consider the following points before you influence the weighting: Use this technique in exceptional circumstances and only after testing has shown that you need to make a particular computer more or less likely to be elected as a master for specific operational reasons. Choose the simplest weighting strategy possible - for example, set servers at 90, laptops at 10 and workstations at 50. The weighting does not guarantee that the more heavily weighted computers will win the election – they may be turned off or another local peer may have already cached more of the requested content. The final weighting value used by the computer during an election may differ from the registry value as Nomad will automatically adjust it depending on the chassis and the network connection used.	

Registry value	Default value	Notes	Installer property
		In the event you no longer need the values to be set, you should remove it and restart the service to resume dynamic election weighting. Setting to 0 is a special case called Sensitive server weighting designed for use on critical servers. The 0 value prevents Nomad from acting as master, and devices with this value will not respond to election requests.	

9.6.12.3.65 P2PEnabled

Determines how the Nomad cache is accessed. Please refer to Nomad cache for more details.

Registry value	Default value	Notes	Installer property
P2PEnabled	9	The default (Hex 0x0009) configures P2P to use SMB and Net Literal Names. You can set more than one option at the same time by combining the bit values. See the table below for details. **Note** We recommend restarting the Nomad Branch service when you modify this parameter.	MODULE.NOMAD.P2PENABLED

Bit	Hex	Decimal	Notes
0	0x0001	1	(Default) Use the SMB protocol to share its own cache, and create the NomadSHR file share upon the start of the Nomad service, unless the CustomShare option has been enabled in SpecialNetShare. When P2PEnabled is set in addition to Bit 5 (use HTTP) or Bit 6 (use HTTPS), Nomad will attempt to use HTTPS/HTTP and will fall-back to SMB if HTTPS/HTTP is unavailable on other peers. To disable SMB P2P, set this bit to 0.

Bit	Hex	Decimal	Notes
1	0x0002	2	Enable connectionless P2P server.
2	0x0004	4	Enable connectionless P2P client.
3	0x0008	8	(Default) Use Net Literal Names when connecting to P2P shares. This causes Nomad to use the Nomad master's IP address when connecting to the share and is recommended when running wirelessly.
4	0x0010	16	Use FQDN when connecting to P2P shares. Recommended when using a multi-forest environment where computers from different forests may be present in the same subnet. This requires that reverse lookup for IP addresses is correctly configured and running. If this is not available Nomad will revert to using the IP address for connecting to the P2P shares.
5	0x0020	32	Use the HTTP protocol to share its own cache and access other caches.
6	0x0040	64	Use the HTTPS protocol to share its own cache and access other caches.

9.6.12.3.66 P2PHttpPort

The HTTP port to use for peer copy.

Registry value	Default value	Notes	Installer property
P2PHttpPort	5080	Default HTTP port to use for peer copy. If you are using a custom port, ensure that all agents use the same custom port.	MODULE.NOMAD.P2PHTTPPORT

9.6.12.3.67 P2PHttpsPort

Registry value	Default value	Notes	Installer property
P2PHttpsPort	5443	Default HTTPS port to use for peer copy. If you are using a custom port, ensure that all agents use the same custom port.	MODULE.NOMAD.P2PHTTPSPORT

9.6.12.3.68 P2PSslSettings

Defines server and client authentication options when using HTTPS for P2P content transfer (i.e. P2PEnabled 0x60 option is set).

Registry value	Default value	Notes	Installer property
P2PSslSettings	0	The default value (0) configures Nomad to use a self-signed certificate for server authentication and disables certificate-based client authentication. P2PSslSettings is a numeric value where, when represented in binary, each bit represents a configurable option as defined in the table below. You can combine these options to derive the required value, for example setting P2PSslSettings to 3 (0x1 + 0x2) configures Nomad to use a PKI certificate for server authentication and also enables certificate-based authentication. These options are only applicable if the HTTPS protocol has been enabled in the P2PEnabled setting. If you are using PKI certificates you must deploy the certificates to all clients before enabling this option. Refer to Peer copy over HTTP or HTTPS for further details on using HTTPS and associated authentication.	MODULE.NOMAD.P2PSSLSETTINGS

Bit	Hex	Decimal	Notes
0	0x0001	1	If not set (0), use self-signed certificate for server (Master) authentication

Bit	Hex	Decimal	Notes
			If set (1), use PKI certificate for server (Master) authentication
1	0x0002	2	Enables certificate-based client authentication (Requires a PKI client authentication certificate) **Note** If this option is enabled and the Configuration Manager client is using self-signed client authentication certificates (or Nomad is being used outside of CM), you should specify CertIssuer to ensure Nomad uses the intended certificate.

9.6.12.3.69 PercentAvailableDisk

The limit on the Nomad cache. Specified as a percentage of the available disk space, it controls the automatic cache cleaning to ensure that the cache does not grow to a size whereby the percentage of available disk space is less than this value.

Registry value	Default value	Notes	Installer property
PercentAvailableDisk	10	By default, the cache will not grow such that less that 10% of total disk space is available. The maximum value is 80. The cache will not grow beyond 20% of the total available disk space. This method for determining the maximum size of the cache is provided as an alternative to MaxCacheSizeMB: If PercentAvailableDisk is greater than zero, its method is used to control the cache size If MaxCacheSizeMB is greater than zero and PercentAvailableDisk is	MODULE.NOMAD.PERCENTAVAILABLEDISK

Registry value	Default value	Notes	Installer property
		zero, MaxCacheSizeMB is used as the method for determining the maximum size of the Nomad cache.	

9.6.12.3.70 PercentDelayedContentReg

Warning

PercentDelayedContentReg is obsolete. Its value may exist in the Nomad registry, but it is not used. Instead, **Content Registration Sync Cycle** is now used, please refer to CacheStateSyncIntervalMinutes.

The **Content Registration Sync Cycle** is available in the following versions of 1E Client, where the Nomad client registers pending and failed content registrations with ActiveEfficiency or Tachyon Platform. Please refer to Single Site Download: Improved resilience of content registration.

Nomad 7.1 in 1E Client 5.2 - uses Content Distribution in Tachyon Platform

Nomad 7.0.200 in 1E Client 5.1 - uses ActiveEfficiency

Nomad 7.0.100 in 1E Client 5.0 - uses ActiveEfficiency

Nomad 7.0 in 1E Client 4.1 - uses ActiveEfficiency

{mul

Registry value	Type	Default value	Notes	Installer property
PercentDelayedContentReg	REG_DWORD	0	Do not modify this setting unless advised by 1E.	none

9.6.12.3.71 PermittedLSZShares

Restricts Nomad LSZ file generation requests to a list of permitted package source locations.

Registry value	Default value	Notes	Installer property
PermittedLSZShares	SMSPKG*$	A list of comma-separated package source locations. Enables increased security and is only used by the	MODULE.NOMAD.PERMITTEDLSZSHARES

Registry value	Default value	Notes	Installer property
	SMS_DP_SMSPKG*$	Nomad client installed on a distribution point. Nomad LSZ file generation requests will only be completed if the content location is listed. If you are using additional package source locations, you must manually add these to this registry value. *PermittedLSZShares* can incorporate wildcard characters to provide flexible naming convention support. If you leave the registry value blank, security checks on package source locations are not carried out. **Note** When Configuration Manager (specifically Distribution Point servers) is configured to use HTTPS only, you must also add *NOCERT_SMS_DP_SMSPKG*$* and CCMTOKENAUTH_SMS_DP_SMSPKG*$ to the PermittedLSZShares registry value.	

9.6.12.3.72 PlatformURL

Note

Platform features are now enabled by using the BackgroundChannelUrl instead of PlatformURL.

The URL of the Tachyon Platform, specifically the Tachyon Background Channel, which provides a reverse proxy for the Content Distribution component of Tachyon Platform. Usually of the form *https://<BackgroundChannelServer>:<BackgroundChannelPort>/Background/*

Registry value	Default value	Notes	Installer property
Platform\ PlatformURL	(empty)	Located under the following registry keys, depending on the component. For *NomadBranch*, it is found under *HKLM\Software\1E\NomadBranch\Platform* For *NomadBranchAdminUIExt* on 64-bit machines, it is found under *HKLM\Software\Wow6432Node\1E\NomadAdminUI\Platform* For *NomadBranchAdminUIExt* on 32-bit machines, it is found under *HKLM\Software\1E\NomadAdminUI\Platform* **Warning** Do not configure this registry setting, it is automatically configured on service startup. To enable SSD when you install Nomad, you must specify the MODULE.NOMAD.SSDENABLED installer property and ensure the Tachyon client is enabled by specifying SWITCH and BACKGROUNDCHANNELURL installer properties. If MODULE.NOMAD.SSDENABLED is specified during installation, the registry value of ContentRegistration is automatically set to 1. If you want to enable SSD as a provider after installation, then you also need to configure the registry values for SSDEnabled and ContentRegistration, in addition to enabling the Tachyon client. The ContentDistribution registry setting is found under the Platform key. Nomad app provides visibility of content distribution activity Single Site Download (SSD) Single Site Peer Backup Assistant (SSPBA) High Availability Peer Backup Assistant (HAPBA) Get Migration Settings task sequence action used to manage computer associations	Not applicable.

Registry value	Default value	Notes	Installer property
		Nomad Pre-caching Nomad Download Pause. In legacy versions of Nomad, Platform features were provided using ActiveEfficiency. This required the PlatformURL setting to be configured. This is no longer required. You will see that the PlatformURL registry is used, but this is configured automatically by Nomad on startup by querying the value that the Tachyon client is using (stored in the 1EClient.conf file).	

9.6.12.3.73 PostCompleteTimeoutHours

The duration (in hours) after which the PBA share is deleted from the host.

Registry value	Default value	Notes	Installer property
NMDS\PostCompleteTimeoutHours	0xA8 (168)	Only applies to a PBA share after the NMDS_COMPLETE command has been run for it, otherwise the PreCompleteTimeoutHours value will apply. The intention is that an incomplete share will only be available for a short period of time, defined in PreCompleteTimeoutHours. Once the NMDS_COMPLETE command is sent, it will be fixed for this longer time. When the share is deleted the	MODULE.NOMAD.POSTCOMPLETETIMEOUTHOURS

Registry value	Default value	Notes	Installer property
		folder and associated user will be removed. This registry value is found under the PBA registry key NomadBranch\NMDS.	

9.6.12.3.74 PrecachePollBatchSize

The number of notifications a client processes in one pre-cache poll cycle.

Registry value	Default value	Notes	Installer property
PrecachePollBatchSize	20	Range is 1 to 500. If the value is greater than 500, it defaults to 500. If you set the value to 0, it defaults to 20.	None

9.6.12.3.75 PrecachePollMinutes

The interval (in minutes) between Nomad polling Content Distribution for new pre-cache jobs.

Registry value	Default value	Notes	Installer property
PrecachePollMinutes	0x5A0 (1440)	Nomad clients normally start their polling cycle when the service starts-up, with a random delay to minimize the possibility of concurrent polls from different clients. The range is 60 - 525600 (1 year). 0 disables polling	MODULE.NOMAD.PRECACHEPOLLMINUTES

9.6.12.3.76 PreCompleteTimeoutHours

The duration (in hours) after which PBA share is deleted from the host.

Registry value	Default value	Notes	Installer property
NMDS\PreCompleteTimeoutHours	0x3 (3)	Located under the PBA registry key NomadBranch\NMDS, it only applies to a PBA share after the NMDS_POLL command has been run, but not the NMDS_COMPLETE command. The intention is that an incomplete share will only be available for a short period of time. When the share is deleted the folder and associated user is removed.	MODULE.NOMAD.PRECOMPLETETIMEOUTHOURS

9.6.12.3.77 RandomizeRemotePaths

Allows you to enable and disable the remote paths randomization for CM and pre-cache jobs.

When Nomad begins content download, its content is pulled from the same distribution point by every client. For example, If a site has four Distribution Points (DP), the first one in the list is always used for downloading. In a very large environment, this can put an unnecessary load on a single DP.

Using**RandomizeRemotePaths**Nomad can randomize the content location list.

<table>
<tr><th>Registry value</th><th>Type</th><th>Default value</th><th>Notes</th><th>Installer property</th></tr>
<tr><td>RandomizeRemotePaths</td><td>REG_DWORD</td><td>0</td><td>By default, RandomizeRemotePaths is not present in the Nomad registry hive. To change the value, you need to create it and set your desired value.

You can enable and disable the remote paths randomization for either Configuration Manager (CM) or pre-cache jobs using the following bits:

<table><tr><th>Bit</th><th>Hex</th><th>Decimal</th><th>Notes</th></tr><tr><td>0</td><td>0x0001</td><td>1</td><td>Enable remote paths randomization for CM jobs.</td></tr><tr><td>1</td><td>0x0002</td><td>2</td><td>Enable remote paths randomization for Pre-cache jobs.</td></tr></table></td><td>MODULE.NOMAD.RANDOMIZEREMOTEPATHS</td></tr>
</table>

9.6.12.3.78 RecycleDPDelay

The delay (in seconds) before restarting retries from the first DP after the whole list of available DPs have been tried.

Registry value	Default value	Notes	Installer property
RecycleDPDelay	600	It is associated with the distribution point resilience feature and is used in conjunction with DownloadTimeout. The default equates to 10 minutes.	MODULE.NOMAD.RECYCLEDPDELAY

9.6.12.3.79 RunUncachedPermittedFastLAN

Determines where the download package is run from under certain conditions.

Registry value	Default value	Notes	Installer property
RunUncachedPermittedFastLAN	0	Works in conjunction with MaxPackageSizeFastLAN (which needs to contain a value value greater than zero). Values are: 0 – do not run package from the distribution point. 1 – run package directly from the distribution point if there is either insufficient disk space to create the cache, or the maximum package threshold is exceeded but the connection is fast (>500kbps). To ensure that the un-cached mode works correctly, set	MODULE.NOMAD.PERMITUNCACHED

Registry value	Default value	Notes	Installer property
		the Program Environment Properties to include the Drive mode/Require drive letter option.	

9.6.12.3.80 SigsFolder

The path to the Configuration Manager signature files.

Registry value	Default value	Notes	Installer property
SigsFolder	C:\SMSSIG$	Relates to RDC integration and must point to the folder where the signature files are held for Configuration Manager. Wildcards are not allowed. For example: `E:\SMSSIG$` When it is not set, Nomad assumes that signature files location as *`C:\SMSSIG$`*, if it exists.	MODULE.NOMAD.SIGSFOLDER

9.6.12.3.81 SiteSSDMinPackageSizeKB

Allows you to configure a minimum content size before making an SSD request.

Registry value	Type	Default value	Notes	Installer property
SiteSSDMinPackageSizeKB	REG_DWORD	0	The default value is 0 which can be changed after installation when it will be an	MODULE.NOMAD.SITESSDMINPACKAGESIZEKB

Registry value	Type	Default value	Notes	Installer property
			installer property. There is no lower limit for this key, upper limit is 10240. If the registry value is greater than 10240, the agent will only consider 10240 and will log a warning. Size of content is first taken from Job data, if that's not available it's taken from the LST file, if it's not present there, this key is ignored and an SSD request is made irrespective of size. **Note**	

Registry value	Type	Default value	Notes	Installer property
			This check is for site SSD, not for local SSD.	

9.6.12.3.82 SiteSsdStagger

Sets the site SSD query stagger duration (seconds).

Deployments to large numbers of clients (30,000 or more) generate significant network traffic from 1E Clients to ContentDistribution that may result in IIS 503 Overload errors on the server, causing content registrations and SSD requests to fail. SiteSsdStagger allows an elected subnet master to wait for a random configurable time before making a site SSD request. All peers in the subnet participating in the election would also synchronize and wait for the same time before copying from master machine.

Registry value	Type	Default value	Notes	Installer property
SiteSsdStagger	REG_DWORD	0	Sets the site SSD query stagger duration in seconds. The stagger is 0 (disabled) by default. The maximum value that can configured is 300	MODULE.NOMAD.SITESSDSTAGGER

Registry value	Type	Default value	Notes	Installer property
			seconds (5 minutes). There is no SSD staggering in WinPE. Site SSD happens when broadcast is enabled or if local SSD is enabled and it does not return any devices from ActiveEfficiency. **Note** Please consult 1E before changing this value. This setting works in conjunction with LocalSsdStagger.	

9.6.12.3.83 SpecialNetShare

Sets various special feature options related to the Nomad share.

Registry value	Default value	Notes	Installer property
SpecialNetShare	0x2060 (8288)	You can set more than one option at the same time by combining the bit values. For example, to have custom share permissions and use the machine account for access to the Nomad share, set the value for SpecialNetShare to 129 (decimal value 1+128 or 0x0081	MODULE.NOMAD.SPECIALNETSHARE

Registry value	Default value	Notes	Installer property
		hex). See for more detail on configuration and security. The default value in different versions has changed, based on feedback. Upgrading does not change the value unless explicitly set. Nomad version / Default in MSI Nomad 8.0 (1E Client 8.0): 0x2060 (8288) — Bit 5: Disables broadcast of download statistics; Bit 6: Enable Nomad FanOut; Bit 13: Use HTTP/S or SMB Nomad 7.1 (1E Client 5.2), Nomad 7.0 (1E Client 4.1 to 5.1): 0x2020 (8224) — Bit 5: Disables broadcast of download statistics; Bit 13: Use HTTP/S or SMB Nomad 6.x: 0x0000 (0) — No special features enabled. The default used in all versions of Client Deployment Assistant	

Registry value	Default value	Notes	Installer property
		(and earlier Endpoint Agent Installer) is 0x2070 (8304): Bit 4: Enable Nomad hidden share as NomadSHR$ Bit 5: Disables broadcast of download statistics Bit 6: Enable Nomad FanOut Bit 13: Use HTTP/S or SMB	

Bit	Hex	Decimal	Description
	0x0000	0	No special features enabled.
0	0x0001	1	Custom Share Permissions: Administrators configure and manage custom share permissions. The service doesn't create the *NomadSHR* share on start-up, leaving the administrator to manually create it and set the permissions. It is also not deleted when the service stops and therefore existing share permissions are preserved.
1	0x0002	2	Enables support for IPv6: If the network supports both IPv6 and IPv4, enable support for both – set bit 1 but not bit 2.
2	0x0004	4	Disables support for IPv4: If the network supports only IPv6, disable IPv4 and set both bit 1 and bit 2.
3	0x0008	8	RESERVED
4	0x0010	16	The Nomad share is hidden and named *NomadSHR$*. When using a hidden share, all Nomad installations must be configured to use this option. See The Nomad share for more detail on configuration and security.
5	0x0020	32	Disables broadcast of download statistics. By default, this is disabled. If enabled, Nomad broadcasts download statistics to all peers when a download is complete.

Bit	Hex	Decimal	Description
			Note Prior to 1E Client 4.1 (Nomad 7.0) this was enabled (0) by default, now it is disabled (1) by default.
6	0x0040	64	Enables Nomad FanOut.
7	0x0080	128	The machine account is used when connecting to a peer client. The SMSNomadP2P& account is not created. Please refer to The Nomad share: Use Machine Account. **Note** Will not work if peers exist in untrusted domains or workgroups.
8	0x0100	256	RESERVED
9	0x0200	512	RESERVED
10	0x0400	1024	RESERVED
11	0x0800	2048	RESERVED
12	0x1000	4096	RESERVED (deprecated)
13	0x2000	8192	Use HTTP/S or SMB. Ensure that this is set if Nomad integration is used by Tachyon. HTTP/S is automatically used if CM client is detected. **Note** Prior to 1E Client 4.1 (Nomad 7.0) this was disabled (0) by default, now it is enabled (1) by default. This setting should be enabled in baseline or other policies.
14	0x4000	16384	Web LSZ generation: enables the Nomad client on Configuration Manager standalone DPs to handle LSZ file generation requests coming from HTTP/HTTPS enabled clients. Used when Nomad clients are configured with either of the following enabled: Bit13 (0x2000) – Use HTTP/S or SMB Bit 15 (0x8000) – Use HTTP/S only, not SMB

Bit	Hex	Decimal	Description
			When enabled, the Nomad distribution point client creates a virtual folder called *LSZFILES*. The permissions for this are copied from the Configuration Manager *SMS_DP_SMSPKGX$* share. By default, access to the LSZFILES folder requires SSL to be enabled. This is the case for Internet facing scenarios where local client access certificates will ensure authentication. If you are using HTTP instead of HTTPS, manually disable SSL on the LSZFILES web folder in order for the Nomad LSZ file generation process to work. Only needs to be enabled when using HTTP or HTTPS on standalone DPs; it is not required on site server DPs because Nomad automatically configures Web LSZ generation on them.
15	0x8000	32768	Use HTTP/S only, not SMB: enables the Nomad client to download content using HTTPS or HTTP depending on the content location provided by Configuration Manager or Tachyon. The Nomad client will not use SMB to download content when this is enabled.

9.6.12.3.84 SSDEnabled

Enables Single Site Download (SSD).

Registry value	Default value	Notes	Installer property
SSDEnabled	0	You can set more than one option at the same time by combining the bit values. For example, to enable clients to fetch downloads using SSD and provide them to peers, set the value to 3 (decimal value 1+2 or 0x3). To enable clients to fetch downloads using site and local SSD and provide them to peers, set the value to 7. To enable SSD when you install Nomad, you must specify the MODULE.NOMAD.SSDENABLED installer property and ensure the Tachyon client is enabled by specifying SWITCH and BACKGROUNDCHANNELURL installer properties. If MODULE.NOMAD.SSDENABLED	MODULE.NOMAD.SSDENABLED

Registry value	Default value	Notes	Installer property
		is specified during installation, the registry value of ContentRegistration is automatically set to 1. If you want to enable SSD as a provider after installation, then you also need to configure the registry values for SSDEnabled and ContentRegistration, in addition to enabling the Tachyon client. The ContentDistribution registry setting is found under the Platform key. Nomad app provides visibility of content distribution activity Single Site Download (SSD) Single Site Peer Backup Assistant (SSPBA) High Availability Peer Backup Assistant (HAPBA) Get Migration Settings task sequence action used to manage computer associations Nomad Pre-caching Nomad Download Pause. In legacy versions of Nomad, Platform features were provided using ActiveEfficiency. This required the PlatformURL setting to be configured. This is no longer required. You will see that the PlatformURL registry is used, but this is configured automatically by Nomad on startup by querying the value that the Tachyon client is using (stored in the 1EClient.conf file). If your network is running over a WLAN or have devices on a wireless network you	

Registry value	Default value	Notes	Installer property
		want to be content providers, set ContentProviderOnWifi=1.	

Bit	Hex	Decimal	Description
	0x0	0	SSD is disabled, the Nomad client takes no part in the SSD on the site.
0	0x1	1	SSD is enabled and the Nomad client fetches downloads using SSD. This setting on its own (without provider mode set) should be used with sensitive server weighting. Provider mode is where a peer gets content from another peer but cannot serve it (it cannot act as a master).
1	0x2	2	SSD is enabled and the Nomad client provides downloads to peers. Enabling this bit causes Nomad to register content with Content Distribution. In practice, this is unlikely to be used on its own. This is automatically disabled for WinPE installations (because cached content is only temporary).
2	0x4	4	Local SSD is enabled and the Nomad client fetches downloads from a local client (also known as a subnet peer master - the term used for local devices which have content but cannot be located during the normal election process because network broadcasts have been disabled) within the subnet. The local SSD feature was introduced to supplement site SSD for clients on networks such as wireless where broadcasts are disabled, to prevent each client becoming its own master and downloading direct from the DP. In a SSD enabled environment, a master queries Content Distribution to get a list of devices on other subnets within the site that have content. With local SSD enabled, the master also queries for devices having content within local subnet. If any local peers with content are available, then the master downloads from them, otherwise it attempts to download from Site peers (other subnets in the site), and if the master still cannot find any peers, it downloads the content direct from the DP. In version 7.0 and later, a master skips using local SSD if it sees broadcast messages from peers. This means clients in mixed network environments can be configured with the same SSDEnabled setting (with Local SSD enabled) and clients can move seamlessly between networks. When on a

Bit	Hex	Decimal	Description
			wireless network (where broadcasts are typically disabled) local SSD can be used. On LAN networks (where broadcasts are typically allowed) local SSD would be skipped because a master is elected and sees broadcast activity from peers. This setting should only be used if networks have broadcasts being disabled (for example wireless networks) and clients are forced to download from the DP as they can't participate in an election. Local SSD requires that a peer on the local subnet be configured to provide downloads to peers, that is at least one client on the subnet must be configured with Bit 1 enabled. To maintain consistency with typical Nomad peer sharing behavior where local SSD is not required, configure all clients with *SSDEnabled=7*. You'll also want to set ContentProviderOnWifi=1. When enabled, the elected master: Queries Content Distribution to get a list of local devices having the content. Queries each of those devices to check if they are available and have the content. The list is ordered by percentage of content the device holds. Repeats the same process for devices on other subnets (existing SSD feature). Stores a list of subnets as well as site devices in memory. Cycles through the list in the following order: Subnet peer master (fetched from list of local devices from Content Distribution) Site master DP. To distinguish between a master derived from Content Distribution and an election, the log records: *Connection::SetDownloadSource = SubnetPeer* (an elected peer) instead of *Connection::SetDownloadSource = Peer* (an SSD peer master).

9.6.12.3.85 SSPBAEnabled

Enables the use of Single Site functionality for PBA data stores. See Single Site peer backup assistant for more details.

Registry value	Default value	Notes	Installer property
SSPBAEnabled	0	Has a dependency on the Tachyon Platform PlatformURL. Values are: 0 – disables single-site integration with ContentDistribution 1 – enables single-site integration with ContentDistribution	MODULE.NOMAD.SSPBAENABLED

9.6.12.3.86 StatusMsgEvents

Determines which Nomad events are reported using Configuration Manager status messages.

Registry value	Default value	Notes	Installer property
StatusMsgEvents	0x0	Nomad can send status messages through Configuration Manager based on specific download events which appear in its deployment status. They are provided mainly for advanced troubleshooting purposes, or for custom reporting solutions. From v7.1 onwards, they are no longer required for the Nomad Dashboard which now gets its status events directly via the Platform Content Distribution feature. However, you may have custom reporting in Configuration Manger that also use these messages, and you can configure this setting accordingly for this purpose. These messages are controlled by the StatusMsgEvents registry value. This is a *REG_SZ* string data type and the format of the parameter must be a 64-bit value. Status messages are only sent when there is an active deployment.	MODULE.NOMAD.STATUSMSGEVENTS

Registry value	Default value	Notes	Installer property
		Warning Status message events should be used with caution as they could impact your Configuration Manager environment when scaled up to tens of thousands of machines. For example, to set the request started, request completed, started copy and master changed events, update the StatusMsgEvents registry value to *0x80002060*. 0x0000000001 – SNO_EVT_START 0x0000000002 – SNO_EVT_STOP 0x0000000004 – SNO_EVT_ERROR 0x0000000008 – SNO_EVT_PAUSED 0x0000000010 – SNO_EVT_RESUMED 0x0000000020 – SNO_EVT_REQUEST_STARTED 0x0000000040 – SNO_EVT_REQUEST_COMPLETED 0x0000000080 – SNO_EVT_SERVICE_RESET 0x0000000100 – SNO_EVT_STARTED_CACHE_MANAGEMENT 0x0000000200 – SNO_EVT_FINISHED_CACHE_MANAGEMENT	

Registry value	Default value	Notes	Installer property
		0x0000000400 – SNO_EVT_STARTED_HASHCHECK 0x0000000800 – SNO_EVT_FINISHED_HASHCHECK 0x0000001000 – SNO_EVT_ELECTION_REQUEST 0x0000002000 – SNO_EVT_MASTER_CHANGED 0x0000004000 – SNO_EVT_FILLIN_MASTER_CHANGED 0x0000008000 – SNO_EVT_MCAST_CENTRALSCHED 0x0000010000 – SNO_EVT_MCAST_ERROR 0x0000020000 – SNO_EVT_MCAST_COMPLETE 0x0000040000 – SNO_EVT_SCHEDULER 0x0000080000 – SNO_EVT_STARTED_TX_CENTRALMCAST 0x0000100000 – SNO_EVT_STOPPED_TX_CENTRALMCAST 0x0000200000 – SNO_EVT_STARTED_TX_ACTIVEMCAST 0x0000400000 – SNO_EVT_STOPPED_TX_ACTIVEMCAST 0x0000800000 – SNO_EVT_STARTED_TX_FILLINMCAST	

Registry value	Default value	Notes	Installer property
		0x0001000000 – SNO_EVT_STOPPED_TX_FILLINMCAST 0x0002000000 – SNO_EVT_STARTED_RX_CENTRALMCAST 0x0004000000 – SNO_EVT_STOPPED_RX_CENTRALMCAST 0x0008000000 – SNO_EVT_STARTED_RX_ACTIVEMCAST 0x0010000000 – SNO_EVT_STOPPED_RX_ACTIVEMCAST 0x0020000000 – SNO_EVT_STARTED_RX_FILLINMCAST 0x0040000000 – SNO_EVT_STOPPED_RX_FILLINMCAST 0x0080000000 – SNO_EVT_STARTED_COPY 0x0100000000 – SNO_EVT_STOPPED_COPY 0x0200000000 – SNO_EVT_WORKRATE_CHANGED 0x0400000000 – SNO_EVT_WRONG_PKG_VERSION 0x0800000000 – SNO_EVT_INFORMATIONAL 0x1000000000 – SNO_EVT_FINALSTATS (see notes below) 0x2000000000 – SNO_EVT_WAIT	

Registry value	Default value	Notes	Installer property

0x4000000000 – SNO_EVT_MAX_EVENTID

SNO_EVT_FINALSTATS notes

For success reporting, this message provides feedback on the status of the download. For example, it can show how much data was received using multicast as opposed to peer-to-peer copying. Turning this message on creates an extra status message per machine for each deployment. The format of the status message is:

```
Evt_FinalStats MD100067 1 170 59195038 170 59195038 0 59195038 0 0
```

Configuration Manager status messages are made up of insertion strings. The strings for the final stats event are:

InstrStr0	Nomad event string (internal reference)	N/A
InstrStr1	Package Id and Package version	MD1000671
InstrStr2	Total number of files in package	170
InstrStr3	Total number of	59195038

Registry value	Default value	Notes			Installer property
			package bytes		
		InstrStr4	Number of files which are cached	170	
		InstrStr5	Bytes which are cached	59195038	
		InstrStr6	Bytes coped from a peer agent (P2P)	0	
		InstrStr7	Bytes copied from the DP	59195038	
		InstrStr8	Bytes received via local multicast	0	
		InstrStr9	Bytes received from a central multicast	0	
		If the package is already cached and is re-deployed with an unchanged package version, the final stats message will not be re-sent.			

9.6.12.3.87 SuccessCodes

A list of Nomad return codes that are translated as success to the Content Transfer Manager (CTM) component of the Configuration Manager client.

Registry value	Default	Notes	Installer property
SuccessCodes	0x206b, 0x2077, 0x103, 0xffffffff, 0x1, 0x70, 0x2050, 0x2051, 0x2052, 0x2053, 0x2054,0x2055, 0x2056, 0x2057, 0x2058, 0x205a, 0x205b, 0x205c, 0x205d, 0x205e, 0x2060, 0x2061,0x2062, 0x2063, 0x2064, 0x2065, 0x2066, 0x2067, 0x2068, 0x2069, 0x209A	This REG_SZ value contains a comma-delimited list of possible Nomad return codes that should be treated as a success and thereby prevent Configuration Manager from attempting to download the content itself or use another Alternate Content Provider (ACP). Any code returned by Nomad that is not on the list will be treated as a failure and trigger the Configuration Manager client to attempt to download the content using alternate means. Nomad also sends a status message to the Configuration Manager site containing its return code. Strictly speaking the Nomad return codes are actually internal status codes, Nomad will only ever return success or failure to the Content Transfer Manager (CTM) component of the Configuration Manager client. When CTM receives a success it passes control to the ExecMgr component of the Configuration Manager client, which attempts to execute the deployment. ExecMgr will fail if Nomad did not download the content and make it available in the Configuration Manager cache. In this case, ExecMgr sends a status message (e.g. failed deployment) back to the Configuration Manager site. If Nomad generates a return code that is not in the list, it passes a fail to the CTM component which causes the Configuration Manager client to try downloading the content itself using BITS, or use another Alternate Content Provider (ACP). This process may itself succeed or fail depending on the	MODULE.NOMAD.SUCCESSCODES (This installer property was introduced in 1E Client 4.1 for Nomad 7.0)

Registry value	Default	Notes	Installer property

conditions that resulted in the original Nomad return code, and may have an undesirable impact on the network.

Note

The special code 0x9999 can be added to the list, or used on its own, to cause Nomad to always return a success to CTM. As a consequence this code is also known as "prevent failover to BITS".

Note

The SuccessCodes list need not be modified under normal circumstances, other than to add or remove the 0x9999 code.

The following table shows the possible Nomad return codes that can be set in the list:

Note

This list is subject to change with each release of Nomad, and provided for reference only.

Return Code	Description	
-1	0xFFFFFFFF	Reserved.
1	0x0001	Reserved.

Registry value	Default	Notes			Installer property
		112	0x0070	Insufficient disk space to create the cache.	
		259	0x0103	Reserved.	
		8272	0x2050	The download has been suspended by APM.	
		8273	0x2051	The user has cancelled this download.	
		8274	0x2052	Invalid command line.	
		8275	0x2053	Command-line execution failure.	
		8276	0x2054	Internal Error.	
		8277	0x2055	The package exceeds the threshold for a RAS connection.	
		8278	0x2056	The package exceeds the threshold for a Slow LAN connection.	
		8279	0x2057	The package exceeds the threshold for a Fast LAN connection.	
		8280	0x2058	Reserved.	

Registry value	Default	Notes			Installer property
		8281	0x2059	Unknown transport. Returned when an attempt is made to download a Software Update from an Internet location (like Microsoft Updates).	
		8282	0x205A	Invalid special package path (set using --pp).	
		8283	0x205B	Incorrect file hash.	
		8284	0x205C	Exited due to a kill request.	
		8285	0x205D	DP path not found.	
		8286	0x205E	The MaxBusyBackOff consecutive event threshold has been exceeded.	
		8287	0x205F	The service has stopped.	
		8288	0x2060	The advertisement has expired.	
		8289	0x2061	Reserved.	
		8290	0x2062	This is an unlicensed version of Nomad.	

Registry value	Default	Notes			Installer property
		8291	0x2063	Invalid alternate cache path (set using --cp).	
		8292	0x2064	No Configuration Manager job data found in WMI.	
		8293	0x2065	Incorrect package hash.	
		8294	0x2066	MaxDuration or execution runtime for this program has been exceeded.	
		8295	0x2067	Reserved.	
		8296	0x2068	Incorrect package version.	
		8297	0x2069	Obsolete package version.	
		8298	0x206A	The BlockSize has been changed during download.	
		8299	0x206B	The "no progress" re-check threshold has been exceeded.	
		8300	0x206C	The parent process has terminated.	

Registry value	Default	Notes			Installer property
		8301	0x206D	Duplicate download for the package.	
		8302	0x206E	The service was reset. This will occur if certain configuration parameters are changed during a download e.g. NomadInhibitedSubnets	
		8303	0x206F	Nomad inhibited.	
		8311	0x2077	Internal error LST incomplete.	
		8346	0x209A	Client certificate missing. Nomad is configured to use certificate-based client authentication but was unable to find an appropriate certificate.	

9.6.12.3.88 SupportWPAD

Provides support for Web Proxy Auto-Discovery Protocol (WPAD).

Nomad always uses System level proxy if it has been set, irrespective of what SupportWPAD has been set to.

SupportWPAD was introduced in v7.1 and when disabled it does not change the default behavior, which is: If system level proxy is set then use it, otherwise access directly without proxy.

When SupportWPAD is enabled in Nomad, the behavior is:

If system level proxy is set then use it and do not try WPAD

If system level proxy is not set then fetch automatic proxy using WPAD and use it

If system level proxy is not set and failed to get automatic proxy using WPAD then try access directly without proxy.

How to know if a system level proxy has been set

```
netsh winhttp show proxy
```

Registry value	Default value	Notes	Installer property
SupportWPAD	0	By default, the WPAD feature is disabled. To enable WPAD in Nomad, add registry key 'SupportWPAD' and set it to 1 at registry path HKLM/Software/1E/NomadBranch To enable or disable the WPAD feature in Nomad: Disable WPAD set SupportWPAD = 0 Enable WPAD set SupportWPAD= 1 (or non-zero value).	MODULE.NOMAD.SUPPORTWPAD

9.6.12.3.89 WakeUpBatchSize

The maximum number of machines to wake up in a single call.

> **Warning**
>
> Nomad integration with WakeUp enables Nomad to share content from its devices that are holding particular content, even if those devices are offline. One reason why peers in the local subnet may not respond to the request even though they have content in their caches is that they are offline (shutdown, in hibernate or sleep mode). However, if WakeUp is integrated, the Nomad client would know which offline device has the content and can wake it up when it queried Content Distribution.
>
> The wake up list is maintained by Content Distribution and is the same list that Single Site Download (SSD) uses. Separate lists of peers are returned for subnet and site. This feature requires Nomad SSD to be enabled, Content Distribution and a NightWatchman infrastructure. The feature is enabled during installation of NightWatchman Management Center. Please refer to Nomad Preparation for requirements.

Registry value	Default value	Notes	Installer property
WakeUpBatchSize	10	Sets the maximum number of machines to wake up in one	MODULE.NOMAD.WAKEUPBATCHSIZE

Registry value	Default value	Notes	Installer property
		call, for subnet and site separately. (So up to twice this number of requests is sent in total if WakeUp is enabled for both subnet and site.) The next batch is launched, if necessary, after a re-election (usually a periodic election). The value cannot be greater than MaxDevicesFromAE, and hence itself cannot be more than 20.	

9.6.12.3.90 WakeUpEnabled

Enables WakeUp integration, see Integrating Nomad with WakeUp for more details.

> **Warning**
>
> Nomad integration with WakeUp enables Nomad to share content from its devices that are holding particular content, even if those devices are offline. One reason why peers in the local subnet may not respond to the request even though they have content in their caches is that they are offline (shutdown, in hibernate or sleep mode). However, if WakeUp is integrated, the Nomad client would know which offline device has the content and can wake it up when it queried Content Distribution.
>
> The wake up list is maintained by Content Distribution and is the same list that Single Site Download (SSD) uses. Separate lists of peers are returned for subnet and site. This feature requires Nomad SSD to be enabled, Content Distribution and a NightWatchman infrastructure. The feature is enabled during installation of NightWatchman Management Center. Please refer to Nomad Preparation for requirements.

Registry value	Default value	Notes	Installer property
WakeUpEnabled	0	Determines the status of the WakeUp integration. If configured by the installer, it is disabled (0) by default. If integration is enabled, Nomad attempts to wake up dormant	MODULE.NOMAD.WAKEUPENABLED

Registry value	Default value	Notes	Installer property
		hosts that are known to have the requested content in their caches. The integration has a dependency on the PlatformURL. To enable integration post-installation, for normal usage, set both bits 0 and 1 (0x3)	

Bit	Hex	Decimal	Description
	0x0	0	Disables WakeUp integration.
0	0x1	1	Enables WakeUp integration only for the local subnet.
1	0x2	2	Enables WakeUp integration only for the site.
	0x3	3	Enables WakeUp integration for the site and the local subnet.

9.6.12.3.91 WakeUpMinPackageSizeMB

The minimum size of content (in megabytes) that will cause a request for a wakeup. See Integrating Nomad with WakeUp for more details.

> **Warning**
>
> Nomad integration with WakeUp enables Nomad to share content from its devices that are holding particular content, even if those devices are offline. One reason why peers in the local subnet may not respond to the request even though they have content in their caches is that they are offline (shutdown, in hibernate or sleep mode). However, if WakeUp is integrated, the Nomad client would know which offline device has the content and can wake it up when it queried Content Distribution.
>
> The wake up list is maintained by Content Distribution and is the same list that Single Site Download (SSD) uses. Separate lists of peers are returned for subnet and site. This feature requires Nomad SSD to be enabled, Content Distribution and a NightWatchman infrastructure. The feature is enabled during installation of NightWatchman Management Center. Please refer to Nomad Preparation for requirements.

Registry value	Default value	Notes	Installer property
WakeUpMinPackageSizeMB	1024	Any content below this size is downloaded from the DP as downloads from the DP for files this size will likely complete before any wakeups will have had a chance to finish. The value can be 0, in which case wakeups will always be attempted. For example, if it is set to 512 and size of the content downloaded is 500 MB, a wake-up request (to site or subnet) is not be sent. Similarly, if size of the content is 600 MB, then wake-up requests (to site and subnet, determined by WakeupEnabled) is be sent. **Note** For standalone downloads (using SMSNomad.exe) and under WinPE, there has no effect as the size of the	MODULE.NOMAD.WAKEUPMINPACKAGESIZEMB

Registry value	Default value	Notes	Installer property
		content cannot easily be determined. Wake-up requests are always sent in these instances.	

9.6.12.3.92 WLanBlipSecs

The duration for temporarily disabling a wireless connection when a wired LAN connection becomes available, to provide time for the OS and Nomad to switch to the LAN connection. This is useful for OS versions and drivers that do not automatically switch to a preferred wired connection.

Registry value	Default value	Notes	Installer property
WLanBlipSecs	0	The value must be 20 seconds or more.	MODULE.NOMAD.WLANBLIPSECS

Nomad provides extra stability by managing a machine's network connections as they move between a wireless and a wired LAN. Depending on the OS version or other factors, once an SMB or HTTP session is running on a wireless connection, it will remain on wireless even when a wired LAN becomes available. Nomad uses **WLanBlipSecs** to temporarily drop a wireless connection when it detects a wired LAN connection, to give time for the OS and Nomad to automatically switch to the LAN connection.

For example, if a Nomad master was initiated when a machine was on a wireless connection and a wired connection subsequently became available, Nomad disables the wireless adapter for a long enough period to enable a switchover to the wired connection. As a result of this, the IP address and the share path will change and peers will log error messages until each peer re-establishes its connection to the master and the new share location.

This feature is turned off by default.

> **Note**
>
> Other applications may be affected when switching from wireless to wired connection.

Irrespective of the **WLanBlipSecs** setting, you can also control which service set identifier (SSID) Nomad connects to by managing a list. To do this, update the NomadBranch WLanProfileList registry value with a comma-delimited list of SSIDs or use the wildcard (*) character for any SSID.

Examples:

```
WLanProfileList REG_SZ WIFIGAP,GUEST
WLanProfileList REG_SZ *
```

9.6.12.3.93 WLanProfileList

A list of wireless SSIDs to enable switching from wireless to wired LAN connections.

Registry value	Default value	Notes	Installer property
WLanProfileList		A comma-delimited list of wireless SSIDs (* for any all) which enables Nomad to switch form wireless to a wired LAN connection when it becomes available.	MODULE.NOMAD.WLANPROFILELIST

9.6.13 Nomad return codes

The following is a list of the Nomad return codes and their descriptions.

> **Note**
>
> This list is subject to change with each release of Nomad, and provided for reference only.

Return Code	Description	
-1	0xFFFFFFFF	Reserved.
1	0x0001	Reserved.
112	0x0070	Insufficient disk space to create the cache.
259	0x0103	Reserved.
8272	0x2050	The download has been suspended by APM.
8273	0x2051	The user has cancelled this download.
8274	0x2052	Invalid command line.
8275	0x2053	Command-line execution failure.

Return Code	Description	
8276	0x2054	Internal Error.
8277	0x2055	The package exceeds the threshold for a RAS connection.
8278	0x2056	The package exceeds the threshold for a Slow LAN connection.
8279	0x2057	The package exceeds the threshold for a Fast LAN connection.
8280	0x2058	Reserved.
8281	0x2059	Unknown transport. Returned when an attempt is made to download a Software Update from an Internet location (like Microsoft Updates).
8282	0x205A	Invalid special package path (set using --pp).
8283	0x205B	Incorrect file hash.
8284	0x205C	Exited due to a kill request.
8285	0x205D	DP path not found.
8286	0x205E	The MaxBusyBackOff consecutive event threshold has been exceeded.
8287	0x205F	The service has stopped.
8288	0x2060	The advertisement has expired.
8289	0x2061	Reserved.
8290	0x2062	This is an unlicensed version of Nomad.
8291	0x2063	Invalid alternate cache path (set using --cp).
8292	0x2064	No Configuration Manager job data found in WMI.
8293	0x2065	Incorrect package hash.

Return Code	Description	
8294	0x2066	MaxDuration or execution runtime for this program has been exceeded.
8295	0x2067	Reserved.
8296	0x2068	Incorrect package version.
8297	0x2069	Obsolete package version.
8298	0x206A	The BlockSize has been changed during download.
8299	0x206B	The "no progress" re-check threshold has been exceeded.
8300	0x206C	The parent process has terminated.
8301	0x206D	Duplicate download for the package.
8302	0x206E	The service was reset. This will occur if certain configuration parameters are changed during a download e.g. NomadInhibitedSubnets
8303	0x206F	Nomad inhibited.
8311	0x2077	Internal error LST incomplete.
8346	0x209A	Client certificate missing. Nomad is configured to use certificate-based client authentication but was unable to find an appropriate certificate.

9.6.14 FIPS compliant communication encryption

Nomad has always provided encryption for most of its communications and uses an advanced FIPS compliant encryption algorithm. The United States Federal Information Processing Standard (FIPS) http://en.wikipedia.org/wiki/FIPS_140-2 is a standard that defines security requirements for software used by the U.S. federal government. It stipulates that applications that encrypt any sensitive data should use only a certain set of approved encryption algorithms.

9.6.14.1 FIPS compliant communication encryption

FIPS encrypts the following types of Nomad data sent over a network in peer-to-peer communications, including:

Election communications

Connectionless data transfer

Nomad FanOut requests

Sign-on/sign-off communication

SSD Package Status Requests

PBA communications.

9.6.14.2 Encryption types

Nomad provides two types of encryption, its default 40-bit RC2 encryption algorithm and FIPS compliant encryption. You can set the encryption type used by Nomad during installation or by modifying a Nomad registry entry.

> **Note**
>
> Nomad clients running different encryption types will be unable to communicate with each other. If you want to use FIPS compliant encryption and earlier versions of Nomad are already deployed, you should roll out Nomad using its default encryption standard. Once all clients have been upgraded, change the encryption level to FIPS compliant.

9.6.14.3 Installing Nomad with FIPS encryption

FIPS encryption can be set when you enable Nomad in the 1E Client. This is done by checking the **Use FIPS encryption** checkbox on the **Nomad** screen of the 1E Client installer, for more information refer to Installing the 1E Client for Nomad.

You can also set FIPS encryption with the MODULE.NOMAD.USEFIPS installer property.

9.6.14.4 Setting FIPS encryption post-installation

To change Nomad's encryption type after installation you can modify the EncryptionType registry value. By default, this is set to 0, for standard Nomad encryption, unless the **Use FIPS encryption** checkbox was checked during installation, in which case it is set to 1.

9.6.15 Glossary

A glossary of Tachyon terminology.

9.6.15.1 Tachyon alphabetical glossary

Term	Definition
1E Client	1E Client provides client features and modules for 1E products including Tachyon. It replaces the Tachyon Agent.

Term	Definition
Action	An Action is a specific type of instruction that is sent to client devices which can be used to modify the state of the target device. For example, setting a registry key, killing a process, deleting a file. Whereas a Question is an instruction that requests information from the target device, but does not change its state. Generally an Action needs to undergo an approval process before it is sent.
Agent	Agent is the old name for the client. The Agent has been replaced by the 1E Client which provides client features and modules for 1E products including Tachyon.
All Instructions Approver	This is a Tachyon system role which allows assigned users to approve actions for all Instruction Sets . Users can approve unless the action was requested by themselves.
All Instructions Questioner	This is a Tachyon system role which allows assigned users to ask questions and view responses for all Instruction Sets; use custom properties.
All Instructions Viewer	This is a Tachyon system role which allows assigned users to view instructions and responses for all Instruction Sets.
Audit information log	The Audit information log page displays audit information related to installation, permissions, instruction set and consumer related operations carried out using the Explorer and Settings applications. See Audit information log page
Historic Data Capture	The old name for Tachyon Activity Record.
Agent Language	The Agent language is an interpretive programming language that is executed by the client in the form of an **instruction payload**. Instructions, and their payload, are based on instruction definitions which are stored in the TachyonMaster database. Definitions are uploaded into the database from the Administrator console by dragging and dropping one or more Instruction Definition files, a Product Pack or ZIP file containing Instruction Definition files.

Term	Definition
	The language, called SCALE, uses Agent modules and methods and is documented in the SDK.
Agent Provider	A plug-in component for the 1E Client which communicates with an external component, such as an operating system facility (for example Windows registry) or a service-provider application (for example Content Distribution). 1E Client modules use Providers to get their work done. Examples: WMI provider Registry provider Nomad provider BASH provider
Auto-curation	Auto-curation is a Catalog function and refers to the automated process of creating match rules in 1E Catalog. These match rules are neither created by the customer not by the 1E curation team. The rules are created in the customer's local 1E Catalog copy using automated logic built by 1E.
Background Channel	The Background Channel is a mechanism by which the Tachyon client can download resources via HTTPS without loading the Switch. Since this traffic does not go through the Switch, the client is still able to receive and process instructions instructions while performing these downloads. From v2.0 onwards, the client is able to download resources via Content Distribution. The Background Channel is a web application on the Tachyon Server Website and provides the following: Stores Tachyon content from the Consumer API in the Background Channel for clients to retrieve Responds to clients retrieving Tachyon content from the Background Channel See Tachyon Architecture and Communication Ports.

Term	Definition
Client module	A plug-in component for the 1E Client which encapsulates business logic. Modules contain Methods, which can be invoked by SCALE. Modules (and their methods) effectively provide a platform independent API. To that end, Modules and their Methods do not (generally) talk about anything platform specific (Windows, Linux, Android etc). Examples: FileSystem OperatingSystem Network Software
Column filters	Some tables contain a column filter that lets you easily filter the information displayed in the table.**Using column filters**The picture opposite shows an example taken from AppClarity. In our example we want to filter the table to show only those items where the **Edition** contains the text **Prof**.To filter the table on the **Edition** column:Click on the filter iconjust beneath the header row in the **Edition** column.The filter popup is displayed.Now select the operator. In our example this will be **contains**.Then type the text **Prof** into the text field.Click **Apply** and a new filter will be added to the table.The table will be filtered to just those items whose **Edition** contains the text **Prof**.**Adding another filter**You can add another filter by clicking on the filter icon for any of the columns. The picture opposite shows another filter added selecting table rows where the **Type** also contains the text **License**. The table will also be filtered accordingly.**Removing filters**You can remove filters by clicking on the filter close icon at the end of the filter.
Column Picker	**Using column picker**Where the column picker control is shown you can choose which columns are displayed. In the following example on the **Microsoft Core License Demand** page we hide the **Unknown Installs** column and move the **License Demand** column to the left of the page.To pick the displayed columns:Click on the Choose columns iconto the right of the header row to view the visible columns.To exclude **Unknown Installs**, select the Unknown Installs row and click **Exclude columns** button.The **Unknown Installs** column is now hidden.To move the **License Demand** column to the top of the list, hover your

Term	Definition
	mouse over **License Demand** and using the direction control drag it to the top of the list.The Microsoft Core License Demand page has now been automatically updated with our changes.
Column sorts	Some tables contain column sorts that let you easily re-order the information displayed in the table.**Using column sorts**The picture opposite shows an example taken from AppClarity. In our example we want to sort the table on the **Cost** column from the highest cost at the top to the lowest at the bottom. To sort the table on the **Cost** column:Click on the sort iconjust beneath the header row in the **Cost** column.The sort popup is displayed.Now select the sort direction. In our example this will be **Sort descending**.After selecting this the data in the table is now sorted on the **Cost** column from highest to lowest and the sort icon has changed to a sort descending icon**Clearing the sort**You can clear the sort by clicking on the sort icon again and selecting the **Clear sorting** menu item from the sorting popup.
Configuration Manager Extensions	The Configuration Manager Extensions currently include. Configuration Manager Agent emergency stop and resume actions Configuration Manager Agent actions Client Health Check Tachyon Run Instruction utility (used by the each of the above right-click actions to request Tachyon to run an instruction) Tachyon Instruction Runner (a mini UI version of the Tachyon Explorer) This feature is included in the Tachyon Toolkit. Documentation for installing and using the Configuration Manager Extensions will be available soon.
Consumer	A Consumer is any application that connects to and uses the Consumer API. An example is the Explorer application.
Consumer API	The Consumer API is a documented set of API endpoints provided by a web application on the Tachyon Web Server called Consumer. It is referred to as the Consumer API in order to avoid confusion with Tachyon Consumers, which are 'consumers' of the API. The Consumer API is a web application on the Tachyon Server Website, actually named Consumer, and provides the following:

Term	Definition
	Processes the consumer requests from the Explorer and other Consumers Publishes Tachyon content to the Background Channel Forwards requests for instrumentation data from the Explorer to the Tachyon Instrumentation component Forwards workflow commands from the Explorer to the Tachyon Workflow component See Tachyon Architecture and Communication Ports.
Consumer requests	A Consumer sends requests to the Consumer API.
Coordinator Service	The Coordinator Service has two modules: Instrumentation module Workflow module See Tachyon Architecture and Communication Ports.
Coordinator Instrumentation module	The Coordinator Instrumentation module is part of the Coordinator Service on the Tachyon Server which processes instrumentation data from the following components: Core Coordinator Workflow module Switch And responds to requests for instrumentation data from the Consumer API. See Tachyon Architecture and Communication Ports.
Coordinator Workflow module	The Coordinator Workflow module is part of the Coordinator Service on the Tachyon Server that provides the following: Forwards workflow commands from the Consumer API to the Core Stores workflow in SQL

Term	Definition
	Connects to remote SMTP to send emails used in the approval process for actions See Tachyon Architecture and Communication Ports.
Core	The Core is a Tachyon Server web component that does the following: Forwards workflow commands from the Coordinator workflow module to the Switch Forwards responses from the Switch to the Responses database (this task requires high throughput) Generates and sends instrumentation data to the Instrumentation service See Tachyon Architecture and Communication Ports.
Core Internal	Core Internal is the part of the Core which allows fast internal communication with the Switch using HTTP instead of HTTPS, restricted to the Switch server's local IP Address only. See Tachyon Architecture and Communication Ports.
Custom Role	Tachyon roles that define which Users have access to which Instruction Set. These roles can be modified in the Administration pages by users assigned to the Full Administrator role.
Custom Properties	Full Administrator can manage the custom properties using the Properties page in Explorer. The only custom property type available after installing the Tachyon server is Coverage tags, further types may be added during installation of other Consumers.
Device tags	Device tags can be used when setting the coverage for a particular question so that only client devices with a particular tag name and value get the question. The names and values of Device tags must be pre-configured by a Full Administrator before setting them on a client device using Device tag actions. Device tags can also be queried directly by Device tag questions.

Term	Definition
	Device tags were previously known as Coverage tags. In 1E Client log files, Device tags are also referenced as scopable tags. Please also see Freeform tags.

DNS Name	DNS Name FQDN is the term used in this documentation to represent the name of a Tachyon Server. Typically a Tachyon Server will have only one DNS Name, which will be the CNAME or an (A) Host record that uniquely represents a server's IP Address. 1E normally recommends using an CNAME record.
	
	In a Tachyon system, each Tachyon Server will have a DNS Name FQDN.
	
	In a single-Switch installation the Switch is on the same server and uses the same DNS Name. When a Response Stack has more than one Switch, each Switch has its own IP Address, so you can choose if the will share the same DNS Name, or if each will have its own DNS Name. The Tachyon Server certificate must have all
	
	`NAME TYPE VALUE`
	`----------`
	`tachyon.acme.com. CNAME tachyon.acme.local.`
	`tachyon.acme.local. CNAME foo.example.com.`
	`foo.example.com. A 192.0.2.23`
	
	`tachyon.acme.com is an Alias record`
	
	`tachyon.acme.local is a CNAME record`
	
	`foo.example.com is a (A) Host record`

Event Subscription	A type of instruction that can be sent to the client. An Event Subscription tells the client to monitor an arbitrary event source for a period of time (defined by the Instruction's TTL), to capture events as they occur and to report them back via the Switch.
Guaranteed State application	The Explorer application is the web portal used by users and administrators. It is an example of a Consumer application. **Note** Explorer can be reached directly using the following URL: `https://<tachyon DNS Name FQDN>/Tachyon/App/#/explorer/`

Term	Definition
	where <tachyon DNS Name FQDN> is the one set up during the preparation phase, as described under the heading DNS Names. It is a web application on the Tachyon Server Website and provides the following: Browser connection providing the Explorer and Administration pages Sends consumer requests to the Consumer API See Tachyon Architecture and Communication Ports.
Filters	There are two kinds of filter: Question filters are used to reduce the responses from the clients; View filters reduce the information displayed in Explorer on the Responses page.
Freeform tags	Freeform tags may be used to set properties on client devices that can subsequently be used in Freeform tag questions. They cannot be used when defining the coverage for a question. Freeform tags can be set with arbitrary names and values that are defined only when running a Freeform tag action. In Tachyon log files, Freeform tags are also known a non-scopable tags. Please also see Device tags.
FQDN	Fully Qualified Domain Name. This is the complete domain name for a specific IP-connected device, and is unique within the network and unambiguous. The FQDN consists of two parts: the hostname and the domain name. For example tachyon.acme.com.
Full Administrator	This is a Tachyon system role which has the combined rights of all the other system roles.
Group Administrator	This is a Tachyon system role which allows assigned users to create, modify and delete Management groups and modify their membership.
Guaranteed State application	Guaranteed State application is used to ensure endpoint compliance to enterprise IT policies. It is an example of a Consumer application. **Note**

Term	Definition
	Guaranteed State can be reached directly using the following URL: `https://<tachyon DNS Name FQDN>/Tachyon/App/#/guaranteedstate/` where <tachyon DNS Name FQDN> is the one set up during the preparation phase, as described in DNS Names.
Instruction	Instruction is the generic term used to describe: Questions Actions An Instruction is sent to one or more clients, and will yield one or more responses.
Instruction Definitions	Instruction Definitions are retrieved from the Core by the Switch. They define the type and functionality of the instructions and are used to control the clients to respond in the appropriate way.
Instruction Definition Files	Instruction Definition files are XML format files that contain definitions for Instructions and any associated resources.
Instruction Sets	Instruction Sets provide a way of organizing instructions and setting permissions on those instructions. They can be created, modified and deleted from the Tachyon Administration console.
Instrumentation data	Each of the Tachyon components creates instrumentation data that can be used to display how the Tachyon system is performing.
JSON Provider	This is an internal provider within the Tachyon agent library, used to deserialize and return a JSON string as a data table. Analogous to the Windows specific PowerShell Provider.
Legacy OS	In this documentation, Windows XP, Vista and Windows Server 2003 are referred to as legacy OS. Microsoft has withdrawn support for Windows XP and Windows Server 2003, but 1E includes Vista in this list because it is not significantly used by business organizations.

Term	Definition
	For details of limitations and additional considerations for these OS, please see Supported Platforms.
License file	1E will provide you with a **Tachyon.lic** license file that defines the applications, tools, and features your Tachyon System is able to use, for how long, and how many devices it supports, this may be an evaluation or subscription license. The license must be activated. Once activated, it may be used only by the Tachyon System that activated it. Licenses can be renewed or updated, but if allowed to expire, then the affected products or features will not be usable. For a new installation, the Tachyon Setup program will let you select the license file from any folder on disk. For an existing installation, the license file is copied into the folder: %PROGRAMDATA%\1E\Licensing on your Tachyon Server. Ensure the following URL is whitelisted: https://license-v1.1e.com This URL must be accessible from the Tachyon Server during setup and running of Tachyon. The Tachyon license must be validated on a regular basis via internet contact with the 1E license service. The regular validation period is set when the license is requested. For whitelisting purposes, the Tachyon Server (specifically the Coordinator Workflow module in the Master Stack) requires an Internet connection to the 1E license service, as defined in the license file itself. If activation fails, then the system will install but not be usable until activation is completed. **Upgrading** When upgrading, you are recommended to get a new license file and update your whitelist with the new URL. The old URL (https://license.1e.com) is suitable only for 8.0 and earlier. However, if you are upgrading and your license file has the old URL then you should also whitelist the old URL.

Term	Definition
License Service	The License Service is hosted in the cloud by 1E, and accessible via an internet connection.
Method	Methods are documented in the SDK.
Normalization	Normalization is a Platform function that refers to the process of finding (or not finding) a match rule in 1E Catalog, then deduplicating and rationalizing the information using Platform logic, and publishing the information on the 1E Catalog UI. Partial Matching for example does not have a match rule in 1E Catalog but it's still normalized and published on the UI using Platform logic.
Patch Success application	Patch Success application is used to report on and ensure successful patching of your enterprise. **Note** Patch Success can be reached directly using the following URL: `https://<tachyon DNS Name FQDN>/Tachyon/App/#/patchsuccess/` where <tachyon DNS Name FQDN> is the one set up during the preparation phase, as described under the heading DNS Names
Permissions	How the Role-Based Access Control feature assigns Users to Roles, providing access to Instruction Sets and Administration pages.
Persistent Storage	The client stores information in Persistent Storage which it needs each time it starts. For example the last processed instruction. A hash value of each item of information is stored in the registry, which the client uses to ensure it trusts each item. Persistent storage includes a local database that is compressed and encrypted in a way that ensures a very low impact on device performance and security. This database is used to store data for the Tachyon Activity Record feature.
PowerShell Provider	This is a Windows specific internal provider within the Tachyon agent library. It provides functionality to execute powershell.exe from a fixed location (System32\WindowsPowerShell\v1.0) on a PowerShell (.sp1) script and return the result.

Term	Definition
	Some earlier versions of Windows (such as Windows XP) do not support PowerShell.
Product Pack	Product Packs contain instructions or other things which extend the capabilities of Tachyon. Product Packs which are required to support Tachyon features out-of-the-box are provided in the Tachyon Platform zip downloaded from the 1E Support Portal. Other Product Packs are available for download from the 1E Exchange. There are two types of Product Packs described in the following table. **Classic Product Packs**: Classic Product Packs contain instructions (actually Instruction Definition files) for use in Explorer and other Tachyon applications. Classic Product Packs can be uploaded into Tachyon using either of the following methods: Tachyon Product Pack Deployment Tool - which will upload the instructions in the pack and create an Instruction Set for them based on the name of the zip (with hyphens converted into spaces) the Tachyon Portal Settings app→ Instructions → Instruction Sets, described in Instructions Menu. This method requires instructions to be organized into Instruction Sets by an Instruction Set Administrator. Settings can also be used to export instructions. Either method requires an Instruction Set Administrator to configure permissions for accessing the instructions. **Integrated Product Packs**: Integrated Product Packs contain policies, rules and fragments for use by

Term	Definition
	Guaranteed State, and may also include instructions. If the Integrated Product Pack contains instructions associated with the policies, the tool creates an Instruction Set using the name in its manifest file. Integrated Product Packs are uploaded using the PPDT.
Tachyon Product Pack Deployment Tool	A tool for uploading Classic and Integrated Product Packs. Please see Tachyon Product Pack Deployment Tool.
Providers	Providers can be used by applications to leverage external tools to perform specific operations. For example the reclaim provider enables software to be uninstalled, thereby extending the functionality of the platform to include uninstallation.
Question	In Tachyon a Question is a specific type of instruction that requests information from client devices. The information is returned to Tachyon as responses.
Report Refresh	You can refresh reports from individual AppClarity screens as well as using the Settings App. Where this is available you can do this by using the refresh icon next to the **Last Refreshed** box:
Response	The data resulting from a client executing an instruction.
Role-Based Access Control	Also known as RBAC. This is a general term for assigning users to roles which allow them access specific features of Tachyon. Roles can be assigned to AD users and groups added in the Administration Security page. A role can be either of the following: System role Custom role

Term	Definition
SCALE	The Agent Language.
SDK	The Tachyon SDK describes the following and is available here: /document/preview/736743#UUID-33c212b3-863e-21bc-bc5d-52e41a0492b3 Agent Language (SCALE) Agent modules and methods
Securable	Refers to an item that may be secured by Tachyon using RBAC.
Server installation account	This is the account used to run Tachyon Setup (and the MSI installer) when installing or upgrading a Tachyon Server. The account is automatically defined as a Tachyon admin user with limited rights which cannot be edited (called a system principal). The installation account only has sufficient rights to add other users, assign them to roles, and install Tachyon applications. The users and roles created by the installation account are then used for ongoing use and management of Tachyon. If you need the installation account to have additional roles or be a Full Administrator, then the recommended approach is: First create a role-based AD Security group, and add the installation and other accounts to this group Then, the installation account: Logs into Tachyon and navigates to Settings → Permissions → Users and Groups Creates a new user for the role-based AD Security Group Assigns the relevant system role(s) to the new user - this can be Full Administrator. When installing a Tachyon Server, the account must be an Active Directory domain account with various rights on the Tachyon Server and the SQL Server instance. For more detail see Tachyon Server Installation Account. For a new installation, only the Server installation account is able to use the Explorer and assign user rights to other users and groups. Once these other users or groups have been assigned, then the Server

Term	Definition
	installation account can be optionally disabled in AD pending future updates and upgrades. The Server installation account is a system principal and cannot be deleted or granted additional rights; it is able to manage additional users and groups, create and edit custom roles, which are then used for ongoing use and management of the system. However, the account may be included in any AD security group assigned to a Tachyon system or custom role.
Server instructions	A special type of instruction, which cannot be run in Explorer. They are for internal use only, run on the server, and used to carry out on-demand or scheduled processing of data across various datasources, such as SQL databases. For example, the Dashboards app uses them to populate tiles and charts with data from the TachyonMaster and Experience databases. They are also called server-side instructions, to differentiate them from client-side instructions which run on client devices.
Settings application	Settings application is used to configure Tachyon system and application settings. It is an example of a Tachyon Consumer application. **Note** Settings can be reached directly using the following URL: `https://<tachyon DNS Name FQDN>/Tachyon/App/#/platform/` where <tachyon DNS Name FQDN> is the one set up during the preparation phase, as described under the heading DNS Names.
Single-Switch installation	A **single-Switch installation** is a type of single-server installation which has only one Switch. This is the simplest Tachyon Server configuration.
Single-server installation	A **single-server installation** is where all Tachyon Server components are installed on the same Web Server, with one to five Switches, and SQL Server either local or remote. A single-Switch installation is the simplest configuration. More than one Switch requires additional hardware resources.

Term	Definition
	If SQL Server is remote then it is also referred to as a **split-server configuration**. Best performance is achieved using a local SQL Server installation. See Tachyon Architecture and Communication Ports.
SMTP gateway	Systems such as the Tachyon Server connect to the gateway in order to send emails. Also known as SMTP relay.
Switch	The Switch component on the Tachyon Server provides the following: Sends instructions to and retrieves responses from the clients Forwards responses to the Core component Receives workflow commands from the Core component Retrieves instruction definitions from the Core component Sends instrumentation data to the Instrumentation component On the Tachyon Server, the Switch Host service is responsible for managing all the local Switches The Switch configuration is stored in the SwitchConfiguration table of the TachyonMaster database. This includes the number of slots and workers used by the Switch which controls the maximum number of devices that can be managed by each Switch. A Switch restart will fail if the Switch failed to de-register itself, therefore the registration entry in the TachyonMaster database will need to be manually removed after troubleshooting. See Tachyon Architecture and Communication Ports.
Switch Host	The Switch Host service is a Windows service that manages local Switches automatically starts each Switch and if a Switch stops, the Switch Host analyses the reason and attempt to restart it has a configuration file contains entries for one or more Switches has its own log file See Tachyon Architecture and Communication Ports.

Term	Definition
System Principal	A system principal is a Tachyon user which cannot be modified in the Administration pages, and is assigned to a system role. The Server installation account is a system principal which is assigned to the Consumer Administrator, Security Administrator and Instruction Set Administrator system roles.
System Role	Tachyon roles which cannot be modified in the Administration pages. Tachyon users can be assigned to these roles. For more information about System and Custom roles, please refer to Roles and Securables. The following are built-in system roles. All Instructions Actioner All Instructions Approver All Instructions Questioner All Instructions Viewer Full Administrator Group Administrator Guaranteed State Administrator Guaranteed State Policy Assigner Guaranteed State User Installer Inventory Administrator Inventory User Tachyon System
Tachyon Activity Record	This is a client feature, also known as inventory, previously known as Historic Data Capture. This feature captures data from a number of sources on the client device, encrypts and stores in compressed form on the client device. Raw and summarized (aggregated) data is stored and can be queried using instructions.

Term	Definition
	See Tachyon client settings.
Tachyon client	Client features are provided by the 1E Client. The 1E Client includes client features and modules for other 1E products including Tachyon. Tachyon enables rapid response to instructions using the client, which supports the retrieval of information, running actions and device tagging. The client can also be extended to support additional features. The client connects to the Switch and the Background Channel. See Tachyon Architecture and Communication Ports.
Tachyon content	Tachyon content is: files (such as scripts) associated with a particular instruction via their which the client will download when it performs that instruction. extensibles (normally in the form of DLLs on Windows), which the client will download when it self-updates. This allows additional client functionality to be deployed. Tachyon content is downloaded on demand via the Background Channel.
1E Exchange	The 1E Exchange is a community platform and library of automation modules (Product Packs) for systems management created by 1E. Our goal for this community is to democratize the development and optimization of automation processes to simplify work. Leveraging SCALE, Tachyon's native language, and the Tachyon Platform we wish to grow into a community that builds powerful modules to serve each other's needs. https://tachyonexchange.1e.com/ You can browse the 1E Exchange but you will need a 1E Support login to download.
Tachyon Instruction Management Studio (TIMS)	This feature is included in the Tachyon Toolkit. TIMS provides a user interface for developing and testing instructions using SCALE. It includes an isolated copy of the 1E Client so that you can develop instructions for that client version, independent of the 1E Client version that may be installed on your computer.

Term	Definition
	By default TIMS and its Tachyon client run under the security context of the user that started it. To use the context of **Local System**, as used by a normal Tachyon client, you can start TIMS using PSexec. More information about TIMS is available in the Tachyon Community on the 1E Support Portal. TIMS should be used to edit and save Instruction Definition files.
Tachyon Instruction Runner	This feature is the graphical user interface part of the Configuration Manager Extensions which is included in the Tachyon Toolkit. It is a mini UI version of Explorer. It is an example of a Tachyon Consumer. It should not to be confused with the Tachyon Run Instruction utility available in the Tachyon Toolkit.
TachyonMaster database	The SQL Server database which contains: Configuration details of the Tachyon System instruction definitions and Instruction Sets Users (Principals) Permissions Roles Devices Audit log The configuration files for the following components contain SQL Connection strings for the TachyonMaster database. Core Coordinator Workflow module Consumer API
Tachyon Master Stack	A Tachyon Master Stack is part of a Tachyon System. There is one Tachyon Master Stack that all the Tachyon Response Stacks

Term	Definition
	communicate with. A Tachyon Master Stack contains the following components: SQL Server instance with TachyonMaster Database (local or remote/split) Consumer API Coordinator Explorer Authentication Registration
Tachyon Portal	The Tachyon Portal is the home page for Tachyon applications, which can be reached using the following URL: `https://<tachyon DNS Name FQDN>/Tachyon` where <tachyon DNS Name FQDN> is the one set up during the preparation phase, as described under the heading DNS Names. The following buttons appear on all application pages of the Tachyon Portal. The refresh button is used to refresh the contents of the page. The expand button toggles the size of the page inside the browser by hiding or showing the menu and main title bar.
TachyonResponses database	The SQL Server database which contains: Responses

Term	Definition
Tachyon Response Stacks	A Response Stack is part of a Tachyon System. This is where one or more Response Stacks talk back to a single Tachyon Master Stack. Multiple Response Stacks are necessary when additional Switches are required for scale, security or for geographic or other network reasons. Each Switch can handle 50000 devices, so each Response Stack can handle a maximum of 250000 devices. Each Response Stack has the following components: Switch Host Switches (up to 5, local or remote/split) Core SQL Server instance with Tachyon Responses database (local or remote/split) Background Channel A Response Stack will typically host Switches and Background Channel using the same DNS Alias.
Tachyon Role	Tachyon roles are used to implement Role-base access control (RBAC) and assign permissions to users and restrict access to areas of Explorer and ability to use instructions in Instruction Sets .The roles may be system roles or custom roles related to specific Instruction Sets .
Tachyon Run Instruction utility	This command-line utility is included in the Tachyon Toolkit and is targeted at 3rd party integration, and can be used by scripts. It is an example of a Tachyon Consumer. It is used by the Configuration Manager Extensions which is also available in the Tachyon Toolkit. More information about the Tachyon Run Instruction utility is available in the Tachyon Community on the 1E Support Portal.
Tachyon Server	A Tachyon Server is any server on which a Tachyon Server component is installed. The following are Tachyon Server components. Coordinator service (Instrumentation and Workflow modules) Switch Host

Term	Definition
	Switches Website (including Explorer and Core) A Tachyon Server can have one or more Switches. See also single-server installation and single-Switch installation. See Tachyon Architecture and Communication Ports.
Tachyon Stack	There are two types of Stack: Master Stack and Response Stack. Every Tachyon system has a single **Master Stack**, which provides web services for Tachyon applications. Master Stack components are typically all installed on a single **Master Server**. Tachyon real-time features require **Response Stacks**, which are made up of one or more **Response Servers**. A **DMZ Server** is an example of a Response Server. Each Response Stack has at least one **Background Channel** for sharing resources, and a single **Core** component that supports an associated set of up to five **Switches**. Switches are the primary mechanism for rapidly requesting and retrieving responses from the **clients**. As each Switch can handle up to 50,000 devices there is a limit of 250,000 devices per Response Stack. Higher numbers can be achieved if you contact 1E for guidance. Switches may be local or remote to the other components in the Response Stack. **Databases** for Tachyon, Catalog, Content Distribution, Experience, SLA and BI, are installed on SQL Server database instance(s) that may also be local or remote to their respective Master and Response servers. It is also possible for multiple Response Stacks to share the same Responses database. The **Cube** used by Patch Success (SLA-BI) is installed on a local or remote SQL Server Analysis Services (SSAS) instance. For more details about architecture and components, please see Tachyon Architecture. Also see Architectural requirements.
Tachyon System	At the top-most level, a Tachyon System consists of Tachyon Server components, grouped into Tachyon Stacks, and a set of clients that are deployed onto the devices that you want to manage. In addition, a system can have one or more Consumers (the built-in Consumer is Explorer). See Tachyon Architecture and Communication Ports.

Term	Definition
	Tachyon System is also a system role, used by Tachyon for service an equivalent account to perform Tachyon system operations.
Tachyon Toolkit	The Tachyon Toolkit is a collection of the following tools, which can be installed on a Windows computer for use by a User who has appropriate permissions. Configuration Manager Extensions - this can be installed only on a computer that has already installed a Supported Platforms Tachyon Instruction Management Studio. .Tachyon Run Instruction utility The toolkit is available for download from the Tachyon Community in the 1E Support Portal. Documentation for installing and using the Toolkit will be available soon.
Tachyon User	A domain account that is authorized to access Explorer portal and/or the Tachyon Administration pages. Authorization is achieved by adding the AD account or group and assigning it to a role.
Tags	There are two types of tag: coverage tags and freeform tags. In Tachyon log files, these tags are also known a scopable and non-scopable tags.
Two-factor authentication	Also known as 2FA. See Two-factor authentication.
Website	The Tachyon Website hosts the following web applications: Master: Admin Consumer - Consumer API CoreExternal Platform

Term	Definition
	Tachyon Response and DMZ: Background - Background Channel Core Optional applications on Master: ContentDistrbution Experience The Website has an HTTP binding and HTTPS binding. The HTTP binding uses the server's hostname FQDN as a host header, and is used only by SLA components - please refer to Removing the HTTP binding from the Tachyon website One or more HTTPS bindings - these use the Tachyon Web Server certificate, the server's DNS Alias as the host name, and has SNI enabled. See Tachyon Architecture and Communication Ports.
Workflow commands	Workflow commands determine how the Coordinator Workflow module processes an instruction, particularly in terms of the permissions required to run the instruction.

9.6.16 Nomad Product Packs reference

Reference information for **Nomad** feature-related Product Packs that are included in the **Tachyon Platform** zip. These Product Packs are required to support various features of **Nomad.**

The **Tachyon Platform** zip is downloaded from the 1E Support Portal (1eportal.force.com/s/tachyontopicdetail). Additional Product Packs are available from Tachyon Exchange (tachyonexchange.1e.com) that are not documented here.

Classic Product Packs contain instructions, for use in Explorer and other Tachyon applications.

Integrated Product Packs contain policies, rules and fragments for use by Guaranteed State, and may also include instructions.

9.6.16.1 1E Nomad product pack

Classic product pack used to create the **1E Nomad** instruction set in Tachyon, required by the following Nomad features:

Downloads tab on Device views - instructions used to populate details about Content download and other Nomad features

Nomad Download Pause - instructions used by the CM Admin Console extensions

Instructions to help with the following Nomad features: Nomad cache, CacheCleaner, Single Site Download, Nomad jobs, NomadBranch service.

Nomad feature	Instruction text (ReadablePayload)	Type	Description	FileName	Version
Nomad cache Nomad jobs	**Get the percentage of content %ContentId% in the local Nomad cache**	Question	Get the percentage of the specified content in the local Nomad cache.	**1E-Nomad-CachedPkgStatus**	8
Nomad cache CacheCleaner Nomad jobs	**Clean the SCCM and Nomad cache for an application %packageId%**	Action	Cleans the SCCM and Nomad cache for an application with the specified package ID. This package ID is the Content ID of the deployment type of the application.	**1E-Nomad-CleanNomadCacheForApplication**	16

Nomad feature	Instruction text (ReadablePayload)	Type	Description	FileName	Version
Nomad cache CacheCleaner Nomad jobs	**Clean the SCCM and Nomad cache for a package %packageId% and %packageVersion%**	Action	Cleans the SCCM and Nomad cache for the package with the specified ID and version.	**1E-Nomad-CleanNomadCacheForPackage**	16
Nomad cache Nomad jobs	**Find the Nomad host that has the greatest percentage of content %ContentId%**	Question	Find the Nomad host that has the greatest percentage of the specified content.	**1E-Nomad-FindBestPkgCache**	8
Nomad jobs	**Find the ConfigMgr locations (i.e. on DPs) that have content %ContentId% at version %Version%**	Question	Find the ConfigMgr locations (i.e. on DPs) that have the specified content.	**1E-Nomad-GetCmContentLocations**	8
Nomad jobs	**Get the status of Nomad jobs**	Question	Get the status of Nomad jobs.	**1E-Nomad-NomadJobsStatus**	11

Nomad feature	Instruction text (ReadablePayload)	Type	Description	FileName	Version
Nomad jobs	**Get the status of Nomad**	Question	Get the status of Nomad.	**1E-Nomad-NomadStatus**	11
Nomad jobs	**Pause any current Nomad job**	Action	Pause any current Nomad job.	**1E-Nomad-PauseCurrentNomadJob**	12
Nomad Download Pause Nomad jobs	**Pause the Nomad job queue for %PauseDurationMinutes% minutes**	Action	Pause Nomad job queue.	**1E-Nomad-PauseNomadJobQueue**	14
Nomad Download Pause Nomad jobs	**Resume the paused Nomad job queue**	Action	Resume paused Nomad job queue.	**1E-Nomad-ResumeNomadJobQueue**	11
Nomad jobs	**Resume any paused Nomad job**	Action	Resume any paused Nomad job.	**1E-Nomad-ResumePausedNomadJob**	12
Single Site Download	**Ask SSD site master with %deviceIdType% '%deviceId%' whether any device has more than %percent%% of content %contentId% v%version% with format %format%**	Question	Ask SSD site master whether any device has more than the specified percentage of the	**1E-Nomad-RunPkgStatusRequest**	9

Nomad feature	Instruction text (ReadablePayload)	Type	Description	FileName	Version
			specified content.		
Single Site Download	**Use SSD to find where at least %percent% percent of content %contentId% v%version% with format %format% is cached with extent %extent% and AllSubnets %allSubnets %, returning up to %maxDevices% devices**	Question	Use Nomad's Single Site Download feature to find where the specified content is cached.	**1E-Nomad-RunSsdQuery**	8
NomadBranch service	**Start the Nomad service**	Action	Start the Nomad service.	**1E-Nomad-StartNomadService**	12
Nomad jobs	**Stop any current Nomad job**	Action	Stop any current Nomad job.	**1E-Nomad-StopCurrentNomadJob**	12
NomadBranch service	**Stop the Nomad service**	Action	Stop the Nomad service.	**1E-Nomad-StopNomadService**	12

9.6.16.2 Nomad Client Health integrated product pack

Integrated Product Pack used to create the **Nomad Client Health** instruction set and **Nomad Client Health** policy.

For more information please refer to Nomad Client Health Policy.

Nomad is included as part of the 1E Client, and as part of that integration, we offer a Nomad client health compliance policy in Guaranteed State. This verifies common Nomad requirements such as ACP registration, disk availability, firewall exceptions, crash notifications and cache monitoring.

The Nomad client health policy replaces the client health tile in the Nomad dashboard plus additional remediation steps:

Keeps content distribution services up and running on Nomad clients, so that users are secure and productive

Ensures Alternative Content Provider (ACP) registration configuration is set

Maintains optimal disk availability and monitors cache size for storage capacity planning

Enforces Firewall exceptions.

Note

This policy is intended for deployment to Windows devices only.

9.6.16.2.1 Instructions

The following table shows the instructions included in the Integrated Product Pack. Unless already uploaded, the following instructions are added to an Instruction set named: **Nomad Client Health**.

Readable Payload	Type	Description	Name	Version
P2P election weight vs criticality	Question	Returns the Nomad peer-to-peer election weight and the criticality of the device. This instruction is useful if you use - and want to correlate - the Nomad feature Sensitive server weighting and Device Criticality. The P2PElectionWeight registry entry does not exist unless it is explicitly set - for example by a Configuration Manager baseline or Tachyon instruction. If the registry entry does not exist, the response will be **Not set**. Similarly, the default criticality value assigned to a device is **Undefined**. The following is an extract from Download once to branch: Election weighting: Click here to expand... Nomad performs automatic weighting depending on its situation, according to the criteria listed below, and stores the value in memory (not registry). The higher the value, the greater the probability of winning the election.	**1E-Explorer-NomadClientHealth-ElectionWeightVsCriticality**	3

Readable Payload	Type	Description	Name	Version
		61 – the agent is running on a server OS and it is not a domain controller (DC) 40 – the agent is running on a laptop 30 – the agent is running on a wireless network 10 – the agent is running on WinPE 50 – default If necessary, you can use the P2PElectionWeight registry setting to increase or decrease a Nomad client's probability of being elected a master. The range for this registry value must be between 0 and 99 inclusive. If not set, Nomad uses the values listed above. The registry key is located at: *HKLM\software\1e\NomadBranch\P2PElectionWeight* To take effect after setting the registry value, the client sevice must be restarted. This method is not recommended because Nomad is already quite efficient in the way it elects a master and needs very little intervention in this process. However, you may want to reduce the chance of computers with low processing power, or prevent critical servers, becoming a master. You should also consider the following points before you influence the weighting: Use this technique in exceptional circumstances and only after testing has shown that you need to make a particular		

Readable Payload	Type	Description	Name	Version
		computer more or less likely to be elected as a master for specific operational reasons. Choose the simplest weighting strategy possible - for example, set servers at 90, laptops at 10 and workstations at 50. The weighting does not guarantee that the more heavily weighted computers will win the election – they may be turned off or another local peer may have already cached more of the requested content. The final weighting value used by the computer during an election may differ from the registry value as Nomad will automatically adjust it depending on the chassis and the network connection used. In the event you no longer need the values to be set, you should remove it and restart the service to resume dynamic election weighting. Setting to 0 is a special case called Sensitive server weighting designed for use on critical servers. The 0 value prevents Nomad from acting as master, and devices with this value will not respond to election requests.		

9.6.16.2.2 Policies

The following table shows the policies included in the Nomad Client Health Integrated Product Pack:

Name	Description
Nomad Client Health	The Nomad Client Health policy ensures that the health of the Nomad client is compliant with a reference baseline.

9.6.16.2.3 Rules

The following table shows the rules included in the Nomad Client Health Integrated Product Pack:

> **Note**
>
> Any parameter values shown in the table below are specifically set in the rules when the pack is uploaded. These may be different to the default values shown in the Fragments and Trigger templates tables. You can modify these if required.

Name	Type	Description	Check and Fix fragments	Triggers	Precondition fragment
Check Nomad ActiveEfficiency connectivity status	Check	Checks the Nomad agent connectivity to ActiveEfficiency.	1E-GuaranteedState-Nomad-Check-AEConnectivity No parameters	TriggerTemplate-WindowsRegistryChange Hive=*HKLM* *Subkey=Software\1E\NomadBranch\ActiveEfficiency* Include Sub keys=0 TriggerTemplate-IntervalHours intervalHours=1	1E-GuaranteedState-Nomad-PreCondition-MultiTests hasCmClient=0 sccmDp=0 smbEnabled=0
Check Nomad can communicate through the Windows Firewall	Check	Check that there are Windows Firewall program exceptions for Nomad and its related executables.	1E-GuaranteedState-Nomad-Check-FirewallExceptions No parameters	TriggerTemplate-WindowsRegistryChange Hive=*HKLM* *Subkey=Software\1E\NomadBranch\NomadBranch* Include Sub keys=1 TriggerTemplate-IntervalHours intervalHours=1	1E-GuaranteedState-Nomad-PreCondition-MultiTests hasCmClient=0 sccmDp=0 smbEnabled=0

Name	Type	Description	Check and Fix fragments	Triggers	Precondition fragment
Ensure Nomad can communicate through the Windows Firewall	Fix	Ensures there are Windows Firewall program exceptions for Nomad and its related executables.	1E-GuaranteedState-Nomad-Check-FirewallExceptions No parameters 1E-GuaranteedState-Nomad-Fix-FirewallExceptions No parameters	TriggerTemplate-IntervalHours intervalHours=1	1E-GuaranteedState-Nomad-PreCondition-MultiTests hasCmClient=0 sccmDp=0 smbEnabled=0
Check Nomad can generate LSZ files on ConfigMgr distribution points	Check	Check that LSZ generation is enabled on ConfigMgr distribution points.	1E-GuaranteedState-Nomad-Check-DpLszEnabled No parameters	TriggerTemplate-WindowsRegistryChange Hive=*HKLM* *Subkey=Software\1E\NomadBranch\NomadBranch* Include Sub keys=1 TriggerTemplate-IntervalHours intervalHours=1	1E-GuaranteedState-Nomad-PreCondition-MultiTests hasCmClient=0 **sccmDp=1** smbEnabled=0
Check Nomad can hash content	Check	Checks Nomad content hashing is enabled.	1E-GuaranteedState-Nomad-Check-HashingEnabled No parameters	TriggerTemplate-WindowsRegistryChange Hive=*HKLM* *Subkey=Software\1E\NomadBranch\NomadBranch* Include Sub keys=1	1E-GuaranteedState-Nomad-PreCondition-MultiTests

Name	Type	Description	Check and Fix fragments	Triggers	Precondition fragment
				TriggerTemplate-IntervalHours intervalHours=1	hasCmClient=0 sccmDp=0 smbEnabled=0
Check Nomad crash dumps status	Check	Checks whether Nomad has generated any crash dump in the last seven days.	1E-GuaranteedState-Nomad-Check-CrashDumps No parameters	TriggerTemplate-WindowsRegistryChange Hive=*HKLM* *Subkey=Software\1E\NomadBranch\NomadBranch* Include Sub keys=1 TriggerTemplate-IntervalHours intervalHours=1	1E-GuaranteedState-Nomad-PreCondition-MultiTests hasCmClient=0 sccmDp=0 smbEnabled=0
Check Nomad does not have its content indexed by ConfigMgr software inventory checks	Check	Checks whether skpswi.dat exists in the Nomad cache directory.	1E-GuaranteedState-Nomad-Check-SkpSwiDat No parameters	TriggerTemplate-FileChange File Name=C:\ProgramData\1E\NomadBranch\skpswi.dat TriggerTemplate-IntervalHours intervalHours=1 **Warning** Do NOT use this Check if you have changed your cache location.	1E-GuaranteedState-Nomad-PreCondition-MultiTests hasCmClient=0 sccmDp=0 smbEnabled=0

Name	Type	Description	Check and Fix fragments	Triggers	Precondition fragment
Ensure Nomad does not have its content indexed by ConfigMgr software inventory checks	Fix	Ensures that skpswi.dat exists in the Nomad cache directory.	1E-GuaranteedState-Nomad-Check-SkpSwiDat No parameters 1E-GuaranteedState-Nomad-Fix-SkpSwiDat No parameters	TriggerTemplate-FileChange File Name=C:\ProgramData\1E\NomadBranch\skpswi.dat TriggerTemplate-IntervalHours intervalHours=1 **Warning** Do NOT use this Fix if you have changed your cache location.	1E-GuaranteedState-Nomad-PreCondition-MultiTests hasCmClient=0 sccmDp=0 smbEnabled=0
Check Nomad has a virtual directory on ConfigMgr distribution points to perform LSZ generation	Check	Check that an LSZFILES virtual directory has been created on a ConfigMgr distribution point.	1E-GuaranteedState-Nomad-Check-DpLszVirtualDirectory No parameters	TriggerTemplate-WindowsRegistryChange Hive=*HKLM* *Subkey=Software\1E\NomadBranch\NomadBranch* Include Sub keys=1 TriggerTemplate-IntervalHours intervalHours=1	1E-GuaranteedState-Nomad-PreCondition-MultiTests hasCmClient=0 **sccmDp=1** smbEnabled=0
Ensure Nomad has a virtual directory on ConfigMgr	Fix	Ensure that an LSZFILES virtual directory has been created on a	1E-GuaranteedState-Nomad-Check-DpLszVirtualDirectory No parameters	TriggerTemplate-IntervalHours intervalHours=1	1E-GuaranteedState-Nomad-PreCondition-MultiTests

Name	Type	Description	Check and Fix fragments	Triggers	Precondition fragment
distribution points to perform LSZ generation		ConfigMgr distribution point.	1E-GuaranteedState-Nomad-Fix-DpLszVirtualDirectory No parameters		hasCmClient=0 **sccmDp=1** smbEnabled=0
Check Nomad has sufficient disk space to download content	Check	Check the drive that Nomad is using for content download has sufficient disk space.	1E-GuaranteedState-Nomad-Check-DiskAvailablility No parameters	TriggerTemplate-WindowsRegistryChange Hive=*HKLM* *Subkey=Software\1E\NomadBranch\NomadBranch* Include Sub keys=1 TriggerTemplate-IntervalHours intervalHours=1	1E-GuaranteedState-Nomad-PreCondition-MultiTests hasCmClient=0 sccmDp=0 smbEnabled=0
Check Nomad is not using the Windows temp directory for caching	Check	Checks that Nomad is not configured to use the Windows temporary directory for caching.	1E-GuaranteedState-Nomad-Check-CacheInTemp No parameters	TriggerTemplate-WindowsRegistryChange Hive=*HKLM* *Subkey=Software\1E\NomadBranch\NomadBranch* Include Sub keys=1 TriggerTemplate-IntervalHours intervalHours=1	1E-GuaranteedState-Nomad-PreCondition-MultiTests hasCmClient=0 sccmDp=0 smbEnabled=0

Name	Type	Description	Check and Fix fragments	Triggers	Precondition fragment
Check Nomad is registered as an Alternate Content Provider with ConfigMgr	Check	Check that Nomad is correctly registered as an Alternate Content Provider with ConfigMgr.	1E-GuaranteedState-Nomad-Check-AlternateContentProvider No parameters	TriggerTemplate-IntervalHours intervalHours=1	1E-GuaranteedState-Nomad-PreCondition-MultiTests **hasCmClient=1** sccmDp=0 smbEnabled=0
Ensure Nomad is registered as an Alternate Content Provider with ConfigMgr	Fix	Ensure Nomad is registered as an Alternate Content Provider with ConfigMgr, registering it if necessary.	1E-GuaranteedState-Nomad-Check-AlternateContentProvider No parameters 1E-GuaranteedState-Nomad-Fix-AlternateContentProvider No parameters	TriggerTemplate-IntervalHours intervalHours=1	1E-GuaranteedState-Nomad-PreCondition-MultiTests **hasCmClient=1** sccmDp=0 smbEnabled=0
Check Nomad run status	Check	Checks that the Nomad service is running.	1E-GuaranteedState-Nomad-Check-StartService No parameters	TriggerTemplate-IntervalHours intervalHours=1 TriggerTemplate-ServiceStatusChange ServiceName=*NomadBranch*	1E-GuaranteedState-Nomad-PreCondition-MultiTests

Name	Type	Description	Check and Fix fragments	Triggers	Precondition fragment
					hasCmClient=0 sccmDp=0 smbEnabled=0
Ensure Nomad is running	Fix	Ensure the Nomad service is running, starting the service if required.	1E-GuaranteedState-Nomad-Check-StartService No parameters 1E-GuaranteedState-Nomad-Fix-StartService No parameters	TriggerTemplate-IntervalHours intervalHours=1 TriggerTemplate-ServiceStatusChange ServiceName=*NomadBranch*	1E-GuaranteedState-Nomad-PreCondition-MultiTests hasCmClient=0 sccmDp=0 smbEnabled=0
Check Nomad variant status	Check	Checks whether the running Nomad service was one supplied with the 1E Client.	1E-GuaranteedState-Nomad-Check-Variant No parameters	TriggerTemplate-IntervalHours intervalHours=1 TriggerTemplate-ServiceStatusChange ServiceName=*NomadBranch*	1E-GuaranteedState-Nomad-PreCondition-MultiTests hasCmClient=0 sccmDp=0 smbEnabled=0

Name	Type	Description	Check and Fix fragments	Triggers	Precondition fragment
Check Nomad's share directory is accessible	Check	Check whether Nomad needs a share, and if it does that it would be accessible to other devices.	1E-GuaranteedState-Nomad-Check-Share No parameters	TriggerTemplate-WindowsRegistryChange Hive=*HKLM* *Subkey=Software\1E\NomadBranch\NomadBranch* Include Sub keys=1 TriggerTemplate-IntervalHours intervalHours=1	1E-GuaranteedState-Nomad-PreCondition-MultiTests hasCmClient=0 sccmDp=0 **smbEnabled=1**
Ensure Nomad's share directory is accessible	Fix	Ensures that Nomad's share is accessible if it is configured to require a share.	1E-GuaranteedState-Nomad-Check-Share No parameters 1E-GuaranteedState-Nomad-Fix-Share No parameters	TriggerTemplate-IntervalHours intervalHours=1	1E-GuaranteedState-Nomad-PreCondition-MultiTests hasCmClient=0 sccmDp=0 **smbEnabled=1**
Check Nomad's share is accessible by specific accounts	Check	Checks that the correct accounts are able to access Nomad's share.	1E-GuaranteedState-Nomad-Check-ShareAccount No parameters	TriggerTemplate-WindowsRegistryChange Hive=*HKLM* *Subkey=Software\1E\NomadBranch\NomadBranch* Include Sub keys=1	1E-GuaranteedState-Nomad-PreCondition-MultiTests hasCmClient=0

Name	Type	Description	Check and Fix fragments	Triggers	Precondition fragment
				TriggerTemplate-IntervalHours intervalHours=1	sccmDp=0 **smbEnabled=1**
Ensure Nomad's share is accessible by specific accounts	Fix	Ensures that the correct accounts are able to access Nomad's share.	1E-GuaranteedState-Nomad-Check-ShareAccount No parameters 1E-GuaranteedState-Nomad-Fix-ShareAccount No parameters	TriggerTemplate-IntervalHours intervalHours=1	1E-GuaranteedState-Nomad-PreCondition-MultiTests hasCmClient=0 sccmDp=0 **smbEnabled=1**

9.6.16.2.4 Fragments

The following table shows the fragments included in the Nomad Client Health Integrated Product Pack:

> **Note**
>
> The **Parameters** column in the following table shows the ranges and default values for the parameters. The default values are used when you create custom rules using these fragments, unless you select alternative values.

Name	Type	Readable Payload and summary	Parameters
1E-GuaranteedState-Nomad-PreCondition-	Precondition	**Check if standard conditions apply for Nomad plus optionally: is a ConfigMgr DP (<sccmDp>); has a ConfigMgr client (<hasCmClient>); SMB sharing is enabled (<smbEnabled>)** The precondition passes for all of the following standard tests:	hasCmClient

Name	Type	Readable Payload and summary	Parameters
MultiTests		The device is running a version of Windows - Nomad is only supported on Windows operating systems The device is not running Windows XP - which is no longer supported by Nomad The *NomadBranch* service is installed, although not necessarily running. The precondition also tests for each of the following if it is enabled by changing its parameter from 0 to 1: **hasCmClient** : The ConfigMgr client is installed **sccmDp** : The device is a ConfigMgr Distribution Point (DP) **smbEnabled** : SMB sharing of Nomad's cache is enabled. If **smbEnabled** test is set in the rule precondition then an additonal test is made to see if the device is a Domain Controller (DC). When installed on a DC Nomad must use its computer account instead of SMSNomadP2P& in order to share its cache. This requires registry value *HKLM\SOFTWARE\1E\NomadBranch\SpecialNetShare* to have its 0x80 bit set. If not set then Nomad does not share its cache on a DC and does not respond to elections. For early adopters, the readable payload of this precondition was: Carries out the specified checks; if any fail (i.e. they are logically AND-ed) then the preconditions fails.	sccmDp smbEnabled Range 0 or 1, defaults=0
1E-GuaranteedState-Nomad-Check-AEConnectivity	Check	**Check whether there is a working connection to ActiveEfficiency** Tests whether the URL given by registry value *HKLM\SOFTWARE\1E\NomadBranch\ActiveEfficiency\PlatformUrl*, if it is not empty, is contactable and returns a 200 code.	None
1E-GuaranteedState-Nomad-	Check	**Check whether Nomad is correctly registered within Microsoft ConfigMgr** Check that the ConfigMgr client's list of ACPs includes an object for Nomad in WMI class	None

Name	Type	Readable Payload and summary	Parameters
Check-AlternateContentProvider		*ROOT\ccm\Policy\Machine\RequestedConfig\CCM_DownloadProvider*, with *CLSID* "*25A6160D-4543-495F-975E-32CFBD6F70E0*", *LogicalName* "*NomadBranch*", *V4CompatibleHash* is set, and just "*<Data></Data>*" in *GlobalSettings*.	
1E-GuaranteedState-Nomad-Fix-AlternateContentProvider	Fix	**Ensures Nomad is correctly registered within Microsoft ConfigMgr** If the same checks as 1E-GuaranteedState-Nomad-Check-AlternateContentProvider are not satisfied, restarts the *NomadBranch* service, waits 10 seconds for Nomad to establish itself as an ACP, then carries out the checks again.	None
1E-GuaranteedState-Nomad-Check-CacheInTemp	Check	**Check whether Nomad's cache is not in a temporary directory** The Nomad cache can sometimes be configured to be in the Windows *Temp* directory (usually *C:\Windows\Temp*) or one of its subdirectories. Since all the contents of the Windows *Temp* directory are considered to be transient and could be deleted at any time, this is not suitable for Nomad's cache which should be a permanent location. The check examines Nomad's *HKLM\SOFTWARE\1E\NomadBranch\LocalCachePath* registry value and verifies that the specified location actually exists. It then gets the *TEMP* environment variable, which, because both the *1E Client* and *NomadBranch* services run as *Local System*, is usually the WIndows *TEMP* directory. If the *LocalCachePath* value is the same as the *TEMP* environment variable, or *LocalCachePath* specifies a subdirectory within it, the check fails.	None
1E-GuaranteedState-Nomad-Check-CrashDumps	Check	**Check whether there have been any crashdump files created by Nomad in last 7 days** Nomad dump files are saved in the same directory as the log file, the parent directory of the *HKLM\SOFTWARE\1E\NomadBranch\LogFileName* registry value. The check looks in here for any files with a "*.dmp*" suffix (ignoring case), and if it finds any examines the modification time (not creation time!) of each, reporting as a failed	None

Name	Type	Readable Payload and summary	Parameters
		check any that were modified in the last 7 days. So the check passes if there are no "*.dmp*" files or they are all older than 7 days.	
1E-GuaranteedState-Nomad-Check-DiskAvailablility	Check	**Checks whether there is sufficient disk space for Nomad** This examines Nomad's *HKLM\SOFTWARE\1E\NomadBranch\ PercentAvailableDisk* registry value. (It ignores the older *MaxCacheSizeMB* value which has been superseded by *PercentAvailableDisk*.) If the value is greater than or equal to 80, the check fails because the setting is too high. It then compares the size of the contents of the folder given by *HKLM\SOFTWARE\1E\NomadBranch\ LocalCachePath* in the registry, i.e. Nomad's cache, with the free space of the drive on which the folder resides, as reported by WMI's *root\cimv\Win32_LogicalDisk*. The check fails if the percentage of free space on the drive is less than or equal too *PercentAvailableDisk*.	None
1E-GuaranteedState-Nomad-Check-DpLszEnabled	Check	**Check whether web LSZ generation is correctly configured on stand alone distribution points** Nomad automatically sets up LSZ file generation on DPs that are ConfigMgr site servers, but extra configuration is required for standalone DPs. The device is a standalone DP if, under registry key *HKLM\SOFTWARE\Microsoft\SMS\Operations Management\SMS Server Role*, the subkey *SMS Distribution Point* exists but *SMS Site Server* does not. If the device is a standalone DP, registry value *HKLM\SOFTWARE\1E\\NomadBranch\SpecialNetShare* should have its 16384/0x4000 bit set to turn on web LSZ generation for HTTP/HTTPS enabled clients; if not, the check fails.	None
1E-GuaranteedState-Nomad-Check-DpLszVirtualDirectory	Check	**Check whether the LSZ directory is correctly configured on distribution points** At time of writing there is a bug such that the overall check status is usually "Passed" even when individually reported checks fail. If the device is a standalone DP, the check first verifes that registry value *HKLM\SOFTWARE\1E\\NomadBranch\SpecialNetShare* has its 16384/0x4000 bit set. (This bit is not required for a DP on a site	None

Name	Type	Readable Payload and summary	Parameters
		server.) Then the *LSZFILES* web site is examined to verify that all these conditions are satisfied: Anonymous authentication is enabled Windows authentication is enabled No SSL Default document is enabled Directory browsing is enabled, with Date, Time, Size, Extension and LongDate all available Content indexing is disabled.	
1E-GuaranteedState-Nomad-Fix-DpLszVirtualDirectory	Fix	**Ensure that the LSZ directory is correctly configured on distribution points** At time of writing there is a bug such that the overall check status is usually "Passed" even when individually reported checks fail. If any of the conditions described above for the corresponding check fragment is not true, the LSZFILES website is reconfigured to set that condition.	None
1E-GuaranteedState-Nomad-Check-FirewallExceptions	Check	**Checks whether firewall exceptions exist for Nomad** First is a check that at least one Windows firewall profile is enabled and that the firewall itself is enabled with either *HKLM\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile\EnableFirewall* set to 1 or *HKLM\SOFTWARE\Policies\Microsoft\WindowsFirewall\StandardProfile\EnableFirewall* set to 1 in the registry. If no firewall and no firewall profile is enabled then no firewall exceptions are necessary and so there is nothing more to do. Otherwise,the Nomad-related firewall rules are examined. These are the rules named: *NomadBranch.exe* *NomadPackageLocatorTcp*	None

Name	Type	Readable Payload and summary	Parameters
		NomadPackageLocatorUdp *PackageStatusRequestTcp* *PackageStatusRequestUdp* *NomadBranchPeerHttp* *NomadBranchPeerHttps* Using the *NomadBranch* service's path of *NomadBranch.exe*, the paths of *NomadPackageLocator.exe* and *PackageStatusRequest.exe* are deduced. Using the *HKLM\SOFTWARE\1E\NomadBranch\P2PEnabled* , *P2P_Port* , *P2PHttpPort* , and *P2PHttpsPort* settings in the registry, the fragment works out which Nomad features are enabled and hence which firewall rules are required. The firewall rule checks involve: Whether the rule even exists That the rule is enabled and not blocked The local port (which may be a specific one or all) Which protocol (TCP or UDP) is involved The path to the associated executable. Rulesfor *NomadBranch.exe* , *NomadPackageLocatorTcp* , *NomadPackageLocatorUdp* , *PackageStatusRequestTcp* and *PackageStatusRequestUdp* must always be correctly defined. *NomadBranchPeerHttp* is only required if the 0x20 bit of *P2P_Enabled* is set, and likewise the 0x40 bit requires *NomadBranchPeerHttps* .	
1E-GuaranteedState-Nomad-Fix-FirewallExceptions	Fix	**Ensures the required firewall exceptions exist for Nomad** This carries out all the checks as described above for 1E-GuaranteedState-Nomad-Check-FirewallExceptions then, for each absent or incorrectly configured rule that is required to support the *P2PEnabled* registry setting,configures that rule.	None

Name	Type	Readable Payload and summary	Parameters
1E-GuaranteedState-Nomad-Check-HashingEnabled	Check	**Check whether hashing is enabled in Nomad** This examines the *HKLM\SOFTWARE\1E\NomadBranch\CompatibilityFlags* registry value. If the host is a ConfigMgr DP the 0x80000 bit should be set ("enable full hash generation for SIS content when an LsZ file is generated on a DP"), otherwise the 0x100000 bit ("abort download on the Nomad client if an LsZ hash mismatch is detected").	None
1E-GuaranteedState-Nomad-Check-Share	Check	**Checks whether the Nomad share is available** This first checks the firewall settings. If the firewall is enabled then "*File and Printer Sharing*" (i.e. SMB) cannot be disabled. Next the 0x10 bit of registry value *HKLM\SOFTWARE\1E\\NomadBranch\SpecialNetShare* is examined to see if the share name is the default "*NomadSHR*" or the hidden "*NomadSHR$*". The share's security descriptor is read and check made that the local "*SMSNomadP2P&*" account has read permission. The share's properties are then verified as follows: The shared directory is that named by registry value *HKLM\SOFTWARE\1E\NomadBranch\ LocalCachePath* The shared directory also matches the *Path* from WMI's *root\cimv2\Win32_Share* object for the share. The *Status* of the *root\cimv2\Win32_Share* object is "*OK*". These additional checks are *not* carried out if the host is a server or a custom share is involved: The maximum number of connections specified by the upper word of *SpecialNetShare* does not exceed the *MaximumAllowed* value of the WMI object. The *Data* value reported back by the check contains the results of the individual checks.	None
1E-GuaranteedState-	Fix	**Ensures the Nomad share is available**	None

Name	Type	Readable Payload and summary	Parameters
Nomad-Fix-Share		This carries out the checks as in 1E-GuaranteedState-Nomad-Check-Share above, then if any of them fails it restarts the *NomadBranch* service which should recreate the share correctly.	
1E-GuaranteedState-Nomad-Check-ShareAccount	Check	**Checks whether the Nomad share account is correctly configured** If the machine account is used rather than the default "*SMSNomadP2P&*", as specified by bit 0x80 in registry value *HKLM\SOFTWARE\1E\\NomadBranch\SpecialNetShare* , no checks are carried out. A WMI *root\cimv2\Win32_UserAccount* object for the local *SMSNomadP2P&* account must exist and the account cannot be disabled.	None
1E-GuaranteedState-Nomad-Fix-ShareAccount	Fix	**Ensures the Nomad share account is correctly configured** If the checks as described above for 1E-GuaranteedState-Nomad-Check-ShareAccount do not pass, the *NomadBranch* service is restarted to create a local *SMSNomadP2P&* account.	None
1E-GuaranteedState-Nomad-Check-SkpSwiDat	Check	**Check whether skpswi.dat exists on disk** A *skpswi.dat* file in a directory prevents ConfigMgr from falsely detecting that software is installed there during a Software Inventory scan, so Nomad requires one in its cache. Such a file must exist in the directory named by the *HKLM\SOFTWARE\1E\NomadBranch\ LocalCachePath* registry value, and it must also be a hidden file.	None
1E-GuaranteedState-Nomad-Fix-SkpSwiDat	Fix	**Ensure skpswi.dat exists on disk** If the directory named by the *HKLM\SOFTWARE\1E\NomadBranch\ LocalCachePath* registry value does not contain a "*skpswi.dat*" file, such a file is created and its hidden attribute set.	None

Name	Type	Readable Payload and summary	Parameters
1E-GuaranteedState-Nomad-Check-StartService	Check	**Checks that Nomad is running** The *NomadBranch* service must be in "*Running*" or "*Starting*" state and be configured to start automatically.	None
1E-GuaranteedState-Nomad-Fix-StartService	Fix	**Ensures that Nomad is running** If the *NomadBranch* service is not in "*Running*" or "*Starting*" state and configured to start automatically, it is started and configured to be so.	None
1E-GuaranteedState-Nomad-Check-Variant	Check	**Check whether the correct variant of Nomad (that supplied with the 1E Client, not standalone Nomad) is used for the service** This verifies that the parent directory of the executable that the Service Control Manager uses to run the *NomadBranch* service is the *Extensibility* directory of the 1E Client, and hence not, for example, an older standalone version of Nomad.	None

9.6.16.2.5 Trigger templates

The following table shows the trigger templates included in the Nomad Client Health Integrated Product Pack:

> **Note**
>
> The **Parameters** column in the following table shows the ranges and default values for the parameters. The default values are used when you create custom rules using these templates, unless you select alternative values.

Name	Readable Payload and summary	Parameters
TriggerTemplate-FileChange	The page: **Trigger templates and preconditions reference**	**File Name**

Name	Readable Payload and summary	Parameters
	was not found. Please check/update the page name used in the 'multiexcerpt-include' macro.	File path of file to be monitored, default is null.
TriggerTemplate-IntervalHours	The page: **Trigger templates and preconditions reference** was not found. Please check/update the page name used in the 'multiexcerpt-include' macro.	**Interval Hours** 0 to 999 hours (approximately 42 days), default interval is 12 hours.
TriggerTemplate-IntervalMinutes	The page: **Trigger templates and preconditions reference** was not found. Please check/update the page name used in the 'multiexcerpt-include' macro.	**Interval Minutes** 0 to 99,999 minutes (approximately 69 days), default interval is 30 minutes.
TriggerTemplate-IntervalSeconds	The page: **Trigger templates and preconditions reference** was not found. Please check/update the page name used in the 'multiexcerpt-include' macro.	**Interval Seconds** 0 to 999,999 seconds (approximately 11 days), default interval is 3600 seconds (1 hour).
TriggerTemplate-ServiceStatusChange	The page: **Trigger templates and preconditions reference** was not found. Please check/update the page name used in the 'multiexcerpt-include' macro.	**Service Name** Short name of service - for example NomadBranch.
TriggerTemplate-WindowsRegistryChange	The page: **Trigger templates and preconditions reference** was not found. Please check/update the page name used in the 'multiexcerpt-include' macro.	**Hive**, which must be one of: HKLM (default) HKCR

Name	Readable Payload and summary	Parameters
		Subkey : free text string, default empty. **Include Sub Keys** : 1/0 default 0.

Integrated Product Pack used to create the **Nomad Client Health** instruction set and **Nomad Client Health** policy.

For more information please refer to Nomad Client Health Policy.

Nomad is included as part of the 1E Client, and as part of that integration, we offer a Nomad client health compliance policy in Guaranteed State. This verifies common Nomad requirements such as ACP registration, disk availability, firewall exceptions, crash notifications and cache monitoring.

The Nomad client health policy replaces the client health tile in the Nomad dashboard plus additional remediation steps:

Keeps content distribution services up and running on Nomad clients, so that users are secure and productive

Ensures Alternative Content Provider (ACP) registration configuration is set

Maintains optimal disk availability and monitors cache size for storage capacity planning

Enforces Firewall exceptions.

Note

This policy is intended for deployment to Windows devices only.

9.6.16.2.6

Note

Instructions

1E-Explorer-NomadClientHealth-ElectionWeightVsCriticality

Policies

Nomad Client Health

Rules

Check Nomad ActiveEfficiency connectivity status

Check Nomad can communicate through the Windows Firewall

Check Nomad can generate LSZ files on ConfigMgr distribution points

Check Nomad can hash content

Check Nomad crash dumps status

Check Nomad does not have its content indexed by ConfigMgr software inventory checks

Check Nomad has a virtual directory on ConfigMgr distribution points to perform LSZ generation

Check Nomad has sufficient disk space to download content

Check Nomad is not using the Windows temp directory for caching

Check Nomad is registered as an Alternate Content Provider with ConfigMgr

Check Nomad run status

Check Nomad variant status

Check Nomad's share directory is accessible

Check Nomad's share is accessible by specific accounts

Fragments

1E-GuaranteedState-Nomad-PreCondition-MultiTests

1E-GuaranteedState-Nomad-Check-AEConnectivity

1E-GuaranteedState-Nomad-Check-AlternateContentProvider

1E-GuaranteedState-Nomad-Fix-AlternateContentProvider

1E-GuaranteedState-Nomad-Check-CacheInTemp

1E-GuaranteedState-Nomad-Check-CrashDumps

1E-GuaranteedState-Nomad-Check-DiskAvailablility

1E-GuaranteedState-Nomad-Check-DpLszEnabled

1E-GuaranteedState-Nomad-Check-DpLszVirtualDirectory

1E-GuaranteedState-Nomad-Fix-DpLszVirtualDirectory

1E-GuaranteedState-Nomad-Check-FirewallExceptions

1E-GuaranteedState-Nomad-Fix-FirewallExceptions

1E-GuaranteedState-Nomad-Check-HashingEnabled

1E-GuaranteedState-Nomad-Check-Share

1E-GuaranteedState-Nomad-Fix-Share

1E-GuaranteedState-Nomad-Check-ShareAccount

1E-GuaranteedState-Nomad-Fix-ShareAccount

1E-GuaranteedState-Nomad-Check-SkpSwiDat

1E-GuaranteedState-Nomad-Fix-SkpSwiDat

1E-GuaranteedState-Nomad-Check-StartService

1E-GuaranteedState-Nomad-Fix-StartService

1E-GuaranteedState-Nomad-Check-Variant

Trigger templates

TriggerTemplate-FileChange

TriggerTemplate-IntervalHours

TriggerTemplate-IntervalMinutes

TriggerTemplate-ServiceStatusChange

TriggerTemplate-WindowsRegistryChange

9.6.16.2.7 Policies

The following table shows the policies included in the Nomad Client Health Integrated Product Pack:

Name	Description
Nomad Client Health	The Nomad Client Health policy ensures that the health of the Nomad client is compliant with a reference baseline.

9.6.16.2.8 Rules

The following table shows the rules included in the Nomad Client Health Integrated Product Pack:

> **Note**
>
> Any parameter values shown in the table below are specifically set in the rules when the pack is uploaded. These may be different to the default values shown in the Fragments and Trigger templates tables. You can modify these if required.

Name	Type	Description	Check and Fix fragments	Triggers	Precondition fragment
Check Nomad ActiveEfficiency connectivity status	Check	Checks the Nomad agent connectivity to ActiveEfficiency.	1E-GuaranteedState-Nomad-Check-AEConnectivity No parameters	TriggerTemplate-WindowsRegistryChange Hive=*HKLM* *Subkey=Software\1E\NomadBranch\ActiveEfficiency* Include Sub keys=0 TriggerTemplate-IntervalHours intervalHours=1	1E-GuaranteedState-Nomad-PreCondition-MultiTests hasCmClient=0 sccmDp=0 smbEnabled=0
Check Nomad can communicate through the	Check	Check that there are Windows Firewall program exception	1E-GuaranteedState-Nomad-Check-FirewallExceptions	TriggerTemplate-WindowsRegistryChange Hive=*HKLM* *Subkey=Software\1E\NomadBranch\NomadBranch*	1E-GuaranteedState-Nomad-PreCondition-MultiTests

Name	Type	Description	Check and Fix fragments	Triggers	Precondition fragment
Windows Firewall		s for Nomad and its related executables.	No parameters	Include Sub keys=1 TriggerTemplate-IntervalHours intervalHours=1	hasCmClient=0 sccmDp=0 smbEnabled=0
Ensure Nomad can communicate through the Windows Firewall	Fix	Ensures there are Windows Firewall program exceptions for Nomad and its related executables.	1E-GuaranteedState-Nomad-Check-FirewallExceptions No parameters 1E-GuaranteedState-Nomad-Fix-FirewallExceptions No parameters	TriggerTemplate-IntervalHours intervalHours=1	1E-GuaranteedState-Nomad-PreCondition-MultiTests hasCmClient=0 sccmDp=0 smbEnabled=0
Check Nomad can generate LSZ files on ConfigMgr distribution points	Check	Check that LSZ generation is enabled on ConfigMgr distribution points.	1E-GuaranteedState-Nomad-Check-DpLszEnabled No parameters	TriggerTemplate-WindowsRegistryChange Hive=*HKLM* *Subkey=Software\1E\NomadBranch\NomadBranch* Include Sub keys=1 TriggerTemplate-IntervalHours intervalHours=1	1E-GuaranteedState-Nomad-PreCondition-MultiTests hasCmClient=0 **sccmDp=1** smbEnabled=0

Name	Type	Description	Check and Fix fragments	Triggers	Precondition fragment
Check Nomad can hash content	Check	Checks Nomad content hashing is enabled.	1E-GuaranteedState-Nomad-Check-HashingEnabled No parameters	TriggerTemplate-WindowsRegistryChange Hive=*HKLM* *Subkey=Software\1E\NomadBranch\NomadBranch* Include Sub keys=1 TriggerTemplate-IntervalHours intervalHours=1	1E-GuaranteedState-Nomad-PreCondition-MultiTests hasCmClient=0 sccmDp=0 smbEnabled=0
Check Nomad crash dumps status	Check	Checks whether Nomad has generated any crash dump in the last seven days.	1E-GuaranteedState-Nomad-Check-CrashDumps No parameters	TriggerTemplate-WindowsRegistryChange Hive=*HKLM* *Subkey=Software\1E\NomadBranch\NomadBranch* Include Sub keys=1 TriggerTemplate-IntervalHours intervalHours=1	1E-GuaranteedState-Nomad-PreCondition-MultiTests hasCmClient=0 sccmDp=0 smbEnabled=0
Check Nomad does not have its content indexed by ConfigMgr	Check	Checks whether skpswi.dat exists in the Nomad cache directory.	1E-GuaranteedState-Nomad-Check-SkpSwiDat No parameters	TriggerTemplate-FileChange File Name=C:\ProgramData\1E\NomadBranch\skpswi.dat TriggerTemplate-IntervalHours intervalHours=1	1E-GuaranteedState-Nomad-PreCondition-MultiTests hasCmClient=0

Name	Type	Description	Check and Fix fragments	Triggers	Precondition fragment
software inventory checks				**Warning** Do NOT use this Check if you have changed your cache location.	sccmDp=0 smbEnabled=0
Ensure Nomad does not have its content indexed by ConfigMgr software inventory checks	Fix	Ensures that skpswi.dat exists in the Nomad cache directory.	1E-GuaranteedState-Nomad-Check-SkpSwiDat No parameters 1E-GuaranteedState-Nomad-Fix-SkpSwiDat No parameters	TriggerTemplate-FileChange File Name=C:\ProgramData\1E\NomadBranch\skpswi.dat TriggerTemplate-IntervalHours intervalHours=1 **Warning** Do NOT use this Fix if you have changed your cache location.	1E-GuaranteedState-Nomad-PreCondition-MultiTests hasCmClient=0 sccmDp=0 smbEnabled=0
Check Nomad has a virtual directory on ConfigMgr distribution points to perform LSZ generation	Check	Check that an LSZFILES virtual directory has been created on a ConfigMgr distribution point.	1E-GuaranteedState-Nomad-Check-DpLszVirtualDirectory No parameters	TriggerTemplate-WindowsRegistryChange Hive=*HKLM* *Subkey=Software\1E\NomadBranch\NomadBranch* Include Sub keys=1 TriggerTemplate-IntervalHours intervalHours=1	1E-GuaranteedState-Nomad-PreCondition-MultiTests hasCmClient=0 **sccmDp=1** smbEnabled=0
Ensure Nomad has a	Fix	Ensure that an LSZFILES	1E-GuaranteedState-Nomad-Check-	TriggerTemplate-IntervalHours intervalHours=1	1E-GuaranteedState-Nomad-

Name	Type	Description	Check and Fix fragments	Triggers	Precondition fragment
virtual directory on ConfigMgr distribution points to perform LSZ generation		virtual directory has been created on a ConfigMgr distribution point.	DpLszVirtualDirectory No parameters 1E-GuaranteedState-Nomad-Fix-DpLszVirtualDirectory No parameters		PreCondition-MultiTests hasCmClient=0 **sccmDp=1** smbEnabled=0
Check Nomad has sufficient disk space to download content	Check	Check the drive that Nomad is using for content download has sufficient disk space.	1E-GuaranteedState-Nomad-Check-DiskAvailablility No parameters	TriggerTemplate-WindowsRegistryChange Hive=*HKLM* *Subkey=Software\1E\NomadBranch\NomadBranch* Include Sub keys=1 TriggerTemplate-IntervalHours intervalHours=1	1E-GuaranteedState-Nomad-PreCondition-MultiTests hasCmClient=0 sccmDp=0 smbEnabled=0
Check Nomad is not using the Windows temp directory for caching	Check	Checks that Nomad is not configured to use the Windows temporary directory	1E-GuaranteedState-Nomad-Check-CacheInTemp No parameters	TriggerTemplate-WindowsRegistryChange Hive=*HKLM* *Subkey=Software\1E\NomadBranch\NomadBranch* Include Sub keys=1 TriggerTemplate-IntervalHours intervalHours=1	1E-GuaranteedState-Nomad-PreCondition-MultiTests hasCmClient=0 sccmDp=0

Name	Type	Description	Check and Fix fragments	Triggers	Precondition fragment
		for caching.			smbEnabled=0
Check Nomad is registered as an Alternate Content Provider with ConfigMgr	Check	Check that Nomad is correctly registered as an Alternate Content Provider with ConfigMgr.	1E-GuaranteedState-Nomad-Check-AlternateContentProvider No parameters	TriggerTemplate-IntervalHours intervalHours=1	1E-GuaranteedState-Nomad-PreCondition-MultiTests **hasCmClient=1** sccmDp=0 smbEnabled=0
Ensure Nomad is registered as an Alternate Content Provider with ConfigMgr	Fix	Ensure Nomad is registered as an Alternate Content Provider with ConfigMgr, registering it if necessary.	1E-GuaranteedState-Nomad-Check-AlternateContentProvider No parameters 1E-GuaranteedState-Nomad-Fix-AlternateContentProvider No parameters	TriggerTemplate-IntervalHours intervalHours=1	1E-GuaranteedState-Nomad-PreCondition-MultiTests **hasCmClient=1** sccmDp=0 smbEnabled=0
Check Nomad run status	Check	Checks that the Nomad	1E-GuaranteedState-Nomad-Check-StartService	TriggerTemplate-IntervalHours intervalHours=1 TriggerTemplate-ServiceStatusChange	1E-GuaranteedState-Nomad-PreConditi

Name	Type	Description	Check and Fix fragments	Triggers	Precondition fragment
		service is running.	No parameters	ServiceName=*NomadBranch*	on-MultiTests hasCmClient=0 sccmDp=0 smbEnabled=0
Ensure Nomad is running	Fix	Ensure the Nomad service is running, starting the service if required.	1E-GuaranteedState-Nomad-Check-StartService No parameters 1E-GuaranteedState-Nomad-Fix-StartService No parameters	TriggerTemplate-IntervalHours intervalHours=1 TriggerTemplate-ServiceStatusChange ServiceName=*NomadBranch*	1E-GuaranteedState-Nomad-PreCondition-MultiTests hasCmClient=0 sccmDp=0 smbEnabled=0
Check Nomad variant status	Check	Checks whether the running Nomad service was one supplied with the 1E Client.	1E-GuaranteedState-Nomad-Check-Variant No parameters	TriggerTemplate-IntervalHours intervalHours=1 TriggerTemplate-ServiceStatusChange ServiceName=*NomadBranch*	1E-GuaranteedState-Nomad-PreCondition-MultiTests hasCmClient=0 sccmDp=0

Name	Type	Description	Check and Fix fragments	Triggers	Precondition fragment
					smbEnabled=0
Check Nomad's share directory is accessible	Check	Check whether Nomad needs a share, and if it does that it would be accessible to other devices.	1E-GuaranteedState-Nomad-Check-Share No parameters	TriggerTemplate-WindowsRegistryChange Hive=*HKLM* *Subkey=Software\1E\NomadBranch\NomadBranch* Include Sub keys=1 TriggerTemplate-IntervalHours intervalHours=1	1E-GuaranteedState-Nomad-PreCondition-MultiTests hasCmClient=0 sccmDp=0 **smbEnabled=1**
Ensure Nomad's share directory is accessible	Fix	Ensures that Nomad's share is accessible if it is configured to require a share.	1E-GuaranteedState-Nomad-Check-Share No parameters 1E-GuaranteedState-Nomad-Fix-Share No parameters	TriggerTemplate-IntervalHours intervalHours=1	1E-GuaranteedState-Nomad-PreCondition-MultiTests hasCmClient=0 sccmDp=0 **smbEnabled=1**
Check Nomad's share is accessible by	Check	Checks that the correct accounts are able to access	1E-GuaranteedState-Nomad-Check-ShareAccount	TriggerTemplate-WindowsRegistryChange Hive=*HKLM* *Subkey=Software\1E\NomadBranch\NomadBranch*	1E-GuaranteedState-Nomad-PreCondition-MultiTests

Name	Type	Description	Check and Fix fragments	Triggers	Precondition fragment
specific accounts		Nomad's share.	No parameters	Include Sub keys=1 TriggerTemplate-IntervalHours intervalHours=1	hasCmClient=0 sccmDp=0 **smbEnabled=1**
Ensure Nomad's share is accessible by specific accounts	Fix	Ensures that the correct accounts are able to access Nomad's share.	1E-GuaranteedState-Nomad-Check-ShareAccount No parameters 1E-GuaranteedState-Nomad-Fix-ShareAccount No parameters	TriggerTemplate-IntervalHours intervalHours=1	1E-GuaranteedState-Nomad-PreCondition-MultiTests hasCmClient=0 sccmDp=0 **smbEnabled=1**

9.6.16.2.9 Fragments

The following table shows the fragments included in the Nomad Client Health Integrated Product Pack:

> **Note**
>
> The **Parameters** column in the following table shows the ranges and default values for the parameters. The default values are used when you create custom rules using these fragments, unless you select alternative values.

Name	Type	Readable Payload and summary	Parameters
1E-GuaranteedState-Nomad-PreCondition-MultiTests	Precondition	**Check if standard conditions apply for Nomad plus optionally: is a ConfigMgr DP (<sccmDp>); has a ConfigMgr client (<hasCmClient>); SMB sharing is enabled (<smbEnabled>)** The precondition passes for all of the following standard tests: The device is running a version of Windows - Nomad is only supported on Windows operating systems The device is not running Windows XP - which is no longer supported by Nomad The *NomadBranch* service is installed, although not necessarily running. The precondition also tests for each of the following if it is enabled by changing its parameter from 0 to 1: **hasCmClient** : The ConfigMgr client is installed **sccmDp** : The device is a ConfigMgr Distribution Point (DP) **smbEnabled** : SMB sharing of Nomad's cache is enabled. If **smbEnabled** test is set in the rule precondition then an additonal test is made to see if the device is a Domain Controller (DC). When installed on a DC Nomad must use its computer account instead of SMSNomadP2P& in order to share its cache. This requires registry value *HKLM\SOFTWARE\1E\NomadBranch\SpecialNetShare* to have its 0x80 bit set. If not set then Nomad does not share its cache on a DC and does not respond to elections. For early adopters, the readable payload of this precondition was: Carries out the specified checks; if any fail (i.e. they are logically AND-ed) then the preconditions fails.	hasCmClient sccmDp smbEnabled Range 0 or 1, defaults=0
1E-GuaranteedState-Nomad-Check-	Check	**Check whether there is a working connection to ActiveEfficiency** Tests whether the URL given by registry value *HKLM\SOFTWARE\1E\NomadBranch\ActiveEfficiency\PlatformUrl,* if it is not empty, is contactable and returns a 200 code.	None

Name	Type	Readable Payload and summary	Parameters
AEConnectivity			
1E-GuaranteedState-Nomad-Check-AlternateContentProvider	Check	**Check whether Nomad is correctly registered within Microsoft ConfigMgr** Check that the ConfigMgr client's list of ACPs includes an object for Nomad in WMI class *ROOT\ccm\Policy\Machine\RequestedConfig\CCM_DownloadProvider*, with *CLSID* "*25A6160D-4543-495F-975E-32CFBD6F70E0*", *LogicalName* "*NomadBranch*", *V4CompatibleHash* is set, and just "*<Data></Data>*" in *GlobalSettings*.	None
1E-GuaranteedState-Nomad-Fix-AlternateContentProvider	Fix	**Ensures Nomad is correctly registered within Microsoft ConfigMgr** If the same checks as 1E-GuaranteedState-Nomad-Check-AlternateContentProvider are not satisfied, restarts the *NomadBranch* service, waits 10 seconds for Nomad to establish itself as an ACP, then carries out the checks again.	None
1E-GuaranteedState-Nomad-Check-CacheInTemp	Check	**Check whether Nomad's cache is not in a temporary directory** The Nomad cache can sometimes be configured to be in the Windows *Temp* directory (usually *C:\Windows\Temp*) or one of its subdirectories. Since all the contents of the Windows *Temp* directory are considered to be transient and could be deleted at any time, this is not suitable for Nomad's cache which should be a permanent location. The check examines Nomad's *HKLM\SOFTWARE\1E\NomadBranch\LocalCachePath* registry value and verifies that the specified location actually exists. It then gets the *TEMP* environment variable, which, because both the *1E Client* and *NomadBranch* services run as *Local System*, is usually the WIndows *TEMP* directory. If the *LocalCachePath* value is the same as the *TEMP* environment variable, or *LocalCachePath* specifies a subdirectory within it, the check fails.	None

Name	Type	Readable Payload and summary	Parameters
1E-GuaranteedState-Nomad-Check-CrashDumps	Check	**Check whether there have been any crashdump files created by Nomad in last 7 days** Nomad dump files are saved in the same directory as the log file, the parent directory of the *HKLM\SOFTWARE\1E\NomadBranch\LogFileName* registry value. The check looks in here for any files with a "*.dmp*" suffix (ignoring case), and if it finds any examines the modification time (not creation time!) of each, reporting as a failed check any that were modified in the last 7 days. So the check passes if there are no "*.dmp*" files or they are all older than 7 days.	None
1E-GuaranteedState-Nomad-Check-DiskAvailablility	Check	**Checks whether there is sufficient disk space for Nomad** This examines Nomad's *HKLM\SOFTWARE\1E\NomadBranch\PercentAvailableDisk* registry value. (It ignores the older *MaxCacheSizeMB* value which has been superseded by *PercentAvailableDisk*.) If the value is greater than or equal to 80, the check fails because the setting is too high. It then compares the size of the contents of the folder given by *HKLM\SOFTWARE\1E\NomadBranch\ LocalCachePath* in the registry, i.e. Nomad's cache, with the free space of the drive on which the folder resides, as reported by WMI's *root\cimv\Win32_LogicalDisk*. The check fails if the percentage of free space on the drive is less than or equal too *PercentAvailableDisk*.	None
1E-GuaranteedState-Nomad-Check-DpLszEnabled	Check	**Check whether web LSZ generation is correctly configured on stand alone distribution points** Nomad automatically sets up LSZ file generation on DPs that are ConfigMgr site servers, but extra configuration is required for standalone DPs. The device is a standalone DP if, under registry key *HKLM\SOFTWARE\Microsoft\SMS\Operations Management\SMS Server Role*, the subkey *SMS Distribution Point* exists but *SMS Site Server* does not. If the device is a standalone DP, registry value *HKLM\SOFTWARE\1E\\NomadBranch\SpecialNetShare* should have its 16384/0x4000 bit set to turn on web LSZ generation for HTTP/HTTPS enabled clients; if not, the check fails.	None

Name	Type	Readable Payload and summary	Parameters
1E-GuaranteedState-Nomad-Check-DpLszVirtualDirectory	Check	**Check whether the LSZ directory is correctly configured on distribution points** At time of writing there is a bug such that the overall check status is usually "Passed" even when individually reported checks fail. If the device is a standalone DP, the check first verifes that registry value *HKLM\SOFTWARE\1E\\NomadBranch\SpecialNetShare* has its 16384/0x4000 bit set. (This bit is not required for a DP on a site server.) Then the *LSZFILES* web site is examined to verify that all these conditions are satisfied: Anonymous authentication is enabled Windows authentication is enabled No SSL Default document is enabled Directory browsing is enabled, with Date, Time, Size, Extension and LongDate all available Content indexing is disabled.	None
1E-GuaranteedState-Nomad-Fix-DpLszVirtualDirectory	Fix	**Ensure that the LSZ directory is correctly configured on distribution points** At time of writing there is a bug such that the overall check status is usually "Passed" even when individually reported checks fail. If any of the conditions described above for the corresponding check fragment is not true, the LSZFILES website is reconfigured to set that condition.	None
1E-GuaranteedState-Nomad-Check-FirewallExceptions	Check	**Checks whether firewall exceptions exist for Nomad** First is a check that at least one Windows firewall profile is enabled and that the firewall itself is enabled with either *HKLM\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile\EnableFirewall* set to 1 or *HKLM\SOFTWARE\Policies\Microsoft\WindowsFirewall\StandardProfile\EnableFirewall* set to 1 in the registry. If no firewall and	None

Name	Type	Readable Payload and summary	Parameters

no firewall profile is enabled then no firewall exceptions are necessary and so there is nothing more to do.

Otherwise,the Nomad-related firewall rules are examined. These are the rules named:

NomadBranch.exe

NomadPackageLocatorTcp

NomadPackageLocatorUdp

PackageStatusRequestTcp

PackageStatusRequestUdp

NomadBranchPeerHttp

NomadBranchPeerHttps

Using the *NomadBranch* service's path of *NomadBranch.exe*, the paths of *NomadPackageLocator.exe* and *PackageStatusRequest.exe* are deduced. Using the *HKLM\SOFTWARE\1E\NomadBranch\P2PEnabled* , *P2P_Port* , *P2PHttpPort* , and *P2PHttpsPort* settings in the registry, the fragment works out which Nomad features are enabled and hence which firewall rules are required. The firewall rule checks involve:

Whether the rule even exists

That the rule is enabled and not blocked

The local port (which may be a specific one or all)

Which protocol (TCP or UDP) is involved

The path to the associated executable.

Rulesfor *NomadBranch.exe* , *NomadPackageLocatorTcp* , *NomadPackageLocatorUdp* , *PackageStatusRequestTcp* and *PackageStatusRequestUdp* must always be correctly defined. *NomadBranchPeerHttp* is only required if the 0x20 bit of *P2P_Enabled* is set, and likewise the 0x40 bit requires *NomadBranchPeerHttps* .

Name	Type	Readable Payload and summary	Parameters
1E-GuaranteedState-Nomad-Fix-FirewallExceptions	Fix	**Ensures the required firewall exceptions exist for Nomad** This carries out all the checks as described above for 1E-GuaranteedState-Nomad-Check-FirewallExceptions then, for each absent or incorrectly configured rule that is required to support the *P2PEnabled* registry setting,configures that rule.	None
1E-GuaranteedState-Nomad-Check-HashingEnabled	Check	**Check whether hashing is enabled in Nomad** This examines the *HKLM\SOFTWARE\1E\NomadBranch\CompatibilityFlags* registry value. If the host is a ConfigMgr DP the 0x80000 bit should be set ("enable full hash generation for SIS content when an LsZ file is generated on a DP"), otherwise the 0x100000 bit ("abort download on the Nomad client if an LsZ hash mismatch is detected").	None
1E-GuaranteedState-Nomad-Check-Share	Check	**Checks whether the Nomad share is available** This first checks the firewall settings. If the firewall is enabled then "*File and Printer Sharing*" (i.e. SMB) cannot be disabled. Next the 0x10 bit of registry value *HKLM\SOFTWARE\1E\\NomadBranch\SpecialNetShare* is examined to see if the share name is the default "*NomadSHR*" or the hidden "*NomadSHR$*". The share's security descriptor is read and check made that the local "*SMSNomadP2P&*" account has read permission. The share's properties are then verified as follows: The shared directory is that named by registry value *HKLM\SOFTWARE\1E\NomadBranch\ LocalCachePath* The shared directory also matches the *Path* from WMI's *root\cimv2\Win32_Share* object for the share. The *Status* of the *root\cimv2\Win32_Share* object is "*OK*". These additional checks are *not* carried out if the host is a server or a custom share is involved:	None

Name	Type	Readable Payload and summary	Parameters
		The maximum number of connections specified by the upper word of *SpecialNetShare* does not exceed the *MaximumAllowed* value of the WMI object. The *Data* value reported back by the check contains the results of the individual checks.	
1E-GuaranteedState-Nomad-Fix-Share	Fix	**Ensures the Nomad share is available** This carries out the checks as in 1E-GuaranteedState-Nomad-Check-Share above, then if any of them fails it restarts the *NomadBranch* service which should recreate the share correctly.	None
1E-GuaranteedState-Nomad-Check-ShareAccount	Check	**Checks whether the Nomad share account is correctly configured** If the machine account is used rather than the default "*SMSNomadP2P&*", as specified by bit 0x80 in registry value *HKLM\SOFTWARE\1E\\NomadBranch\SpecialNetShare* , no checks are carried out. A WMI *root\cimv2\Win32_UserAccount* object for the local *SMSNomadP2P&* account must exist and the account cannot be disabled.	None
1E-GuaranteedState-Nomad-Fix-ShareAccount	Fix	**Ensures the Nomad share account is correctly configured** If the checks as described above for 1E-GuaranteedState-Nomad-Check-ShareAccount do not pass, the *NomadBranch* service is restarted to create a local *SMSNomadP2P&* account.	None
1E-GuaranteedState-Nomad-Check-SkpSwiDat	Check	**Check whether skpswi.dat exists on disk** A *skpswi.dat* file in a directory prevents ConfigMgr from falsely detecting that software is installed there during a Software Inventory scan, so Nomad requires one in its cache. Such a file must exist in the directory named by the *HKLM\SOFTWARE\1E\NomadBranch\ LocalCachePath* registry value, and it must also be a hidden file.	None

Name	Type	Readable Payload and summary	Parameters
1E-GuaranteedState-Nomad-Fix-SkpSwiDat	Fix	**Ensure skpswi.dat exists on disk** If the directory named by the *HKLM\SOFTWARE\1E\NomadBranch\LocalCachePath* registry value does not contain a "*skpswi.dat*" file, such a file is created and its hidden attribute set.	None
1E-GuaranteedState-Nomad-Check-StartService	Check	**Checks that Nomad is running** The *NomadBranch* service must be in "*Running*" or "*Starting*" state and be configured to start automatically.	None
1E-GuaranteedState-Nomad-Fix-StartService	Fix	**Ensures that Nomad is running** If the *NomadBranch* service is not in "*Running*" or "*Starting*" state and configured to start automatically, it is started and configured to be so.	None
1E-GuaranteedState-Nomad-Check-Variant	Check	**Check whether the correct variant of Nomad (that supplied with the 1E Client, not standalone Nomad) is used for the service** This verifies that the parent directory of the executable that the Service Control Manager uses to run the *NomadBranch* service is the *Extensibility* directory of the 1E Client, and hence not, for example, an older standalone version of Nomad.	None

9.6.16.2.10 Trigger templates

The following table shows the trigger templates included in the Nomad Client Health Integrated Product Pack.

Note

The **Parameters** column in the following table shows the ranges and default values for the parameters. The default values are used when you create custom rules using these templates, unless you select alternative values.

Name	Readable Payload and summary	Parameters
TriggerTemplate-FileChange	**On change of file "<fileName>"** When a file changes (Windows only)	**File Name** File path of file to be monitored, default is null.
TriggerTemplate-IntervalHours	**Every <intervalHours> hours** Periodic (hours)	**Interval Hours** 0 to 999 hours (approximately 42 days), default interval is 12 hours.
TriggerTemplate-IntervalMinutes	**Every <intervalMinutes> minutes** Periodic (minutes)	**Interval Minutes** 0 to 99,999 minutes (approximately 69 days), default interval is 30 minutes.
TriggerTemplate-IntervalSeconds	**Every <intervalSeconds> seconds** Periodic (seconds)	**Interval Seconds** 0 to 999,999 seconds (approximately 11 days), default interval is

Name	Readable Payload and summary	Parameters
		3600 seconds (1 hour).
TriggerTemplate-ServiceStatusChange	**On change of running state of the "<serviceName>" service** When the state of the named Windows service changes **Note** You can determine the short name of a service using the PowerShell cmdlet `get-service -DisplayName "Network Location Awareness"` This will return **NlaSvc** in the above example. It is this short name you specify in the <ServiceName> parameter.	**Service Name** Short name of service - for example NomadBranch.
TriggerTemplate-WindowsRegistryChange	**On change of registry values in "<hive>\<subkey>" (include subkeys=<includeSubkeys>)** When the value of a Windows registry key changes.	**Hive**, which must be one of: HKLM (default) HKCR **Subkey** : free text string, default empty. **Include Sub Keys** : 1/0 default 0.

9.6.17 Nomad release information

9.6.17.1 Nomad 8.1 release information – last updated 09-August-2022

These notes contain late-breaking information about Nomad 8.1 that you need to have to successfully install and use the product. For the most up-to-date information please see the online

readme. You should read these release notes and the online documentation for Nomad 8.1 thoroughly before installing the software.

9.6.17.1.1 New features in Nomad 8.1

This release introduces the following new and enhanced features:

9.6.17.1.1.1 Platform

Insights on how Nomad enhances user experience - with the rapid shift to a Work From Anywhere (WFA) workforce and an increased focus on the Digital End-User eXperience, Nomad on Tachyon Platform now provides insights into how it helps to ensure a great user eXperience. With the introduction of Nomad's Bandwidth Protection Reporting, you can now see how Nomad is preventing end-user disruption due to software and update deployments. Bandwidth Protection Reporting will allow you to see the positive impact Nomad is having across the organization, to individual sites, subnets, all the way down to a single client.

Support for Cloud-based content in Task Sequences- cloud-based services to support Work From Anywhere (WFA) users are becoming more critical to the way enterprises work, there is an increased reliance on Cloud Distribution Points for distributing content.

Feature improvements - as Configuration Manager evolves and new features are released, Nomad on Tachyon Platform is being continuously maintained to ensure it works seamlessly with new releases.

Content Distribution service no longer uses SQL Linked Server to connect to Microsoft Endpoint Configuration Manager.

9.6.17.1.1.2 Client

NomadBranch 8.1 client is the Nomad module in 1E Client 8.1

Support for Cloud-based content in Task Sequences - cloud-based services to support Work From Anywhere (WFA) users are becoming more critical to the way enterprises work, there is an increased reliance on Cloud Distribution Points for distributing content.

Enhancements:

Improvements to the Certificate Selection criteria to authenticate with a DP (or any download source)

Download reporting now includes back-off data, for Bandwdith Protection Reporting.

9.6.17.1.1.3 Tools

Nomad AdminUI Console Extensions now require .NET Framework 4.8

Cloud infrastructure support

Enhancements:

Provide a way for SCCM Console users to use alternate credentials to authenticate with ContentDistribution/Platform

PlatformUrl validation is improved, by logging a warning during installation. In UI mode users have the option of continuing with the installation.

9.6.17.2 Troubleshooting

9.6.17.2.1 Online help

Nomad comes with online help that shows you how to install, configure and use the product. Click the following link to view the help:

Introducing Nomad.

For support queries, please:

Use https://support.1e.com/ where you can search the KB or submit a support case.

Contact support@1e.com.

9.6.17.2.2 Known issues

The current known issues related to the installation and running of Nomad 8.1 can be found on the Troubleshooting Known issues page of the Nomad documentation.

Known issues for the Tachyon Platform and other applications can be found in the 1E platform - Known issues documentation.

9.6.17.3 Nomad Release History

9.6.17.3.1 8.1.2.60 11 Mar 2022

9.6.17.3.1.1 Features and enhancements

For new features in this release please refer to the top of the page.

Nomad and Content Distribution are included in Tachyon Platform 8.1.

NomadBranch 8.1 client is the Nomad module in 1E Client 8.1.

9.6.17.3.1.2 Contained fixes (Nomad and Content Distribution)

Q22048 - An unhandled exception is thrown if Content Distribution is installed on a non-English server. (TFS 247999)

Q22010 - Task sequence does not get synced if an entry of precached task sequence was created before the CMSync (TFS 247742)

Q21984 - Multiple Task sequences with same name displayed on Nomad dashboard TaskSequence page. (TFS 246962)

Q21982 - Nomad Sites page on Nomad dashboard displays 0 for “Unknown” category of site. (TFS 246477)

Q21980 - NomadBranch Admin UI Extensions: "Pre-caching Jobs" view only shows 50 most recent jobs (TFS 246609)

Q21978 - Device tab displays status as "Partially Downloaded" (TFS 247193)

Q21976- Subnet Drawer displays "Partially downloaded" status (TFS 247268)

Q21974 - Selecting Subnet Drawer of TS content causes exception (TFS 247269)

Q21972 - Precache jobs report incorrectly as “Partially Downloaded” (TFS 245156)

Q21856 - Subnets counts on Nomad Site page gets changed by changing time filter. (TFS 245938)

Q21854 - Subnet Drawers and Site Detail page shows null subnet (TFS 245937)

Q21852 - Device Details page shows incorrect counts (TFS 245936)

Q21850 - Content Details page never returns data. (TFS 245939)

9.6.17.3.1.3 Contained fixes (client)

Q22068 - Content download from Cloud DP does not work when Enhanced HTTP is enabled in CM 2107 (TFS 248101)

Q22056 - Superfluous informational message in NomadBranch log (TFS 249059)

Q22054 - Failing to decrypt content while downloading from Cloud Distribution Points (TFS 247202)

Q21930 - Nomad precache content status is not in sync with Content Download DB (TFS 244875)

Q21928 - Nomad download over enhanced HTTP fails with CM 2107 (TFS 245217)

9.6.17.3.1.4 Contained fixes (tools)

Q22028 - ConfigMgr Console Crashes when attempting to search in Nomad specific views (TFS 246444)

Q22026 - Nomad Baseline wizard creates incorrect baseline for missing integer values (TFS 247629)

Q22024 - Support for providing alternate credentials in SCCM Extensions to authenticate with Tachyon Platform (TFS 246003)

9.6.17.3.2 8.0.4.298 29 Oct 2021

9.6.17.3.2.1 Features and enhancements

For new features in this release please refer to Nomad features by release.

Nomad and Content Distribution are included in Tachyon Platform 8.0.

NomadBranch 8.0 client is the Nomad module in 1E Client 8.0.

OSD Tools and Nomad Configuration Manager console extensions are now included in a single installer called Nomad Branch Tools.

9.6.17.3.2.2 Contained fixes (Nomad and Content Distribution)

Q21754 - CM Sync fails to sync content because of null SourceVersion (TFS 241994)

Q21750 - Nomad clients are unable to communicate with ContentDistribution (TFS 244275)

Q21702 - An error occurred whilst migrating legacy pre cache data. CM sync failed. (TFS 237645)

Q21700 - Get Migration Settings TS action sets an incorrect PBAComputerName for restore (TFS 239635)

Q21698 - Failed to register devices because Ip4SubnetAddr column does not allow nulls. (TFS 232498)

Q21678 - Duplicate Devices in Tachyon and Nomad dashboards (TFS 229352)

Q21612 - Support for feature updates in TS (TFS 233798)

Q21610 - Known Subnets are showing under Unknown as well in Nomad Dashboard (TFS 234520)

Q21608 - CM sync's failing in CD due to FOREIGN KEY constraint (TFS 234770)

Q21598 - CM Sync's failing in Content Distribution (TFS 233608)

9.6.17.3.2.3 Contained fixes (client)

Q21786 - Nomad - Automatic CacheClean updates. (TFS 244966)

Q21784 - Nomad is not doing any DP load balancing (TFS 234960)

Q21782 - Nomad failing download content requested by VMware Workspace One (TFS 244963)

Q21724 - Nomad - Get Migration Settings step is not using correct MAC address to query CM computer association (TFS 241912)

Q21694 - Nomad - CDSSync doesn't report complete download data (TFS 236909)

Q21692 - Nomad isn't honouring Job timeout (TFS 237633)

Q21690 - Nomad crashing on multiple devices (TFS 235899)

Q21628 - Nomad fails during byte-range download if ContentRegistration is disabled (TFS 235180)

Q21602 - Standardize Nomad date logging (TFS 231355)

Q21600 - Nomad hash errors on 3rd party software update downloads via WUMU (TFS 230142)

9.6.17.3.2.4 Contained fixes (tools)

Q21790 - AdminUI - Automatic CacheClean updates. (TFS 244966)

Q21788 - AdminUI - Nomad is not doing any DP load balancing (TFS 234960)

Q21696 - Nomad Branch Tools - Nomad isn't honouring Job timeout (TFS 237633)

Q21604 - Nomad Branch Tools - Standardize Nomad date logging (TFS 231355)

Q21538 - Nomad Branch Tools - SSD is not working in Windows PE (TFS 232110)

9.6.17.3.3 7.1.5.456 25 Mar 2021

For new features in this release please refer to Nomad features by release.

Nomad is now an application in Tachyon Platform 5.2, and ActiveEfficiency has been replaced by Content Distribution in Tachyon Platform 5.2.

NomadBranch 7.1 client is the Nomad module in 1E Client 5.2.

Nomad Branch (OSD) Tools and Nomad Configuration Manager console extensions are provided as separate installers.

9.6.17.3.3.1 Contained fixes (client)

Q21386 - Nomad does not work as ACP after CM Client upgrade to 5.00.9040.1015 (CB 2010) (TFS 221969)

Q21374 - Nomad - Fails to retrieve content locations from the MP if there are no boundary groups except the default (TFS 220818)

Q21330 - Nomad - Failing to get patches from WUMU (TFS 212827)

9.6.17.3.3.2 Contained fixes (tools)

Q21372 - ValidateWiFi step fails on non-English machines in WSA task sequence (TFS 221362)

9.6.17.3.4 7.0.200.214 24 Jul 2020

9.6.17.3.4.1 Features and enhancements

This maintenance release is implemented as the Nomad module in 1E Client 5.1 and introduces the following features:

Certificate-based client authentication for Nomad P2P communication

Configuration Manager Enhanced HTTP support

Support for multiple Certificate Authorities

Improved PKI client certificate selection logic

VMWare Workspace One support

Handling download content for "expired" offer

Improved handling of updated Software Update content

Option to reduce election notifications in Nomad logs

Nomad 1EClient Telemetry

9.6.17.3.4.2 Contained fixes

Q21089 - Unable to download Pre-cache Content from Cloud DP on VPN clients

Q21061, Q21051 - CertIssuer - specifying issuer name sub string does not work for selecting Server Auth PKI cert for Nomad P2P / PBA over HTTPS

Q21021, Q21033 - Support pre-caching on internet clients using AE on internet and content distributed on CDP or IBCM based DP

Q21021, Q21033 - Nomad failing to download the content in first attempt (from CMG) and succeeding in second attempt after 10 min

Q20979, Q20973 - If enhanced http was enabled, the Pre-stage Content Using Nomad step failed to download the content.

Q20979, Q20973 - If using SMB to download content from DP in WinPE, the login to the DP share failed and Nomad failed to download the content.

Q20979, Q20973 - The Pre-stage Content Using Nomad step failed to download content over SMB if the SMB path had a backslash at the end

Q20943 - Enable DP recycling feature in Win-PE by default

Q20983 - Legacy Pre-Stage using Nomad task sequence step fails in CB1910

Q20983, Q20979, Q20973 - Nomad Task Sequence steps fail if Nomad module is not initialized

Q20973 - Nomad fails a download when similar expired deployment is present

9.6.17.3.5 7.0.100.77 27 Mar 2020

9.6.17.3.5.1 Features and enhancements

NomadBranch 7.0.100 client is the Nomad module in 1E Client 5.0

9.6.17.3.5.2 Contained fixes

Q20694 - When an LST is created for a cloud DP a zero byte file causes download failure

Q20682 - LSZGEN fails on long file path with Nomad SECure enabled

Q20680 - LSZGEN issues on DP when CACHEPATH installer property has no trailing backslash

Q20678 - Physical path in the LSZFILES virtual directory in IIS is not updated when LocalCachePath is changes after installation

Q20676 - Nomad downloads previous version of content

Q20674 - Captive Portal Web page (eg Logon Page from Public Wifi) may cause issues with Nomad Downloads

Q20570 - Nomad fails to download updated task sequence references with future deployment dates

Q20672 - Nomad fails to download updated task sequence references with ConfigMgr Pre-download option

Q20670 - Nomad service failure on PBA host with hidden share enabled during PBA backup

Q20666 - PBA Size estimation doesn't update TS progress bar

Q20664 - Nomad not failing package on CRC failure

Q20662 - Nomad Status Message Improvements

Q20660 - Nomad service may fail whilst running cachecleaner manually

Q20658 - Unable to download 0365 updates with Nomad

Q20733 - Local SSD is not working

Q20592 - 1EClient Nomad Module's install fails if Windows Firewall service is disabled or in stopped state

9.6.17.3.6 7.0.0.203 04 May 2019

9.6.17.3.6.1 Features and enhancements

NomadBranch 7.0 client is replaced as the Nomad module in 1E Client 4.1

Support for NomadBranchTools installation on SCCM SMS Provider

Support for Windows 10 Express Files Update

Support for Regular Software Update (including Win 10 Feature updates) downloads from Windows Update / Microsoft Update (WUMU)

Support for Windows 10 Express Files and Office 365 downloads from Windows Update / Microsoft Update (WUMU)

New Content Registration Cycle to mark failed content registrations with ActiveEfficiency server

New Nomad registry settings to average out the content registration and SSD request load in AE where CM deployment size is of the order of 100K or more.

Support for P2P downloads when a client machine switches from NomadInhibitedAdSite to a non InhibitedAdSite

Ignore Local SSD if machine is in a NomadInhibitedSubnet

Support for SSD usage as a criteria for Nomad cache clean cycle

Some registry values have new defaults set to support new features and running Tachyon on computers that do not have the Configuration Manager client. These include SpecialNetShare and CompatibilityFlags.

DP recycling feature in WinPE is enabled by default, for upgrade from previous version the previous settings will be preserved.

Dynamic Block Size (DBS) is now disabled by default (even in WinPE), for upgrade from previous version the previous settings will be preserved.

MulticastSupport is now disabled by default, for upgrade from previous version the previous settings will be preserved.

Broadcasting download statistics is disabled by default, for upgrade from previous version the previous settings will be preserved.

Support for downloading from source over HTTP/S or SMB is enabled by default, for upgrade from previous version the previous settings will be preserved.

By default SHA-256 is used to verify integrity of downloaded content.

Stage Nomad and Install Nomad TS steps updated to support staging and installing 1EClient

Added 'SMSTSNomadDefaultCachePriority' TS variable to be used when SMSTSNomad is unable to get cache priority from package policy or policy itself is missing from TS variables.

Support for TLS 1.1/1.2 in environments where TLS 1.0 is disabled

Status Message consistency improvements

1E Client Health feature has been removed

9.6.17.3.6.2 Contained fixes

Q20390 - Allow WSA to exclude data backup

Q20384 - Cache cleaner unable to remove content when cache already exceeded configured size

Q20382 - Nomad O365 download from untrusted forest not using Network Access Account (NAA)

Q20368 - Active Efficiency Web service logs exception if FQDN is missing from client data

Q20350 - Same disqualified master keeps winning elections

Q20322 - Don't download content to USB if it's already in the Nomad cache

Q20314 - HTTP Proxy causes failures while downloading from Windows Update

Q20310 - Nomad Service Failure while logging disqualification details

Q20266 - SMSTSNomad fails if the Nomad service is slow to start

Q20262 - NMDS ExtraReplyDelayMS setting capped at 5000

Q20260 - Nomad download logs CopyLoopWait CopyError: Missing File(s)

Q20256 - Nomad failing to download SU from Cloud Distribution Points

Q20254 - TLS 1.2 compliance testing and fixes for Nomad

Q20252 - CTM DP order with neighboring boundary group DPs

Q20250 - Nomad O365 downloads fail when requested range does not exist

Q20248 - Active Efficiency Nomad sync is failing with a "Arithmetic overflow error converting expression to data type bigint" error

Q20246 - Cannot download software updates from Windows Update

Q20198 - LSZ downloads fail when package contains files with Unicode names

Q20196 - Ignore Local SSD if machine is in a NomadInhibitedSubnet

Q20194 - SSD queries may connect on inhibited subnets if the master moves

Q20192 - Active Efficiency experiencing database deadlocks at high utilization

Q20144 - Express Update support for Nomad (from on premises DP)

Q20142 - RDC doesn't work in some cases

Q20140 - Nomad downloads previous version of content

Q20138 - SMSTSNomad does not set cache priority correctly

Q20136 - Issues working Nomad HTTP with WINHTTP Proxy

Q20134 - Disqualifications sent when too many connections reached over HTTP(S)

Q20132 - Slow Nomad downloads from DP when BranchCache is enabled

Q20130 - NomadBranch Range Overlap Exception

Q20128 - Nomad Not Sending Error Status Messages

Q20056 - NomadBranch fails on NMDS_FIND HTTPPull when trying to restore a PBA user state backup

Q20054 - Nomad not failing package on CRC failure

9.6.17.4 Nomad 8.1 release information – last updated 09-August-2022

These notes contain late-breaking information about Nomad 8.1 that you need to have to successfully install and use the product. For the most up-to-date information please see the online readme. You should read these release notes and the online documentation for Nomad 8.1 thoroughly before installing the software.

9.6.17.4.1 New features in Nomad

Many Nomad features are available with minimal configuration of the 1E Client. However, some features require additional configuration of the 1E Client on Configuration Manager Distribution Points.

9.6.17.4.1.1 Platform

Works with Tachyon 8.1

Insights on how Nomad enhances user experience - with the rapid shift to a Work From Anywhere (WFA) workforce and an increased focus on the Digital End-User eXperience, Nomad on Tachyon Platform now provides insights into how it helps to ensure a great user eXperience. With the introduction of Nomad's Bandwidth Protection Reporting, you can now see how Nomad is preventing end-user disruption due to software and update deployments. Bandwidth Protection Reporting will allow you to see the positive impact Nomad is having across the organization, to individual sites, subnets, all the way down to a single client.

Support for Cloud-based content in Task Sequences - cloud-based services to support Work From Anywhere (WFA) users are becoming more critical to the way enterprises work, there is an increased reliance on Cloud Distribution Points for distributing content.

Feature improvements - as Configuration Manager evolves and new features are released, Nomad on Tachyon Platform is being continuously maintained to ensure it works seamlessly with new releases.

9.6.17.4.1.2 Client

NomadBranch 8.1 client is the Nomad module in 1E Client 8.1

Support for Cloud-based content in Task Sequences - cloud-based services to support Work From Anywhere (WFA) users are becoming more critical to the way enterprises work, and there is an increased reliance on Cloud Distribution Points for distributing content.

Enhancements:

Improvements to the Certificate Selection criteria to authenticate with a DP (or any download source)

Download reporting now includes back-off data, for Bandwdith Protection Reporting.

9.6.17.4.1.3 Tools

Nomad AdminUI Console Extensions now require .NET Framework 4.8

Cloud infrastructure support

Enhancements:

Provide a way for SCCM Console users to use alternate credentials to authenticate with ContentDistribution/Platform, for details refer to Using Nomad pre-caching.

PlatformUrl validation is improved, by logging a warning during installation. In UI mode users have the option of continuing with the installation, for details refer to Installing Nomad Branch Tools.

9.6.17.5 Nomad features by release

9.6.17.5.1 Summary

A list of the Tachyon features organized by the release they were implemented in. Links through to the features have been provided for convenience.

9.6.17.5.2 New features in Nomad 8.1

This release introduces the following new and enhanced features:

9.6.17.5.2.1 Platform

Insights on how Nomad enhances user experience - with the rapid shift to a Work From Anywhere (WFA) workforce and an increased focus on the Digital End-User eXperience, Nomad on Tachyon Platform now provides insights into how it helps to ensure a great user eXperience. With the introduction of Nomad's Bandwidth Protection Reporting, you can now see how Nomad is preventing end-user disruption due to software and update deployments. Bandwidth Protection Reporting will allow you to see the positive impact Nomad is having across the organization, to individual sites, subnets, all the way down to a single client.

Support for Cloud-based content in Task Sequences- cloud-based services to support Work From Anywhere (WFA) users are becoming more critical to the way enterprises work, there is an increased reliance on Cloud Distribution Points for distributing content.

Feature improvements - as Configuration Manager evolves and new features are released, Nomad on Tachyon Platform is being continuously maintained to ensure it works seamlessly with new releases.

Content Distribution service no longer uses SQL Linked Server to connect to Microsoft Endpoint Configuration Manager.

9.6.17.5.2.2 Client

NomadBranch 8.1 client is the Nomad module in 1E Client 8.1

Support for Cloud-based content in Task Sequences - cloud-based services to support Work From Anywhere (WFA) users are becoming more critical to the way enterprises work, there is an increased reliance on Cloud Distribution Points for distributing content.

Enhancements:

Improvements to the Certificate Selection criteria to authenticate with a DP (or any download source)

Download reporting now includes back-off data, for Bandwdith Protection Reporting.

9.6.17.5.2.3 Tools

Nomad AdminUI Console Extensions now require .NET Framework 4.8

Cloud infrastructure support

Enhancements:

Provide a way for SCCM Console users to use alternate credentials to authenticate with ContentDistribution/Platform

PlatformUrl validation is improved, by logging a warning during installation. In UI mode users have the option of continuing with the installation.

9.6.17.5.3 Released in Nomad 8.0

9.6.17.5.3.1 Platform

Works with Tachyon Platform 8.0

Integrating Nomad with WakeUp

Enhancements:

Task Sequence support for Windows feature updates

Automatic grooming of the Content Distribution database

Support for Windows Authentication between Background Channel and Content Distribution API

Tachyon Setup: Nomad screen has improved authentication options

Improving performance of the dashboards

API versioning using Tachyon SDK.

9.6.17.5.3.2 Client

NomadBranch 8.0 client is the Nomad module in 1E Client 8.0

New registry setting **SiteSSDMinPackageSizeKB**to set the minimum size of content before making SSD request

Installer changes:

Integrating Nomad with WakeUp

Enable **Nomad FanOut** as a default - default value of **SpecialNetShare**has changed to 0x2060 (8288)

Platform features enabled by using the BackgroundChannelUrl instead of PlatformURL

Enhancements to **CacheCleaner** functionality to better support remote users as part of the Working From Anywhere initiative.

9.6.17.5.3.3 Tools

A single combined installer called **Nomad Branch Tools** containing both OSD Tools and Nomad Configuration Manager console extensions.

9.6.17.5.4 Released in Nomad 7.1

9.6.17.5.4.1 Platform

Works with Tachyon Platform 5.2

Modernized backend infrastructure - Nomad requires a back-end server, which was previously the legacy ActiveEfficiency platform, this has been replaced by the Tachyon Platform to provide Single-Site download, Pre-caching and a new Dashboard. For customers moving to Modern Management, Nomad provides visibility and control of Delivery Optimization, which is used by Intune, MS store and MS update.

Leverage the Tachyon Platform and 1E Client - with the Tachyon Platform you can enable further features including Experience, User Sentiment, Guaranteed State and Patch Success, as well as opening up real-time management to any task by acquiring the appropriate license.

Content Distribution - Content Distribution is a new component of the Tachyon Platform that provides control and visibility on content deployments and delivery in an organization

Replaces ActiveEfficiency features, maintaining support during upgrade for legacy Nomad clients (versions earlier than Nomad 7.1 in 1E Client 5.2)

Nomad 7.1 clients now connect to Tachyon Response Stack components (Switch and Background Channel) which act as a proxy for Content Distribution, and legacy clients continue to connect directly to Content Distribution.

Nomad app - the user interface for Content Distribution, provides real-time visibility of what content is downloading or available in each location, subnet and client, see how much WAN traffic is being saved overall and each day

Delivery Optimization (DO) Visibility - visibility of Delivery Optimization downloads and content availability in each location, subnet and device

Delivery Optimization (DO) and Windows Update Agent (WUA) monitoring - track Windows download or Microsoft Endpoint Configuration Manager deployments on clients being downloaded via Delivery Optimization in real time, their peer to peer downloads efficiency, sources of the downloaded content and see this reported in the Nomad app dashboards

Overview page - gives a high-level view of the current status of content throughout the entire network

Content page - provides a Content-centric view of content distributed throughout your network

Task Sequences page - provides that visibility by grouping the reference content for each Task Sequence into a single view, so you can see which content is cached and which is not

Devices page - lists all Devices that have sent Nomad device registration events and have sent download events within a selected time period, links through to Device View

Nomad Sites page - shows how the network is being used for content distribution in different locations

Client Health page - shows information from two Integrated Product Packs provided with the Tachyon Platform.

9.6.17.5.4.2 Client

NomadBranch 7.1 client is the Nomad module in 1E Client 5.2

ActiveEfficiency features are now provided by Content Distribution on Tachyon Platform 5.2

Client status messages are sent via Tachyon event policy system - Content Distribution uses these instead of StatusMsgEvents using Configuration Manager

New client settings:

DeliveryOptimizationReportingEnabled - monitoring of Delivery Optimization downloads and reporting them to Content Distribution - disabled by default

SupportWPAD - provides support for Web Proxy Auto-Discovery Protocol (WPAD) - disabled by default.

9.6.17.5.4.3 Tools

ActiveEfficiency features are now provided by Content Distribution on Tachyon Platform 5.2.

9.6.17.5.5 Released in Nomad 7.0.200

Certificate-based client authentication . Nomad peers can now use client authentication certificates to authenticate peer-to-peer communications, as an alternative to the default Windows authentication using the local SMSNomadP2P& account that the Nomad service creates and manages. When you enable this option, Nomad will not create the local account and you no longer need to allow the local account to access the computer from the network. This feature is supported in the full OS, in Windows PE and for Peer Backup Assistant. This enables organizations to implement Nomad in conjunction with best practice security policies.

Configuration Manager Enhanced HTTP Support . Microsoft introduced Enhanced HTTP in CM1810 to allow organizations that struggled to manage PKI certificates to use secure communication between clients and DP without the need for PKI-generated certificates. Enhanced HTTP also allows administrators to remove the Network Access Account as it implements a new token-based authentication endpoint on DPs and MPs that do not require Windows authentication. Nomad is now able to communicate with this token-based endpoint and download content from a DP when Enhanced HTTP has been enabled. In this scenario the Network Access account can also be removed. Refer to the Microsoft Configuration Manager documentation for more details on Enhanced HTTP and the Network Access Account

Support for multiple Certificate Authorities . When configuring Nomad to use HTTPS when communicating with a DP or for P2P communication, the Nomad CertIssuer registry setting defines the issuing Certificate Authority (CA). Nomad now allows multiple CAs to be defined and also supports sub-string matching (for example, if you have ROOTCA1 and ROOTCA2, you can specify ROOTCA as the CertIssuer and Nomad will be able to use a certificate from either ROOTCA1 or ROOTCA2).

Improved PKI client certificate selection logic . When using HTTPS for communication with HTTPS CM Site Systems or P2P communication using PKI client certificates and the CM client is using PKI client certiicates, Nomad will use the same certificate that CM uses. If CM is using self-signed certificates (or is not present at all) then in most cases Nomad will be able to select an appropriate certificate from the local computer personal store without additional configuration.

VMWare Workspace One support. Nomad 7.0.200 includes updates that will enable VMWare Workspace One clients to download and share content using Nomad. This will be supported in an upcoming VMWare Workspace One release.

Improved handling of updated Software Updates . If the source for a Software Update is updated after it has been distributed to one or more clients, Nomad clients may get into a situation where they get into a loop downloading an invalid LsZ file from peers that have the older version of the content. Improvements have been made that can be enabled through the CompatibilityFlags.

Option to turn off or reduce election notifications in Nomad log. By default, Nomad logs all election responses when elections occur. In large subnets this can result in the logs filling up and rolling over. You can now turn off or limit the number of election responses that are logged.

1E Client telemetry for Nomad feature usage. To help 1E understand how customers are using and configuring our products, a telemetry feature has been implemented in Tachyon Platform 5.1. When the Tachyon Platform is implemented, the 1E Client sends telemetry data relating to enabled Nomad features to the Tachyon server. This data will be forwarded to 1E if you enable email and telemetry in Tachyon Setup. If telemetry is not enabled in the platform, the data can be manually exported and may be requested by 1E Support when troubleshooting issues.

The Nomad 7.0.100 maintenance release was implemented as the Nomad module in 1E Client 5.0. This release included rolled up hotfixes but did not introduce any new features.

The main Nomad 7.0 release contained the following features:

NomadBranch 7.0 client is the Nomad module in 1E Client 4.1 - refer to Installing and upgrading for more details on how to install/upgrade Nomad 7.0

Support for NomadBranchTools installation on remote SMS Providers - NomadBranchTools can now be installed on remote SMS Providers without the manual steps that were required previously.

Support for Windows 10 Express File Updates - 1E Client 4.1 supports download of express installation files deployed through Configuration Manager. To use this feature in Nomad, you must first configure Delivery Optimization Download Mode to 0 on all clients. For new installations, the feature is enabled by default and for upgrades it can be enabled in 1E Client 4.1 by setting bit 26 (0x4000000, 67108864 in decimal) of the **CompatibilityFlags** registry value.

Support for downloading content for CM Software Updates from Microsoft Update - if you deploy Software Updates, including regular updates, Windows 10 express updates and Office 365 updates with Configuration Manager and in the deployment settings select the option
If software updates are not available on distribution points in current, neighbor or site boundary groups, download content from Microsoft Updates, Nomad will be used to download that content from Microsoft Update if it is not available from a DP or local Nomad peers. (Please refer to **CompatibilityFlags** bits 27 and 28 for further details).

Enhancements:

SSD optimizations

Large Configuration Manager deployments and downloads to 30K or more machines could result in significant traffic spike from 1E Client to an ActiveEfficiency server that may result in IIS 503 Overload errors, this has been optimized.

When Local SSD is enabled to support networks where broadcasts are disabled, it is not used when a Nomad master detects broadcasts. This allows the same SSD setting to be used by all clients in a mixed network environment.

Improved resilience of content registration - a Content Registration Cycle mechanism has been introduced that registers the pending and failed content registrations with ActiveEfficiency.

Support for TLS 1.1/1.2 in environments where TLS 1.0 is disabled.

9.6.17.5.6 Summary

A list of the Tachyon features organized by the release they were implemented in. Links through to the features have been provided for convenience.

9.6.17.5.7 New features in Nomad 8.1

This release introduces the following new and enhanced features:

9.6.17.5.7.1 Platform

Insights on how Nomad enhances user experience - with the rapid shift to a Work From Anywhere (WFA) workforce and an increased focus on the Digital End-User eXperience, Nomad on Tachyon Platform now provides insights into how it helps to ensure a great user eXperience. With the introduction of Nomad's Bandwidth Protection Reporting, you can now see how Nomad is preventing end-user disruption due to software and update deployments. Bandwidth Protection Reporting will allow you to see the positive impact Nomad is having across the organization, to individual sites, subnets, all the way down to a single client.

Support for Cloud-based content in Task Sequences- cloud-based services to support Work From Anywhere (WFA) users are becoming more critical to the way enterprises work, there is an increased reliance on Cloud Distribution Points for distributing content.

Feature improvements - as Configuration Manager evolves and new features are released, Nomad on Tachyon Platform is being continuously maintained to ensure it works seamlessly with new releases.

Content Distribution service no longer uses SQL Linked Server to connect to Microsoft Endpoint Configuration Manager.

9.6.17.5.7.2 Client

NomadBranch 8.1 client is the Nomad module in 1E Client 8.1

Support for Cloud-based content in Task Sequences - cloud-based services to support Work From Anywhere (WFA) users are becoming more critical to the way enterprises work, there is an increased reliance on Cloud Distribution Points for distributing content.

Enhancements:

Improvements to the Certificate Selection criteria to authenticate with a DP (or any download source)

Download reporting now includes back-off data, for Bandwdith Protection Reporting.

9.6.17.5.7.3 Tools

Nomad AdminUI Console Extensions now require .NET Framework 4.8

Cloud infrastructure support

Enhancements:

Provide a way for SCCM Console users to use alternate credentials to authenticate with ContentDistribution/Platform

PlatformUrl validation is improved, by logging a warning during installation. In UI mode users have the option of continuing with the installation.

9.6.17.5.8 Released in Nomad 8.0

9.6.17.5.8.1 Platform

Works with Tachyon Platform 8.0

Integrating Nomad with WakeUp

Enhancements:

Task Sequence support for Windows feature updates

Automatic grooming of the Content Distribution database

Support for Windows Authentication between Background Channel and Content Distribution API

Tachyon Setup: Nomad screen has improved authentication options

Improving performance of the dashboards

API versioning using Tachyon SDK.

9.6.17.5.8.2 Client

NomadBranch 8.0 client is the Nomad module in 1E Client 8.0

New registry setting **SiteSSDMinPackageSizeKB**to set the minimum size of content before making SSD request

Installer changes:

Integrating Nomad with WakeUp

Enable **Nomad FanOut** as a default - default value of **SpecialNetShare**has changed to 0x2060 (8288)

Platform features enabled by using the BackgroundChannelUrl instead of PlatformURL

Enhancements to **CacheCleaner** functionality to better support remote users as part of the Working From Anywhere initiative.

9.6.17.5.8.3 Tools

A single combined installer called **Nomad Branch Tools** containing both OSD Tools and Nomad Configuration Manager console extensions.

9.6.17.5.9 Released in Nomad 7.1

9.6.17.5.9.1 Platform

Works with Tachyon Platform 5.2

Modernized backend infrastructure - Nomad requires a back-end server, which was previously the legacy ActiveEfficiency platform, this has been replaced by the Tachyon Platform to provide Single-Site download, Pre-caching and a new Dashboard. For customers moving to Modern Management, Nomad provides visibility and control of Delivery Optimization, which is used by Intune, MS store and MS update.

Leverage the Tachyon Platform and 1E Client - with the Tachyon Platform you can enable further features including Experience, User Sentiment, Guaranteed State and Patch Success, as well as opening up real-time management to any task by acquiring the appropriate license.

Content Distribution - Content Distribution is a new component of the Tachyon Platform that provides control and visibility on content deployments and delivery in an organization

Replaces ActiveEfficiency features, maintaining support during upgrade for legacy Nomad clients (versions earlier than Nomad 7.1 in 1E Client 5.2)

Nomad 7.1 clients now connect to Tachyon Response Stack components (Switch and Background Channel) which act as a proxy for Content Distribution, and legacy clients continue to connect directly to Content Distribution.

Nomad app - the user interface for Content Distribution, provides real-time visibility of what content is downloading or available in each location, subnet and client, see how much WAN traffic is being saved overall and each day

Delivery Optimization (DO) Visibility - visibility of Delivery Optimization downloads and content availability in each location, subnet and device

Delivery Optimization (DO) and Windows Update Agent (WUA) monitoring - track Windows download or Microsoft Endpoint Configuration Manager deployments on clients being downloaded via Delivery Optimization in real time, their peer to peer downloads efficiency, sources of the downloaded content and see this reported in the Nomad app dashboards

Overview page - gives a high-level view of the current status of content throughout the entire network

Content page - provides a Content-centric view of content distributed throughout your network

Task Sequences page - provides that visibility by grouping the reference content for each Task Sequence into a single view, so you can see which content is cached and which is not

Devices page - lists all Devices that have sent Nomad device registration events and have sent download events within a selected time period, links through to Device View

Nomad Sites page - shows how the network is being used for content distribution in different locations

Client Health page - shows information from two Integrated Product Packs provided with the Tachyon Platform.

9.6.17.5.9.2 Client

NomadBranch 7.1 client is the Nomad module in 1E Client 5.2

ActiveEfficiency features are now provided by Content Distribution on Tachyon Platform 5.2

Client status messages are sent via Tachyon event policy system - Content Distribution uses these instead of StatusMsgEvents using Configuration Manager

New client settings:

DeliveryOptimizationReportingEnabled - monitoring of Delivery Optimization downloads and reporting them to Content Distribution - disabled by default

SupportWPAD - provides support for Web Proxy Auto-Discovery Protocol (WPAD) - disabled by default.

9.6.17.5.9.3 Tools

ActiveEfficiency features are now provided by Content Distribution on Tachyon Platform 5.2.

9.6.17.5.10 Released in Nomad 7.0.200

Certificate-based client authentication . Nomad peers can now use client authentication certificates to authenticate peer-to-peer communications, as an alternative to the default Windows authentication using the local SMSNomadP2P& account that the Nomad service creates and manages. When you enable this option, Nomad will not create the local account and you no longer need to allow the local account to access the computer from the network. This feature is supported in the full OS, in Windows PE and for Peer Backup Assistant. This enables organizations to implement Nomad in conjunction with best practice security policies.

Configuration Manager Enhanced HTTP Support . Microsoft introduced Enhanced HTTP in CM1810 to allow organizations that struggled to manage PKI certificates to use secure communication between clients and DP without the need for PKI-generated certificates. Enhanced HTTP also allows administrators to remove the Network Access Account as it implements a new token-based authentication endpoint on DPs and MPs that do not require Windows authentication. Nomad is now able to communicate with this token-based endpoint and download content from a DP when Enhanced HTTP has been enabled. In this scenario the Network Access account can also be removed. Refer to the Microsoft Configuration Manager documentation for more details on Enhanced HTTP and the Network Access Account

Support for multiple Certificate Authorities . When configuring Nomad to use HTTPS when communicating with a DP or for P2P communication, the Nomad CertIssuer registry setting defines the issuing Certificate Authority (CA). Nomad now allows multiple CAs to be defined and also supports sub-string matching (for example, if you have ROOTCA1 and ROOTCA2, you can specify ROOTCA as the CertIssuer and Nomad will be able to use a certificate from either ROOTCA1 or ROOTCA2).

Improved PKI client certificate selection logic . When using HTTPS for communication with HTTPS CM Site Systems or P2P communication using PKI client certificates and the CM client is using PKI client certiicates, Nomad will use the same certificate that CM uses. If CM is using self-signed certificates (or is not present at all) then in most cases Nomad will be able to select an appropriate certificate from the local computer personal store without additional configuration.

VMWare Workspace One support. Nomad 7.0.200 includes updates that will enable VMWare Workspace One clients to download and share content using Nomad. This will be supported in an upcoming VMWare Workspace One release.

Improved handling of updated Software Updates . If the source for a Software Update is updated after it has been distributed to one or more clients, Nomad clients may get into a situation where they get into a loop downloading an invalid LsZ file from peers that have the older version of the content. Improvements have been made that can be enabled through the CompatibilityFlags.

Option to turn off or reduce election notifications in Nomad log. By default, Nomad logs all election responses when elections occur. In large subnets this can result in the logs filling up and rolling over. You can now turn off or limit the number of election responses that are logged.

1E Client telemetry for Nomad feature usage. To help 1E understand how customers are using and configuring our products, a telemetry feature has been implemented in Tachyon Platform 5.1. When the Tachyon Platform is implemented, the 1E Client sends telemetry data relating to enabled Nomad features to the Tachyon server. This data will be forwarded to 1E if you enable email and telemetry in Tachyon Setup. If telemetry is not

enabled in the platform, the data can be manually exported and may be requested by 1E Support when troubleshooting issues.

The Nomad 7.0.100 maintenance release was implemented as the Nomad module in 1E Client 5.0. This release included rolled up hotfixes but did not introduce any new features.

The main Nomad 7.0 release contained the following features:

NomadBranch 7.0 client is the Nomad module in 1E Client 4.1 - refer to Installing and upgrading for more details on how to install/upgrade Nomad 7.0

Support for NomadBranchTools installation on remote SMS Providers - NomadBranchTools can now be installed on remote SMS Providers without the manual steps that were required previously.

Support for Windows 10 Express File Updates - 1E Client 4.1 supports download of express installation files deployed through Configuration Manager. To use this feature in Nomad, you must first configure Delivery Optimization Download Mode to 0 on all clients. For new installations, the feature is enabled by default and for upgrades it can be enabled in 1E Client 4.1 by setting bit 26 (0x4000000, 67108864 in decimal) of the **CompatibilityFlags** registry value.

Support for downloading content for CM Software Updates from Microsoft Update - if you deploy Software Updates, including regular updates, Windows 10 express updates and Office 365 updates with Configuration Manager and in the deployment settings select the option **If software updates are not available on distribution points in current, neighbor or site boundary groups, download content from Microsoft Updates**, Nomad will be used to download that content from Microsoft Update if it is not available from a DP or local Nomad peers. (Please refer to **CompatibilityFlags** bits 27 and 28 for further details).

Enhancements:

SSD optimizations

Large Configuration Manager deployments and downloads to 30K or more machines could result in significant traffic spike from 1E Client to an ActiveEfficiency server that may result in IIS 503 Overload errors, this has been optimized.

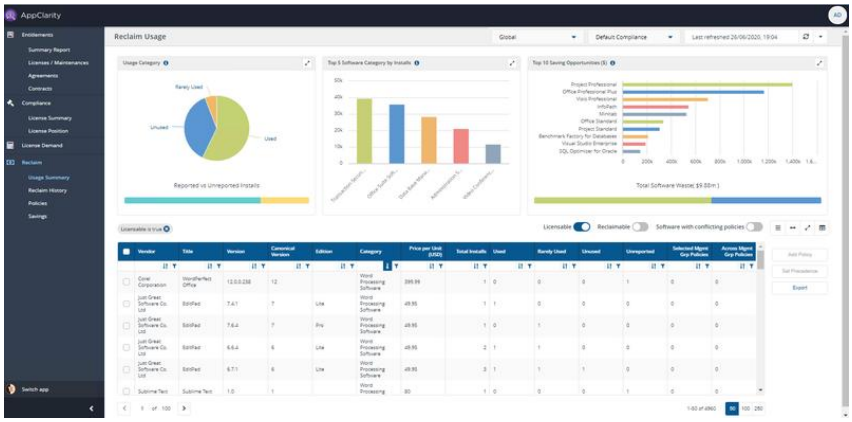
When Local SSD is enabled to support networks where broadcasts are disabled, it is not used when a Nomad master detects broadcasts. This allows the same SSD setting to be used by all clients in a mixed network environment.

Improved resilience of content registration - a Content Registration Cycle mechanism has been introduced that registers the pending and failed content registrations with ActiveEfficiency.

Support for TLS 1.1/1.2 in environments where TLS 1.0 is disabled.

10 AppClarity

AppClarity is aimed at Software Asset Management (SAM) users, helping you get to grips with software waste, take control of license compliance and manage application portfolios easily. It offers an immediate reduction in software costs by helping you manage your software assets on desktops more effectively and maintain software license compliance.



10.1Introducing AppClarity

An overview of AppClarity, what it does, and how it can benefit your organization. An introduction to the features of AppClarity is provided, alongside a high-level explanation of the AppClarity architecture.

AppClarity is a Tachyon application aimed at Software Asset Management (SAM) users, helping you get to grips with software waste, take control of license compliance, and manage application portfolios easily. It offers an immediate reduction in software costs by helping you manage your software assets on desktops more effectively and maintain software license compliance.

The main benefits of using AppClarity are:

Software license compliance – provides a summary of whether a particular product is license compliant or not

Efficient management of entitlements and agreements for an organization

Software waste identification – shows unused or rarely used software which is probably the two largest forms of software waste and enables to reclaim

License Demand based on different metrics for vendors

Efficient application management – identifies version sprawl where many versions of the same product are in use.

Now, you can financially quantify all software waste by identifying and controlling unused software across your enterprise and improving your compliance status.

10.1.1 AppClarity Features

An overview of AppClarity features.

10.1.1.1 New features

Works with Tachyon 8.1

No features or feature changes added in this release, but includes any hotfixes from previous versions.

10.1.2 AppClarity Architecture

The AppClarity architecture is identical to the Tachyon platform architecture, please refer to Tachyon Architecture.

Please refer to Design considerations for a simpler description, with design considerations for AppClarity.

10.2Implementing AppClarity

Everything you need to know about getting AppClarity installed and running in your network. This section is structured in a way that leads you through a typical implementation project.

10.2.1 Design considerations

Information that will help you design and plan the implementation of AppClarity in your organization.

This page is part of the design phase of implementation.

10.2.1.1 Architecture

The picture opposite shows the AppClarity consumer application installed on a Tachyon server, along with other applications that are installed using Tachyon Setup.

If you have an older version of Tachyon, or SLA Platform, then you will need to upgrade it to Tachyon 5.1 to install AppClarity. For more information on installing and upgrading, please refer to Installation scenarios below.

10.2.1.1.1 Software Reclaimer

The Software Reclaimer is an optional feature. It's an executable run on Windows clients responsible for implementing reclaim policies provided by AppClarity. For more information, please refer to Deploying Software Reclaimer.

If you intend to use Software Reclaimer, then consider whether you will use HTTP or HTTPS, and which port.

A default installation of Tachyon uses standard ports HTTP 80 and HTTPS 443. You may wish to use a different port for Software Reclaimer, for example, if you previously used:

HTTP 8335 or HTTPS 8336 with AppClarity 5.2

HTTP 8080 or HTTPS 8443 with SLA Platform 3.3 and AppClarity 6.1

You can manually add a website binding after installation of Tachyon. You may already be using a non-standard port if specified in Tachyon Setup during its installation, or you manually added a binding after installation for another application like Application Migration, or ActiveEfficiency.

If you intend on using Software Reclaimer with HTTPS then the following applies to the Tachyon website's SSL certificate:

It must be trusted by clients running the Software Reclaimer. This is also the same requirement for Tachyon clients. Please refer to Client authentication certificates

Its public key must be encoded in each of the Software Reclaimer XML file(s) as described in Deploying Software Reclaimer.

10.2.1.1.2 AI Powered Auto-curation

Using the AI Powered Auto-curation feature, you'll be able to increase the total amount of normalized software in your Inventory repositories. This is done using AI that integrates with the inventory consolidation process. By using AI, your organization will benefit from significant numbers of normalized software and a reduced manual effort needed to normalize software.

You can enable AI Powered Auto-curation either when you install Tachyon or post installation. Refer to AI Powered Auto-curation to find out how you can do this.

10.2.1.2 Installation scenarios

For all installation scenarios you require:

A valid licensed installation of Tachyon

The license must include AppClarity and Inventory.

10.2.1.2.1 New installation

> **Note**
>
> AppClarity is included with Tachyon, so you'll need to use the Tachyon setup wizard to install AppClarity. To activate AppClarity you'll need a valid license file.
>
> 1E will provide you with a **Tachyon.lic** license file that defines the products and features your Tachyon System is able to use, for how long, and how many devices it supports, this may be an evaluation or subscription license.

The license must be activated. Once activated, it may be used only by the Tachyon System that activated it.

Licenses can be renewed or updated, but if allowed to expire, then the affected products or features will not be usable.

For a new installation, the Tachyon Setup program will let you select the license file from any folder on disk.

For an existing installation, the license file is copied into the folder: %PROGRAMDATA%\1E\Licensing on your Tachyon Server.

> For details of what the license file needs to contain, please refer to License requirements for consumer applications.
>
> Before installing Tachyon, please refer to Planning for Tachyon, this includes details of server sizing. The addition of AppClarity does not affect sizing, as it is included with Tachyon.

10.2.1.2.2 Existing Tachyon installation

You may already have Tachyon installed, perhaps with the Application Migration consumer application installed to support 1E Windows Servicing Suite (WSS).

You can install AppClarity as a local consumer application on your existing Tachyon web server if it is Tachyon 5.1 or later.

Please refer to Upgrading to Tachyon Platform.

10.2.1.2.3 Existing SLA Platform installation

You may still have a legacy SLA Platform installation, perhaps with Application Migration to support 1E Windows Servicing Suite (WSS), or AppClarity 6.1.

You can upgrade SLA Platform to Tachyon 5.1 and then upgrade that to 1E 8.1. Please refer to Upgrading to Tachyon Platform.

> **Tip**
>
> If you only require the Inventory features of Tachyon, and do not require its Real-time features, then you do not need a Response Stack, and you can choose the Tachyon Master Stack configuration inTachyon Setup.

10.2.1.3 Migrating from AppClarity 5.x

There is no upgrade path to AppClarity 8.1 from AppClarity 5.x.

If you have AppClarity 5.x, the simplest scenario is to install Tachyon platform and AppClarity on a separate server. Before installation, you should consider taking a copy of your existing Catalog database and using that for the new Tachyon platform installation. You will then have two installations of 1E Catalog, and you will have to maintain both site-defined Catalog entries separately until you decommission AppClarity 5.x.

You can install Tachyon platform and AppClarity on the same server as an existing AppClarity 5.x installation, provided the hardware specification is suitable. Both installations can share the same 1E Catalog, provided AppClarity 5.x is already using 1E Catalog 2.0 or later. You can have separate Catalog installations if you want, but sharing the same Catalog ensures your site-defined Catalog entries are accessible to both systems.

In either scenario, after installation, you can optionally migrate certain entitlements from AppClarity 5.2 to AppClarity using the AppClarity v5.2 connector.

10.2.1.4 Comparison of AppClarity 5.2 and AppClarity 6.1 features

The following differences are not definitive or exhaustive. Later versions of AppClarity have additional features not included in AppClarity 6.1.

Area	Feature	New feature in 6.1	Comparison with 5.2
Entitlement	Types	SKU, defined in Catalog, auto-populates product details and rights. Contracts	Entitlement storage is compliant with ISO 19770-3. AppClarity 5.x was first tool on market using this standard developed by 1E. 6.1 console does not have renewals reminder. Renewal Date column appears as End Date in 6.1.

Area	Feature	New feature in 6.1	Comparison with 5.2
		can be linked to agreements and link back to licenses soft copies can be uploaded and attached	The table below explains differences between entitlement entry screens.

Category name in 5.2	5.2	6.1
Entitlement types	The **New Entitlement** screen allows you to select the type of entitlement: License Maintenance Evaluation Other You can also select if it is a renewal, upgrade or consolidation, and link to an existing entitlement.	Entitlement type must be selected first: License Maintenance Agreement Contract (the selector provides this option, but Contract is not actually an entitlement type) More options for linking.
Version, edition, upgrade, downgrade, and persistent	Default settings for upgrade, downgrade, and	

Area	Feature	New feature in 6.1	Comparison with 5.2		
			rights apply only to Maintenance entitlements. Only one can be selected.	persistent rights depend on type of entitlement, and now specified in **Rights** category.	
			Product	Edition must be selected before version.	Version must be selected before edition.
				One or more editions can be selected from the Catalog.	Only one edition can be selected, depending on version. Product name is now renamed Title.
			All versions	All versions	
			< , <= , = , => , >	Specific version, with optional trailing wildcard	
			N/A		
			If the entitlement is for a bundle, you need to select the	The Catalog determines if a product	

Area	Feature	New feature in 6.1	Comparison with 5.2		
			bundle option, and then identify other bundle products.	is part of a bundle. SKU, defined in Catalog, auto-populates product details and rights New options in 6.1: Software Assurance (as an Entitlement modifier)	
			Quantity & Metrics	Supported metric types: Device User Resource (CPU, RAM, Disk, etc.) Other The following exist only in 5.2: Metric Name (imported	**Metrics** is now part of new sub-category **Summary**. Supported metric types: Device Processor Core Processor Value Unit (PVU) Other

Area	Feature	New feature in 6.1	Comparison with 5.2		
				as **Metric Other** only if **Metric Type** is Other) Metric Description	
			Rights & Limitations	The following exist onlyin 5.2: Limitations (OS, hostname, country, language, etc.)	Category renamed as **Rights**. New in 6.1: Secondary use More flexibility regarding rights - see above.
			Cost & Order	Frequency: Perpetual Monthly Yearly	Category renamed as **Costs**. Frequency: OnceOff Monthly Quarterly Yearly
			Invoice sub-category.	Sub-category moved to **Additional i**	

Area	Feature	New feature in 6.1	Comparison with 5.2	
				nformation.
			Purchase Order sub-category.	Sub-category moved to **Additional information**.
			Direct Supplier Purchase Order sub-category.	Sub-category renamed as **Direct Supplier** and moved to **Additional information**.
			Internal order sub-category.	Sub-category moved to **Additional information**. Also includes Line item number.
			Licensor sub-category.	Sub-category renamed as **Licensor details** and moved to **Additional i**

Area	Feature	New feature in 6.1	Comparison with 5.2		
				nformation. Also includes Line item number.	
			Product Details	Separate category only in 5.2. The following exist only in 5.2: Entitlement Key Channel Type Product Family Registration Key Persistent ID	Category no longer exists. **SKU** is now part of **Product**. **FOSS details** is now a separate sub-category under **Additional information**. New in 6.1: FOSS trademark
			Audit & Exclusions	The following exist onlyin 5.2 Audit penalty	Category exists with same name.
			Internal Details	Sub-category	**Internal Details** is a new sub-

Area	Feature	New feature in 6.1	Comparison with 5.2		
				doesn't exist in 5.2. You must choose the management group before creating an entitlement. An entitlement can belong to only one management group.	category of **Additional information**, with options: Management group Business Unit Sponsor
Import	Staged bulk upload as drafts for verification in the console, and then published.	6.1's Entitlement .tsv connector (file upload of TSV) uses different headings to 5.2 6.1 does not have: The entitlements ISO utility (XML export) importing of XML			
License Demand Calculation	LDC	LDCs for the following complex metrics: IBM Processor Value Unit (PVU)			

Area	Feature	New feature in 6.1	Comparison with 5.2	
		Microsoft Core - only for SQL Server currently Oracle Processor		
Compliance	Compliance	Create separate compliance repositories for separate environments by linking them to a unique set of Inventory and Entitlement repositories Server-based software licensing and compliance Complex license metric covered such as core/processor Effective license position summary table Entitlement usage summary table License optimization	6.1 does not use XPS for reports; XPS Viewer is no longer a requirement. The following is a list of XPS reports available in 5.2 and similar in 6.1. Some of these reports are not related to Compliance but included here for completeness. Also see other reports in Introducing Inventory.	
			Adobe Acrobat	Viewing software install counts across all devices
			Compliance Risk Report	Running your first Compliance License Summary
			Product Installation	Viewing software install counts across all devices
			Product Reclaimer	Viewing the software reclaim reports
			Product Suite Optimization	Not available in 6.1

Area	Feature	New feature in 6.1	Comparison with 5.2	
			Shelfware Identification	Viewing your effective license position
			Software Reclaim Savings	Viewing the software reclaim reports
			Specific Device	Viewing product usage and Viewing the software reclaim reports
			System Diagnostics	SLA report: Basic Summary report
			Unused Software Identification	Viewing product usage
			Vendor Compliance	Viewing your effective license position
			VMware Optimization	Not available in 6.1
Currency		Default currency is configurable in the database.		

Area	Feature	New feature in 6.1	Comparison with 5.2
		Currency exchange rates, and consolidation into a single currency is not used.	
Reclaim	Policies	A single policy can support multiple editions and versions. Multiple editions can be selected. Versions support wildcards. For example, Microsoft Visio 8.* to create a policy for Visio with major version 8. Each VTVE in the 1E Catalog can then have its own custom command line. 6.1 allows reclaim policies to be created for products that are not yet inventoried, provided they exist in the 1E Catalog. A reclaim policy can be applied globally or to one or more management groups. Any machine can only have one policy applied for a product, therefore AppClarity warns you if there are similar	Usage is calculated slightly differently, so you will see different numbers in AppClarity 5.2 and 6.1. See Usage categories. The following reclaim features are not available in 6.1: multiple custom command lines (only a single command is possible) - **fixed in 7.0 hotfix** integration scripts custom SCCM Uninstall - **added in 7.0** changing the 7/30/90 day Usage categories (in 5.2 these were configurable in the database) reclaim on server OS (only Windows workstations are supported) Big red button: The 'disable integration services' option in 5.2 is replaced by a Reclaimer provider on/off button in 6.1. 6.1 version of the pre-flight (evaluate) report does not have summary details.

Area	Feature	New feature in 6.1	Comparison with 5.2
		policies and lets you set a **precedence** for which policy to apply.	
Software Reclaimer		Software Reclaimer executable, its settings, and its API are the same as before. Only the base URL is changed, which means new deployments are required. In 6.1, the Software Reclaimer and API are installed as part of the SLA Platform; policies are managed by the AppClarity consumer application.	
SLA Platform	Console	New web based UI instead of the old click-to-run Console. AppClarity 6.x is a consumer application, installed on the SLA Platform web server. This is why you sometimes see the name AppClarity Web.	
Catalog	SLA Platform console	For 6.1, SLA Platform connects directly to the 1E Catalog, allowing you to create site-defined	

Area	Feature	New feature in 6.1	Comparison with 5.2
	allows for bulk export of Catalog entries from the Console into a macro-enabled Excel spreadsheet, and using macros to import via theSLA Platform API.	entries via either the SLA Platform console, or Catalog console. For 5.2, AppClarity connects directly to the 1E Catalog. Site-defined entries are created in the Catalog console. BDNA integration is not included in 6.1.	
Connectors to data sources	AppClarity uses SLA Platform connectors to get invent	AppClarity 6.x does not require ActiveEfficiency. ActiveEfficiency and its Scout are replaced by SLA Platform and its connectors.	

Area	Feature	New feature in 6.1	Comparison with 5.2
	ory and usage data from various data sources, including Tachyon, and third party sources such as SCCM, BigFix, ServiceNow, vCenter, as well as general SQL queries to SQL Server and Oracle, and file uploads. The above	AppV and iQSonar not supported in 6.1.	

Area	Feature	New feature in 6.1	Comparison with 5.2
	connectors are provided by SLA Platform, AppClarity provides additional connectors for importing entitlements. See Connectors page.		
Management groups	More flexible. AppClarity now supports devices in multiple management groups	Management groups operate differently. In 5.x devices can be a member of only one management group according to precedence rules. In 6.x devices can be a member of multiple management groups.	

Area	Feature	New feature in 6.1		Comparison with 5.2
	, including global, and uses precedence to decide which reclaim policy should be used if a device is a member of different management groups with similar policies. Management groups are configured in SLA Platfor	Inventory	5.2	6.1
		Machine (Device)	name OU name domain name	same as 5.2 in 6.1.0 multiple new rules in 6.1.100
		Application (Product)	publisher (vendor) name (title)	multiple new rules in 6.1.100
		Tag	tag name + value	n/a
		In 6.1, Entitlement is assigned to a management group in the Additional		

Area	Feature	New feature in 6.1	Comparison with 5.2
	m using rules. There are rules for device hardware, Active Directory, processor and product.	information section, but this is not used in any built-in reports, but can be used in custom BI reports for example.	
Access control		SLA Platform supports only users, not AD security groups. SLA Platform does not have role-based access control (RBAC), therefore all SLA Platform users are able to access all platform and consumer features, including AppClarity.	
Email		No emails, therefore administrative alerts not sent by email.	
Installation license key		Single license for AppClarity covering all features;	

Area	Feature	New feature in 6.1	Comparison with 5.2
		previously Desktop, Server and Reclaim were separate licenses.	
Repositories	Admins can create multiple repositories for Inventory, Entitlement and Compliance, to allow opportunities for tasks like testing and audit projects.	Although not the same, 6.1 has Entitlement repositories, and 5.2 has Entitlement libraries.	
Business Intelligence	BI Dashboard	BI 2.0 for 6.1 is an SLA Platform consumer application, and does not require any third party product, other than SQL Server	BI 1.0 for AppClarity 5.2 (Dundas) has the following dashboards: Estate overview (tiles listed in **bold** are also visible in this overview) Device Listing (by OS, Form Factor, listing)

Area	Feature	New feature in 6.1	Comparison with 5.2
		Analysis Server (SSAS).	Software (by OS, **usage**, end of support date, **top vendors**)
		Overview	Entitlements (by **value**, management group, type, **upcoming renewals**, maintenance)
		Top 5 compliance risk	Reclaim (**savings**, status, history, operations)
		Top 5 optimization opportunity	Compliance (**risks/gaps**, list)
		Top 5 reclaims opportunity	
		Upcoming renewals	
		Usage	
		Entitlements	
		Virtualization technology	
		Software	
		installation count	
		compliance	
		usage	
		entitelments	
		management groups	
		OS	
		Device types	

10.2.2 Requirements

Please refer to Supported Platforms a list of all the platforms supported by AppClarity and the software required to allow you to install AppClarity successfully.

10.2.3 Preparation

What you will need to prepare in advance of implementing AppClarity in your network. Typically, these are tasks that may take some time, depending on how your organization works.

10.2.3.1 Installation order

Note

AppClarity is included with Tachyon, so you'll need to use the Tachyon setup wizard to install AppClarity. To activate AppClarity you'll need a valid license file.

1E will provide you with a **Tachyon.lic** license file that defines the products and features your Tachyon System is able to use, for how long, and how many devices it supports, this may be an evaluation or subscription license.

The license must be activated. Once activated, it may be used only by the Tachyon System that activated it.

Licenses can be renewed or updated, but if allowed to expire, then the affected products or features will not be usable.

For a new installation, the Tachyon Setup program will let you select the license file from any folder on disk.

For an existing installation, the license file is copied into the folder: %PROGRAMDATA%\1E\Licensing on your Tachyon Server.

For details of what the license file needs to contain, please refer to License requirements for consumer applications.

Before installing Tachyon, please refer to Planning for Tachyon, this includes details of server sizing. The addition of AppClarity does not affect sizing, as it is included with Tachyon.

10.2.3.2 SQL Server

Installation and upgrade requires that the Tachyon service account, which is set to the Network Service account, has an SQL Login with certain permissions:

10.2.3.2.1 SQL Login for the Network Service account

The SQL Login that is used by the Tachyon Server web applications and services depends on whether the SQL Server is remote from the Tachyon Server or is local, as described in the following table:

Installation scenario	Service account SQL Login
Tachyon Server is remote from SQL	The computer account of the remote Tachyon Server. For example **ACME\ACME-TCN01$**

Installation scenario	Service account SQL Login
Tachyon Server and SQL are local	The local network service account, **NT AUTHORITY\NETWORK SERVICE**

Note

Before upgrading Tachyon, or installing or upgrading Consumer applications like Application Migration or AppClarity, the SQL Login must be granted the following rights to support Database Snapshot of the 1E Catalog and SLA databases, to restore them if an error occurs:

dbcreator rights on the SQL database instance hosting the 1E Catalog database.

dbcreator rights on the SQL database instance hosting the SLA databases.

During installation, the Tachyon Setup will **always**:

Attempt to create the SQL Login

Grant it **db_owner** permission on each of the Tachyon databases

Remove the **db_owner** permissions when installation is completed.

10.2.3.3 Accounts needed to install AppClarity

10.2.3.3.1 Tachyon Server Installation Account

The server installation account has the following requirements on the server.

Local admin rights on the Tachyon Server. It must be an Directory domain user account that is a direct or indirect member of the Administrators local group on the server where Tachyon Server will be installed.

Can be disabled (not deleted) in Directory after additional Tachyon admin users have been created in Tachyon, and installation has been verified.

In addition, the server installation account requires SQL rights as described in SQL Server and SSAS Databases.

The server installation account is granted the following permissions as a Tachyon user, configured during installation of the Tachyon Server.

It is the first Tachyon user account and is a **System Principal**, which means it cannot be deleted or assigned any other rights

It is assigned to the Tachyon system role of Installer

It should be used to add additional Tachyon users and administrators, assign them to Tachyon roles, which should then be used for ongoing use and management of Tachyon.

It may be included in any AD security group assigned to a Tachyon system or custom role.

Refer to Roles and Securables for a complete reference of Tachyon system roles, custom roles, securables and operations.

> **Note**
>
> For a new installation of Tachyon, the only account that exists in Tachyon will be the **installation account**, which by default is assigned to the Tachyon roles listed above. You will need to add users and assign roles to them.
>
> When upgrading from SLA Platform, SLA users are migrated to Tachyon, but are not assigned to any roles. You will need to assign users to appropriate roles in Tachyon.
>
> For steps on viewing existing users and adding a new user in Tachyon please refer to Users and Groups page.
>
> **Warning**
>
> When installing Tachyon or upgrading from SLA Platform, do not install Tachyon using an **installation account** that you also intend for using and administrating Tachyon and AppClarity. The Tachyon **installation account** is purposefully given limited capabilities which can't be easily edited later.

10.2.4 Installing and upgrading

How to install AppClarity in your organization.

10.2.4.1 Installing AppClarity

AppClarity is installed through Tachyon setup. The **Select Configuration** section of setup allows you to choose whether to install AppClarity.

For full details of how to setup Tachyon, please refer to Tachyon Setup.

10.2.4.2 Upgrading AppClarity

Guidance for upgrading AppClarity.

10.2.4.2.1 Supported upgrade paths

AppClarity 8.1 can be upgraded directly from AppClarity 6.1.100 or from AppClarity 7.0.0.

Supported upgrade paths for AppClarity.

Source (Existing setup)	Destination (Upgrading to)		
1E Catalog	1.2.0	1E Catalog*	2.1.0
SLA Platform	3.3.0 (with Hotfixes)	SLA Platform*	5.1.0
AppClarity	**6.1.100**	Tachyon Server*	5.1.0

Source (Existing setup)	Destination (Upgrading to)
AppClarity*	**7.1.0**

Source (Existing setup)	Destination (Upgrading to)		
1E Catalog	1.2.100	1E Catalog*	2.1.0
SLA Platform	3.3.100 (with Hotfixes)	SLA Platform*	5.1.0
AppClarity	**6.1.100**	Tachyon Server*	5.1.0
AppClarity*	**7.1.0**		

Source (Existing setup)	Destination (Upgrading to)		
1E Catalog*	2.0.0	1E Catalog*	2.1.0
Tachyon Server*	5.0.0	SLA Platform*	5.1.0
SLA Platform*	5.0.0 (with HotFixes)	Tachyon Server*	5.1.0
AppClarity	**7.0.0**	AppClarity*	**7.1.0**

Note

*The AppClarity, 1E Catalog, SLA Platform and Tachyon Server installers are bundled together and are installed using a single installation process. They do not need to be installed separately.

10.2.4.2.2 Upgrading AppClarity 6.1.100 to AppClarity 7.1.0

Note

Before upgrading AppClarity, refer to Tachyon Setup and Installing AppClarity for full installation instructions.

To upgrade from AppClarity 6.1.100 to AppClarity 7.1.0 follow these steps:

Run Tachyon Setup to upgrade to AppClarity 8.1

Once the upgrade has completed, execute the attached post upgrade database script (see Running the post upgrade database script section below) for data cleansing and correction as a part of your post upgrade activity.Ensure this script is successfully executed.

To include the latest data, run an Inventory sync (a Basic Inventory Consolidation refresh is enough). Then, refresh the following reports in the same order:

LDC reports for - Microsoft Core LDC, Oracle Processor LDC, IBM Processor Value Unit (PVU) LDC, Red Hat Socket LDC

Entitlement Consolidation report

Compliance report

Reclaim Consolidation report

Reclaim Reporting report.

10.2.4.2.2.1 Running the post upgrade database script

Download the AppC_v7.1.0_Post_Upgrade_ProviderOperation.zip

When the script is run, it performs a retention of:

Policy data (which are in process under Policy Admin section)

Policy historical data and their correct status.

If you do not run the script, there is an expectation that:

Reclaim is setup in AppClarity 6.1.100 with some reclaimable policies

Some reclaim policies have already resulted in successful reclaims

Few reclaims are in process (i.e. needs administrator action by accepting or rejecting their opt-out requests)

Reclaim History displays for some reclaim transactions.

After a successful upgrade to AppClarity 8.1, if the **Post_Upgrade_ProviderOperation** script is not run, then:

In transit reclaims (i.e. which are to be accepted or rejected by an administrator), will be lost or unstable behavior may observe

History status of reclaim transactions, which had been opt-out, would be spoiled and may display an incorrect status.

> **Note**
>
> If reclaim is notcorrectlyconfigured or simply not being used (as in, no reclaimable policy exists or is published), and the post upgrade database script is run there should be no observable errors, but there may be some unwanted behavior in the application.
>
> **Warning**

We do not recommend running the post upgrade database script if reclaim is not correctly configured or simply not being used.

10.2.4.2.3 Upgrading AppClarity 7.0.0 to AppClarity 8.1.0

Note

Before upgrading AppClarity, refer to Tachyon Setup and Installing AppClarity for full installation instructions.

To upgrade from AppClarity 7.0 to AppClarity 8.1 follow these steps:

Refer to Planning for Tachyon and Upgrading Tachyon Platform, then run Tachyon Setup to upgrade to AppClarity 8.1

Once the upgrade has been completed, the system is ready for use.

Refresh the following reports in the same order:

License Demand Consolidation reports for - Microsoft Core License Demand, Oracle Processor License Demand, IBM Processor Value Unit (PVU) License Demand, Red Hat Socket Demand.

Entitlement Consolidation report.

Compliance report.

Reclaim Consolidation report.

Reclaim Reporting.

Note

When you upgrade from AppClarity 7.0 to AppClarity 8.1,you do not need to run the **Post_Upgrade_ProviderOperation** database script.

Please refer to Design Considerations regarding migration from AppClarity 5.x and the co-existence of AppClarity 5.x and AppClarity 8.1.

10.2.5 Verifying

Verification of AppClarity after installation.

10.2.5.1 Verifying the AppClarity installation

AppClarity is a consumer of Tachyon. When it's installed, all its components will be added to the Tachyon portal.

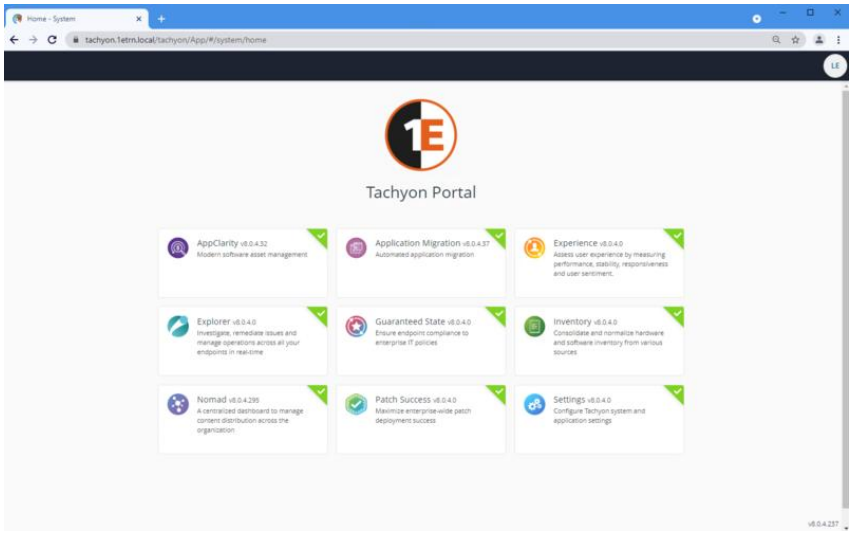
The Tachyon Portal website will be available after installation using the Tachyon DNS Alias FQDN. For example:

Note

https://tachyon.1etrn.local/Tachyon

After installation, log on to Tachyon using the Tachyon installation account

Once you've entered the site, a list of Tachyon applications are displayed, to confirm that **AppClarity**is present.



10.2.5.2 Accessing AppClarity

The Tachyon installation account is restricted by default to a minimum set of permissions required to bootstrap other users into the system but not access any of the applications other than **Settings**.

If you used the Tachyon installation account to install AppClarity or you followed the instructions for setting the Tachyon roles for the AppClarity installation account - please refer to Accounts needed to install AppClarity for more details.

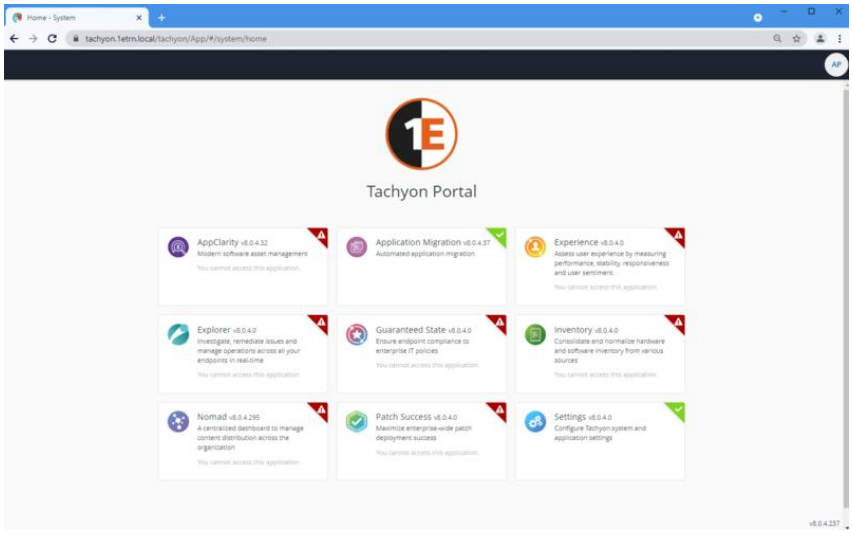
Initially, you will not be able to access AppClarity as you require a Tachyon account with permissions to view the application. If you click on AppClarity on the list of applications displayed on first entering the portal, you will see a screen similar to the one shown.

Note

AppClarity now comes with a number of roles that can be applied to Tachyon users. Refer to Tachyon roles for configuring AppClarity and AppClarity user roles for details.

Tip

You can view which applications are installed and manage them using the **Maintenance** screen in the Tachyon installer. Refer to Maintenance for details.



10.2.5.3 Adding the AppClarity Administrator role to a user to verify AppClarity installation

To verify AppClarity installed successfully, you will need to add the appropriate permissions to a Tachyon account. You'll first need to add an existing AD domain user to Tachyon.

10.2.5.3.1 Adding Tachyon users

Log on to the Tachyon portal using a Tachyon user account with the **Full Administrator**, or the **Installer** role if it is a new Tachyon installation.

Navigate to the **Settings**→**Permissions**→**Users and Groups** page.

Click on the **Add** button, doing this displays the **Add user** popup.

In the **Select AD user or security group** field, type the name, or part of the name, for the Active Directory user or security group that you want to add, then click the search icon.

Select the Active Directory user or security group from the list of matching names displayed in the drop-down list and click **Add**.

You can now apply the **AppClarity Administrator** role to the user you've just added.

10.2.5.3.2 Adding Tachyon roles to users or groups

Once added to Tachyon, you can use **Assignments** to edit the roles for a Tachyon user or group:

On the **Settings**→**Permissions**→**Users and Groups** page, click on the **Assignments** link for the user or group you want to add the role to, this displays the Assignments page focused on the selected user.

On the Assignments page, the focus is on **Users and Groups**.

Click the plus sign button to add a **Role** and your choice of associated **Management Group**.

Once you've selected your Tachyon Roles and Management Groups, click the **Save** button.

For details about how Assignments in Tachyon refer to Assignments page.

The **Assignments** page lets you view and manage current assignments for Tachyon roles, management groups, users and groups, from this page you can:

View all current assignments

Add new assignments

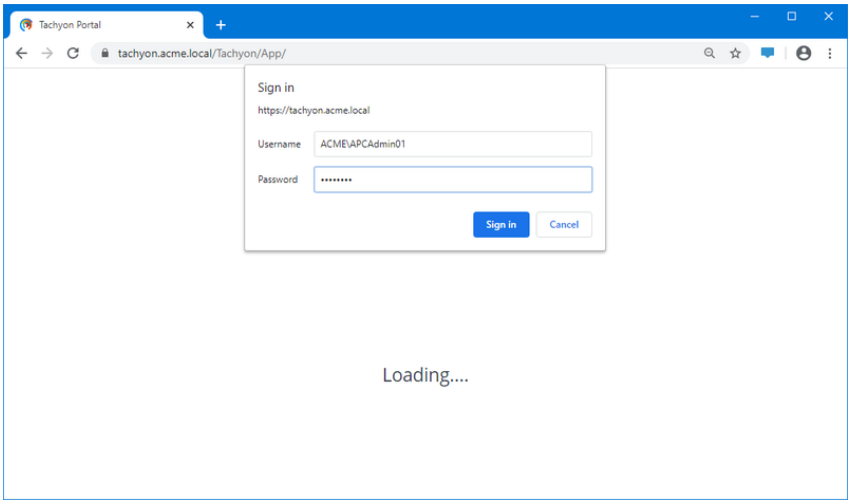
Remove current assignments.

10.2.5.4 Verifying AppClarity in the Tachyon portal

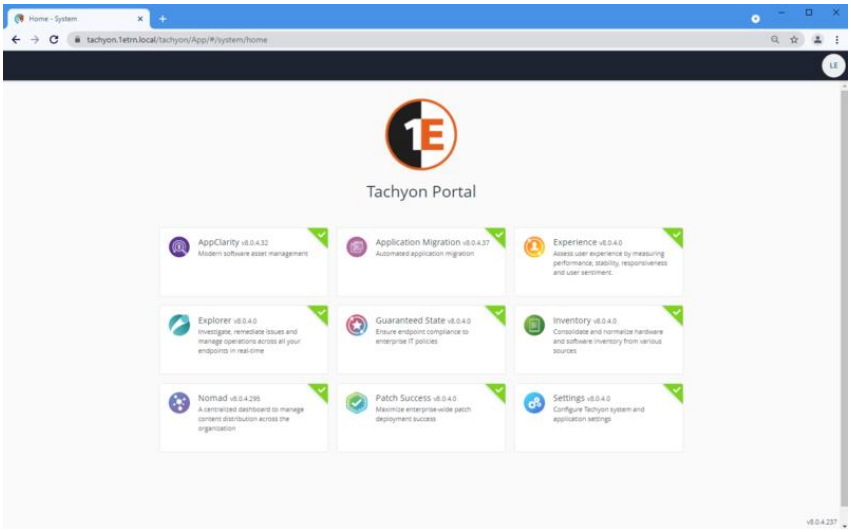
Log on to Tachyon as the new Tachyon user with the AppClarity Administrators role set.

The new **Tachyon user** will now have permissions to view and interact with the AppClarity application. They will be able to complete the verification of the AppClarity installation. To do this:

Log on to the Tachyon portal using the credentials for the Tachyon user added in the previous steps. In our example, this is **ACME\APCAdmin01**, as shown.



The user credentials will be verified and then the applications list will be displayed, as shown. Click on the **AppClarity** application at the top of the list.



This time, the user has the correct role set to be able to view the AppClarity application.

10.2.5.4.1 Verifying the application

Once you've entered the application, you will see four main headings:

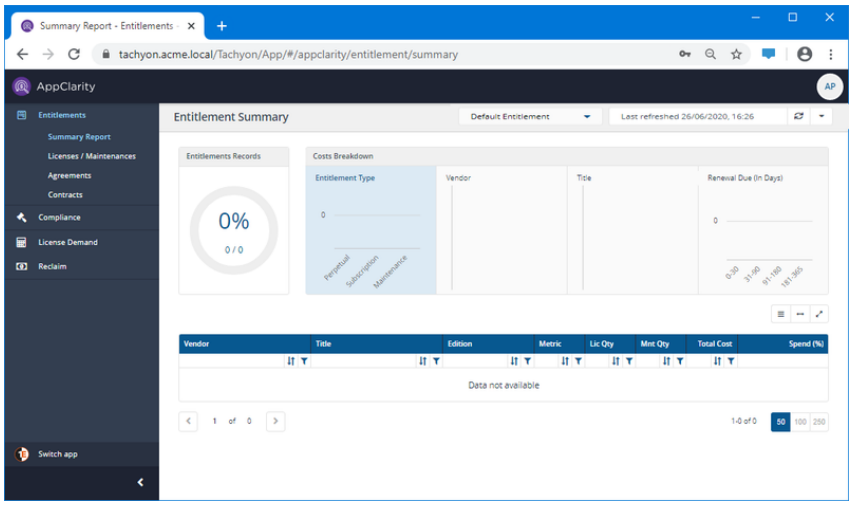
Entitlements

Compliance

License Demand

Reclaim.

The first page that is displayed is the **Entitlement Summary.** Initially the page will contain no data, and you'll see the message **Data not available**. For now don't worry about this, information will appear later after you've entered and published your first entitlement.



10.2.5.4.2 Verifying the new AppClarity default repositories

When AppClarity is installed it **creates** two new default repositories in Tachyon, one for each new repository type:

Default compliance

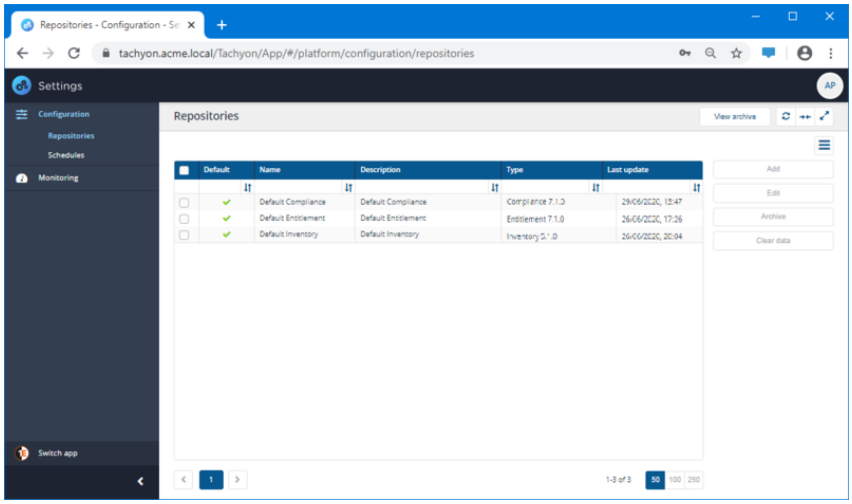
Default entitlement.

You can verify these have been added in the **Settings** application:

From the **Switch app** menu at the bottom-left of the console select **Settings**.

In the **Settings** application navigate to **Configuration**->**Repositories**.

Verify the two new default repositories have been added.



10.2.5.4.3 Verifying the new AppClarity repository types

When AppClarity is installed it creates two new repository types in Tachyon:

Entitlement - this can be used to create new repositories to hold your licenses

Compliance - this can be used to create new repositories to hold different compliance positions - derived from a combination of an Inventory repository and an Entitlement repository.

To verify these have been added, in the **Settings** application:

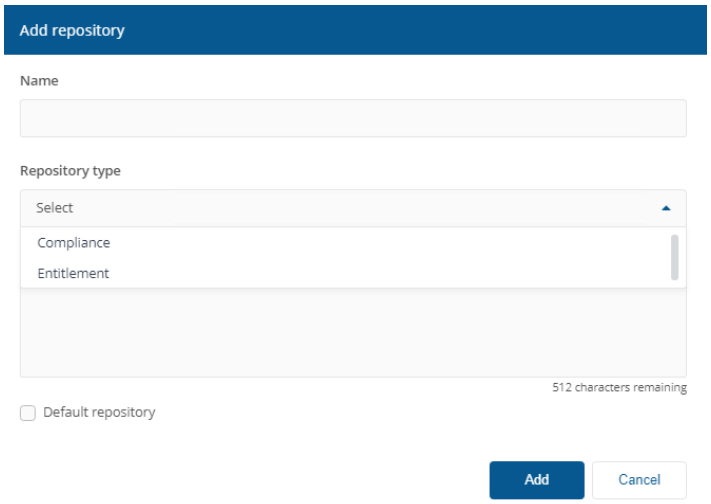
Navigate to **Settings** → **Configuration** → **Repositories**.

Select any of the displayed repositories then click **Add**.

In the **Add repository** dialog click on the **Repository type** dropdown.

Verify that the two new repository types have been added.

Click **Cancel**.



10.3 Configuring AppClarity

How to configure AppClarity.

10.3.1 Tachyon roles for configuring AppClarity

Tachyon and AppClarity roles needed to successfully configure AppClarity.

10.3.1.1 AppClarity Configuration

AppClarity comes with a number of roles, as described in AppClarity user roles, that can be applied to Tachyon users, as described in Configuring Access Rights - tutorial.

To perform all the configuration tasks needed for AppClarity, you need the following roles:

Tachyon Role	Description
Inventory Administrator	This Tachyon System role is needed to be able to: Populate and view inventory repositories Create and test connectors for populating the inventory and entitlement repositories.
AppClarity Administrator	This AppClarity Custom role is needed to be able to access and perform configurations and actions in the AppClarity application.

10.3.2 Connectors page

Tachyon platform uses connectors to connect to other 1E and third-party systems. In addition to the inventory connectors provided, the following entitlement connectors are provided by AppClarity.

Please refer to the Connectors page for details.

10.3.2.1 AppClarity v5.2 connector

Exports entitlements from an AppClarity 5.2 database into a TSV file, which can then be reviewed and imported into AppClarity. You only require access to the AppClarity 5.2 database, you do not require a full installation of AppClarity 5.2. The TSV export file contains all the exported entitlements, this is a summary of the process:

Set permissions on the AppClarity 5.2 database

Set permissions on the export folder

Configure the AppClarity v5.2 connector

After export, you should review the TSV file you will need to use the Entitlement .tsv connector to import them into AppClarity. See Entitlement import files reference page regarding structure and content of TSV files.

> **Note**
>
> If you are migrating from AppClarity 5.2 please contact 1E for help, with using this process and reviewing the contents of your TSV file before importing into AppClarity.

The AppClarity 5.2 connector is a preview for a forthcoming feature that will enable the migration of entitlements from AppClarity 5.2 so that they can be imported into AppClarity. We recommend that this feature is not used in a production environment and evaluated only in a lab environment.

The following limitations apply:

Only license and maintenance entitlement types are exported from AppClarity 5.2

Linked entitlements only support a single license with associated maintenance entitlements. For example, License1 is associated with Maintenance1, Maintenance2, Maintenance3 etc.

Files attached to contracts in AppClarity 5.2 are not exported or imported.

Management groups must exist in Tachyon if they are referenced in any entitlements in AppClarity 5.2. Please refer to Management Groups page.

Bundled entitlements are not supported for extended cases and may result in incorrect linking or export results. For example, when a single license is associated with multiple contracts or when a single maintenance is associated with multiple licenses and many more such cases.

There are some input value restrictions in AppClarity that are not in AppClarity 5.2. For example, contract number is allowed as alphanumeric in AppClarity 5.2, but must be a number only in AppClarity. Issues should be highlighted as caveats during import, most of which you can resolve by editing any problematic entitlement.

Metric Type and Metric Name in AppClarity 5.2 do not map directly to Metric Type and Metric Other in AppClarity. Therefore, you will see Invalid Metric Other caveat for every entitlement you import, unless the original Metric Type is Other. For Metric Type of Device, which is most common, you can publish directly without any concern. For remaining metric types, you can review before import, or correct after import.

10.3.2.1.1 Set permissions on the AppClarity 5.2 database

The connector requires an SQL login to exist in the AppClarity 5.2 database, with explicit *Execute* permissions to the stored procedure **dbo.APSP_ExportEntitlement**

This can be granted in any of the following ways:

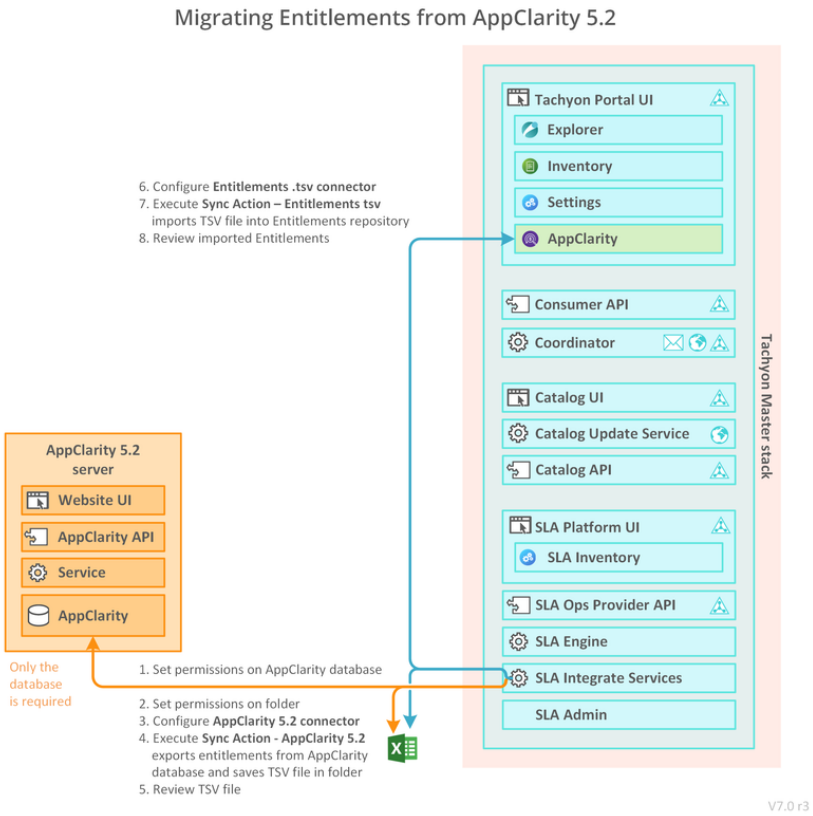
If the connector is using **Trusted Connection**, the SQL login is the **SLA Integrate Services Agent account** which is normally **Network Service**

If the connector is not using **Trusted Connection**, then you can use any SQL login on the AppClarity database and grant it the above rights, and use this login as User ID and password in the AppClarity 5.2 connector.

10.3.2.1.2 Set permissions on the export folder

The connector requires a folder location that must be file share, or a folder on the Tachyon server, to which the **SLA Integrate Services Agent account** has **write** access to.

The folder location can be a folder on the Tachyon server, or a remote share, provided write access is given to the **SLA Integrate Services Agent account** which is normally **Network Service**.



10.3.2.1.3 Configure the AppClarity v5.2 connector

Navigate to **Settings**→**Configuration**→**Connectors**.

Click the **Add** button.

In the **Add Connector** popup select the required **Connector type** from the list of connector types.

Once you've made a selection the **Add connector** popup will show fields appropriate to the selected **Connector type**.

Enter **Connector name**.

In **Name**, enter a logical name for this connector, for example **AppClarity 5.2 production**

> **Tip**
>
> You should use a naming convention for connector names:
>
> **<connector type> <scope> <RCR>**

Scope describes where data is coming from or what it's being used for. For example Demo, Test, Lab, Q2 Audit.

In **SQL Server**, enter the name of the SQL Server instance where the AppClarity 5.2 database is hosted. If it is a named instance, append it to the server name, for example *Server_Name**Instance*.

In **Database**, enter the name of the AppClarity 5.2 database, this is usually **AppClarity**.

If you are using Windows Authentication to authenticate with the SQL Server instance:

Check **Trusted Connection**

You do not need to populate the **User Id** and **Password** fields.

If you are using a SQL Login to authenticate with the SQL Server instance:

Uncheck **Trusted Connection**

In **User Id**, enter the name for the SQL login you want to use to connect to the database.

In **Password**, enter the password for this login.

In **Folder Location**, enter the location for where your exported TSV file will be written.

Click **Save**.

Note

Test will confirm whether the **SLA Integrate Services Agent account**, or specified SQL Login, can connect to the specified database instance.

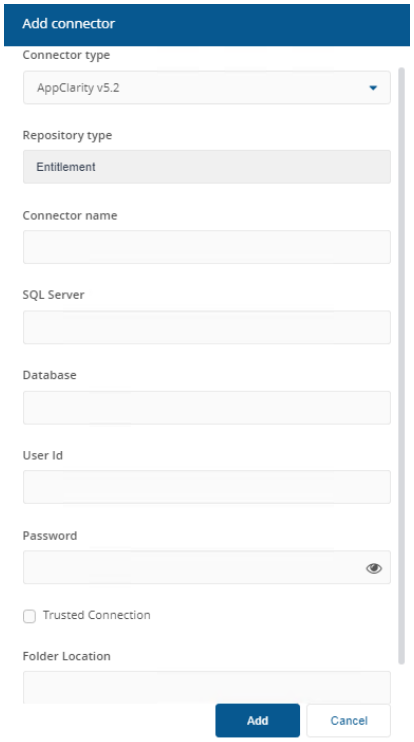
It does not test the following:

If permissions on the AppClarity 5.2 database have been set correctly (refer to Set permissions on the AppClarity 5.2 database)

If permissions on the AppClarity 5.2 database have been set correctly (refer to Set permissions on the export folder).

It is only when you attempt to use the connector (create new action Sync Data) that you will experience an issue if these points are not addressed. Then you will find the export TSV file is not created, and not see any error or warning.

Additionally, **Test** does not test if the stored procedure has been hotfixed.



10.3.2.1.4 Execute Sync Action - AppClarity 5.2

When a new connector is saved a new action is defined in Tachyon. This new action will have a name of the form: **Sync Data - Connector name**, for example **Sync Action - AppClarity 5.2 production**.

Click the **Execute** button.

In the **Execute action** popup subsequently displayed, use the **Repository** menu to select the inventory repository you want to populate.

Once the repository has been selected you can then select the action to run. In the case of inventory repositories the actions will be restricted to inventory related actions. For a connector you will be looking for an action with the form **Sync Data - <connector name>**.

For inventory syncs you have the option to check the **Clean Sync** checkbox.

10.3.2.2 Entitlement .tsv connector

Uploads entitlements from a folder containing one or more tab or comma separated value file(s).

Entitlement files can be created using the AppClarity v5.2 connector (if you are migrating from AppClarity 5.2), or created manually.

10.3.2.2.1 Requirements

Before adding a new **Entitlement .tsv** connector, you will need the following:

Entitlement files must be either tab or comma separated with corresponding **.tsv** or **.csv** extension

Entitlement files must have the correct column structure and content, as described in the reference page: Entitlement import files

The location of entitlement TSV files, which can be a folder location, or share, with at least **read access** for the **SLA Integrate Services Agent account**.

10.3.2.2.2 Entitlement .tsv connector configuration

In **Name**, enter a logical name for this connector

> **Tip**
>
> You should use a naming convention for connector names:
>
> **<connector type> <scope> <RCR>**
>
> **Scope** describes where data is coming from or what it's being used for. For example Demo, Test, Lab, Q2 Audit.

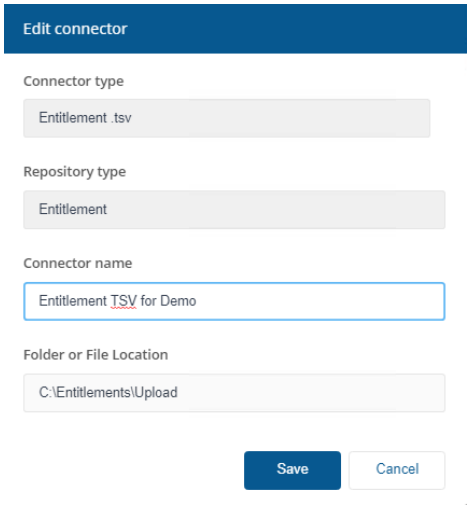
In **Folder or File Location**, enter the location for your entitlement TSV file(s)

> **Tip**
>
> The folder location can be a folder on the server, or a remote share, which the **SLA Integrate Services Agent account** has read access to.
>
> All files in the folder location will be uploaded, including sub-directories. Files can have any name, provided they have a **.tsv** or **.csv** extension.

Click **Save**

> **Tip**
>
> **Test** will error if the service account does not have read access to the folder location, or if there are no files in the folder.
>
> **Note**
>
> Once uploaded, ensure you remove uploaded files from the location. Duplicates will be created if you upload the same file(s) to the same Entitlements repository, which you will then need to manually delete.

Execute or schedule an action as described on the Connectors page.



10.3.3 Repositories page

How to configure repositories for use with AppClarity.

10.3.3.1 Managing your repositories

Go to**Settings → Configuration → Repositories**

Adding a new repository

Click on the **Add** button.

In the **Add repository** popup enter the details for the new repository.

Enter a suitable **Name** for the repository this must not match any existing repository.

Select the **Repository type**.

Enter a suitable description for the new repository.

If you want the new repository to be the default for the selected **Repository type** then check the **Default repository** checkbox, otherwise leave this unchecked.

When all the settings have been made click **Add** to create the repository.

> **Tip**
>
> You should use a naming convention for repository names:
>
> **<scope> <repository type>**
>
> Naming with **scope** first makes it easier to know which repository you are using. The name of the **repository** you are currently using is visible in a drop-down list at the top of pages in the user interface.
>
> Including the **repository type** in the name helps when creating an action or schedule.

10.3.3.1.1 Changing the name of a repository

Select a repository and click **Edit**

In the **Edit repository** popup change the Name

Change the description if required.

If you want the repository to be the default for the selected **Repository type** then check the **Default repository** checkbox, otherwise leave this unchecked.

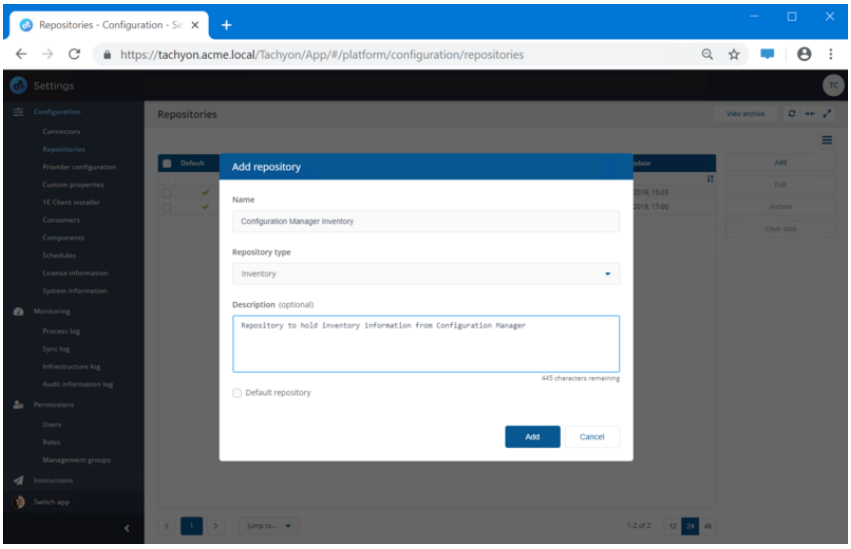
Click **Save**.

10.3.3.1.2 Setting the default repository

Select a repository, for example **Configuration Manager Inventory** and click **Edit**.

In the **Edit repository** popup check the **Default repository** checkbox and click **Save**.

Confirm the repository is listed as Default for its repository Type.



From this point on all pages that show information from an inventory repository would show the **Configuration Manager Inventory** by default. You can still change the repository for a particular page by clicking on the repository selector at the top-right of the page.

If you no longer wish a repository to be the default, then you must choose another repository instead.

> **Tip**
>
> Repositories are useful when you want to segregate different types of data. For example, you could have one inventory repository for Configuration Manager inventory data, and another one for BigFix data. Alternatively, you can have connectors to different inventory sources pushing data into one repository. Any Management Groups that you create will span all the repositories you have.

> **Note**
>
> Once you've created a new repository you cannot delete it. You can only change its details, clear its data or archive it.
>
> The name of a repository must be unique, but can be changed.

Setting a repository as the default repository means it is used as the default on certain screens.

10.3.3.2 Creating a new compliance or entitlement repository

The process is similar to creating a new inventory repository with the additional step of Configuring associations for a new compliance repository. Each **compliance** repository must be associated with one **entitlement** repository and one **inventory** repository.

When you first installed AppClarity, two repositories were created called **Default compliance** and **Default Entitlement** to add to the existing **Default Inventory**. You can associate using the steps described in Running your first Compliance License Summary.

When creating new repositories, please refer to Naming conventions.

10.3.3.2.1 Guidance for using multiple repositories

In general, you will not need additional repositories. Once a compliance repository has been used you should not change its associated entitlement or inventory repositories because that will produce inconsistent compliance results, you should keep all your:

Entitlements in a single entitlements repository, for example **Default Entitlements**, you can use additional entitlements repositories for testing entitlement imports

Reclaim policies in a single compliance repository, for example **Default compliance**, the reclaim system uses all compliance repositories, so if you create reclaim policies in multiple compliance repositories they will all be used and troubleshooting may be difficult, but you can use management groups to manage reclaim policies.

You can use a single compliance repository for compliance reporting. If you want you can create a new compliance repository for a specific compliance audit project, for example, every quarter or annually, so that you can compare one period with another. You would associate each compliance repository with your default entitlement repository, but maybe associate an additional inventory repository for each snapshot inventory.

10.3.3.2.2 Configuring associations for a new compliance repository

To create a new **compliance** repository and associate it with one **entitlement** repository and one **inventory** repository, you'll need to:

Under the **Settings**→**Configuration**→**Repositories** click **Add**.

In the **Add repository** screen for:

Name - enter a logical name for the new repository.

Repository type - select Compliance from the drop-down menu.

Inventory repository - select which Inventory repository is used by Compliance.

Entitlement repository - select which Entitlement repository is used by Compliance

Description (optional) - enter a description for the new repository.

Default repository - check if you want this to be a default repository.

When you first run AppClarity the **Entitlement repository** dropdown in the **Add repository** screen will only contain the **Default Entitlement** repository, you can select the default or other entitlement repository if you have created one.

You're now ready to start populating the compliance repository.

10.3.4 SCCM Uninstall Provider

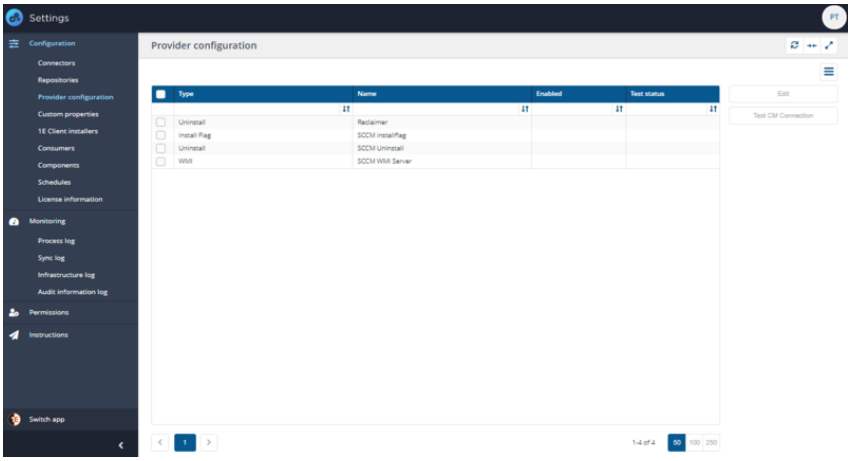
10.3.4.1 Configuring the SCCM Uninstall Provider

Enable the SCCM Uninstall provider to support the use of the SCCM custom Reclaim feature.

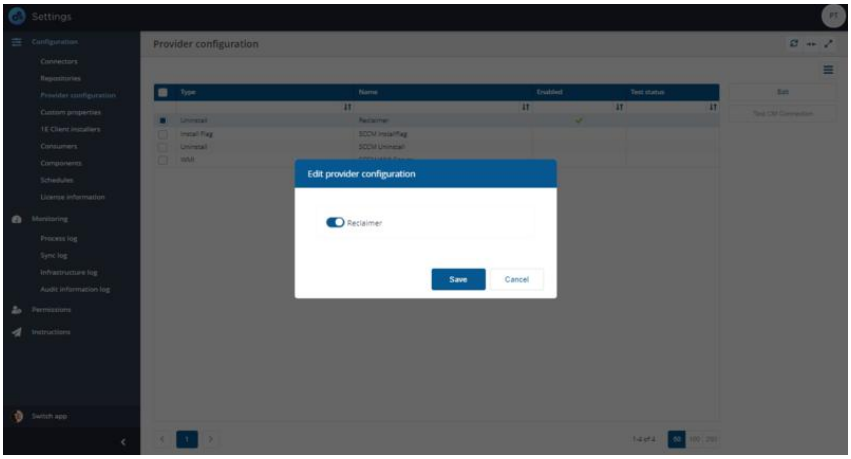
> **User role**
>
> Ensure you have **Full Administrator** role assigned to enable/disable SCCM Uninstall provider configuration from **Settings**.

To switch the **SCCM Uninstall** on:

Switch app to **Settings**→**Configuration**→**Provider Configuration** and select the **Reclaimer** provider type.

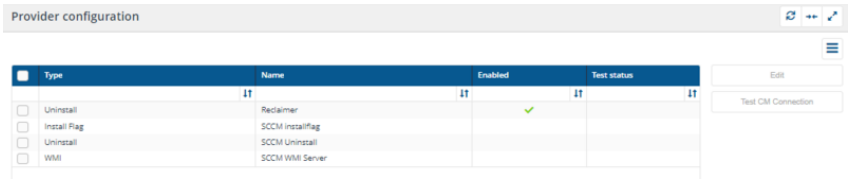


Click **Edit**.



Slide the toggle to **ON** next to **Reclaimer**.

Click **Save**.



Once you have set up the SCCM Uninstall provider configuration, on the Provider Configuration screen, select **SCCM Uninstall** and click **Test CM Connection**. A successful test connection ensures the provider configuration can connect with your SCCM server using the provided information and is ready to use.

To use the SCCM custom Reclaim, please refer to Reclaiming a product using SCCM Uninstall.

10.3.5 Deploying Software Reclaimer

The **Software Reclaimer** is an executable that is run on Windows clients and is responsible for implementing reclaim policies provided by AppClarity. It can be distributed to devices using Configuration Manager. For more details on how to set up reclaim policies, please see Reclaiming a product based on its usage.

10.3.5.1 Software Reclaimer files

Note

Software Reclaimer is deployed and run on client devices, it is not installed. The supported deployment method is using Microsoft System Center Configuration Manager, described in Configuration Manager setup below.

Before deployment, the Software Reclaimer requires configuration, described in Configuring the Software Reclaimer below.

During installation of Tachyon, Tachyon Setup (specifically the SLA Platform installer) copies three files into **C:\ProgramData\1E\SLA Platform**

AppClarity.SoftwareReclaimer.exe	The Software Reclaimer executable
AppClarity.SoftwareReclaimer.xml	Template for optional customization of the software reclaim dialog. See Customizing the dialogs. Contains the public key of the Tachyon web server when using HTTPS.
logo.png	The banner logo, preferably 500x90 pixels. See Customizing the dialogs.

If the executable is run without the customization files, it will display the default English text and 1E banner logo.

10.3.5.2 Configuring the Software Reclaimer

10.3.5.2.1 Overview

The Software Reclaimer is designed to run in two modes using the **-mode** parameter. These modes should be run at different times of the day, on all Windows workstations.

Optout mode processes optional software reclaim policies. When run, it contacts the **SLA Operations Provider API** to determine whether there is software to optionally uninstall from the local machine, and displays a dialog to the user only if there are polices for optional uninstallation. Optout mode does not uninstall any software. The Software Reclaimer does not need elevated rights to run in this mode, but does require a user to be logged on.

If there isn't software to optionally uninstall, the **SLA API** returns an empty list, and the Software Reclaimer exits without displaying anything;

If there is, the Software Reclaimer prompts the user for a response, and sends back the user's response to the **SLA Operations Provider API**

If the response is **Remove software**, then the server will convert the reclaim policy from optional to mandatory, so that the software will be uninstalled later. If the response is **I still need this**, then software is not uninstalled.

> **Tip**
>
> Optout mode is best used at a time when users are most likely at their computers so that they can respond to prompts.

Mandatory mode processes mandatory reclaim policies. In this mode, the Reclaimer runs unattended and does not display any dialog or progress bars. When run, it contacts the **SLA Operations Provider API** service to determine whether there is software to uninstall from the local machine. For this to work, the Software Reclaimer must be run with administrative privileges.

If there isn't software to uninstall, the server returns an empty list, and the Software Reclaimer exits

If there is, the **SLA Operations Provider API** returns the software it considers the highest priority to remove for the Software Reclaimer to act on immediately. The Reclaimer attempts to uninstall the software, returning the result to the **SLA Operations Provider API**.

> **Tip**
>
> Mandatory mode is best used at a time when users are not at their computers so that any software uninstall does not disrupt them during working hours.
>
> Mandatory mode should be run at least one hour after optout in order to allow the server to process opt-out responses. Typically, you will configure deployments to run opt-out mode in the morning when the user is logged on, and mandatory mode in the afternoon when the computer is switched on.
>
> **Note**
>
> Regardless of the mode in which it is run, by default the Software Reclaimer will wait a random amount of time before it begins. The random wait is anywhere between 0 and

60 minutes and is implemented to prevent flooding the **SLA Operations Provider API** in larger organizations.

Mandatory reclaim process will reclaim only one software in a cycle.

Note

The supported deployment method is using Microsoft System Center Configuration Manager, described in Configuration Manager setup.

10.3.5.2.2 Software Reclaimer command line

```
AppClarity.SoftwareReclaimer.exe [-mode <mode>] [-service "<serverURL>/CoreExternal/api/ReclaimAction/Action/"]
```

Name	Value options	Notes
-mode	mandatory optout both (default)	This parameter determines the Software Reclaimer request mode. Although this parameter is optional, you should always use it with a value of **mandatory** or **optout**. **Warning** Do not use the value**both**unless testing; because it will run optout and then immediately run mandatory, without sufficient time for the server to have processed the opt-out response, especially if you have used the **-nowait** parameter. You would typically wait for several minutes up to an hour to allow opt-out responses to be processed.
-service	`<serverURL>/CoreExternal/api/ReclaimAction/Action/`	**<serverURL>** is the binding used to connect to the Tachyon server which hosts the SLA Operations Provider API, for example: **https://tachyon.acme.local:443** If this parameter is not used, the Software Reclaimer will attempt to use the URL specified in **<appClarityReclaimerServiceUrl>** under the **<appSettings>** section of the **AppClarity.SoftwareReclaimer.xml** file. The URL in the template XML files uses HTTPS. You can change the URL to use HTTP, or keep HTTPS and add the public key of the Tachyon web server. **Warning** To use HTTPS please refer to Configuring Software Reclaimer to use HTTP or HTTPS. Using HTTP does not require any additional configuration if the **-service** parameter is used. This parameter is not required in Demo mode, however if not provided you will see COM exception errors logged.

Name	Value options	Notes
-nowait		By default, the Software Reclaimer waits a random amount of time before it contacts the server, regardless of the mode in which it is run. The random wait is anywhere between 0 and 60 minutes and is implemented to prevent flooding the AppClarity service in large organizations. The **-nowait** parameter can be used to avoid the random wait, which is useful when testing. **Note** The **-nowait** parameter is for testing purposes only and must never be used in a production environment.

10.3.5.2.3 Configuring Software Reclaimer to use HTTP or HTTPS

10.3.5.2.3.1 If using HTTP

Specify HTTP in the server URL used to connect to the Tachyon Web Server (Master Stack):

Either edit the server URL in each XML file(s)

Use the **-service** parameter to override XML file(s).

10.3.5.2.3.2 If using HTTPS

You can configure the Software Reclaimer to use SSL over HTTPS to connect to the Tachyon website. The following applies to the Tachyon website's SSL certificate:

It must be trusted by clients running the Software Reclaimer. This is also the same requirement for Tachyon clients. Please refer to Client authentication certificates

Its public key must be encoded in each of the Software Reclaimer XML file(s)

Use the attached ReclaimerPublicKey.ps1 to encode the public key and add it to the XML file.

Either run the script on the Tachyon Web Server (Master Stack)

Or copy the XML file from the Web Server into the same folder as the PowerShell script, and then run the script

If you have multiple XML files to support customizations then you will need to add the public key to each of them.

10.3.5.2.3.3 Using a non-standard port

A default installation of Tachyon uses standard ports HTTP 80 and HTTPS 443. You may wish to use a different port for Software Reclaimer, for example, if you previously used:

HTTP 8335 or HTTPS 8336 with AppClarity 5.2

HTTP 8080 or HTTPS 8443 with SLA Platform 3.3 and AppClarity 6.1

You can manually add a website binding after installation of Tachyon. You may already be using a non-standard port if specified in Tachyon Setup during installation of Tachyon, or you manually added a binding after installation for another application like Application Migration, or ActiveEfficiency.

10.3.5.2.4 Testing Software Reclaimer

If you simply want to demonstrate how the reclaimer behaves, or test customizations (refer to Customizing the dialogs), then you can use Demo mode.

If you run Software Reclaimer on a device that has a reclaim policy then it will process the reclaim in the normal way. That is, it will present the optout dialog if the policy is configured for optional uninstall, and uninstall the software in mandatory mode. You will not be able to easily repeat the test even if you re-install the software, because the policy will have been processed on the server and be subject to Site Settings affecting the Software Reclaimer, including uss_AutomaticUninstallOptOutInterval_Days (7) and uss_MinimumResendCompletedPolicy_Days (14).

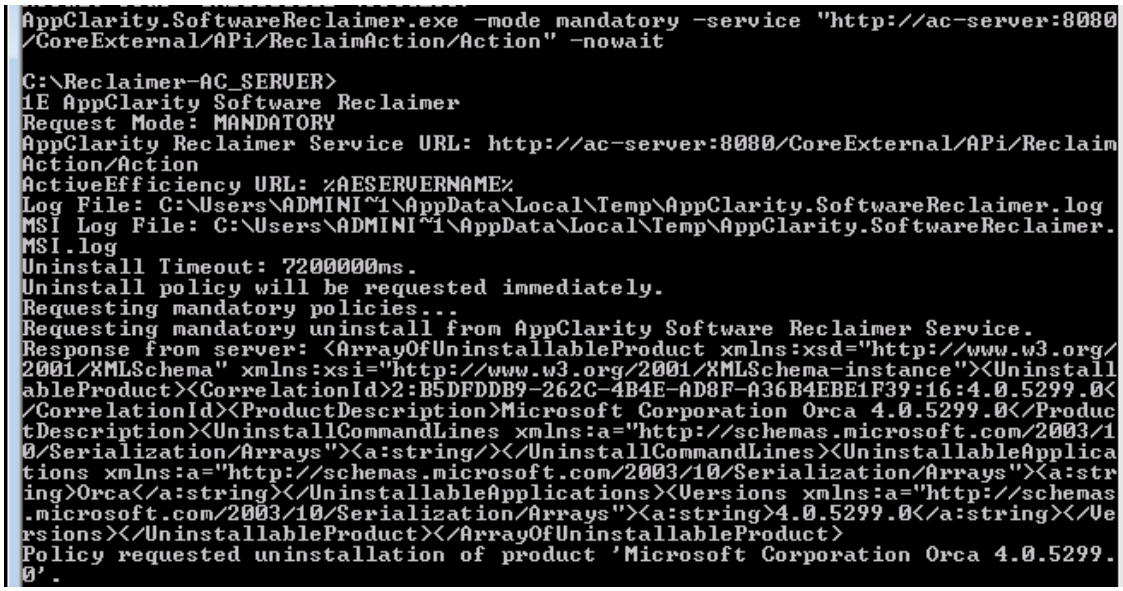
Warning

Only add the -nowait parameter when testing.

```
AppClarity.SoftwareReclaimer.exe [-mode <mode>] [-service <serverURL>/CoreExter
nal/api/ReclaimAction/Action/] -nowait
```

You can see reclaim reports in Viewing the software reclaim reports.

10.3.5.2.5 Example command-line for testing mandatory mode



To view what policies affect a device, without processing a reclaim, you can test the URL in a browser:

```
<serverURL>/CoreExternal/api/ReclaimAction/Action/OptionalPolicy?machinegroup=<
Domain Name>&machinename=<Machine Name>
```

```
<serverURL>/CoreExternal/api/ReclaimAction/Action/UninstallPolicy?machinegroup=
<Domain Name>&machinename=<Machine Name>
```

<serverURL> is the binding used to connect to the Tachyon server which hosts the SLA Operations Provider API, for example: **https://tachyon.acme.local:443**

Below is an example XML response for a mandatory request. You would only see details for one application at any time. If you have multiple reclaims for the same device then the server will prioritize one at a time.

Example XML response for a mandatory request Expand source

```
<ArrayOfUninstallableProduct xmlns="http://www.1e.com/appclarity/services/softw
arereclaimer/" xmlns:i="http://www.w3.org/2001/XMLSchema-instance">
 <UninstallableProduct>
   <CorrelationId>1:2345:5678</CorrelationId>
   <ProductDescription>Microsoft Visio Premium 2010</ProductDescription>
   <UninstallCommandLines xmlns:a="http://schemas.microsoft.com/2003/10/Seriali
zation/Arrays">
      <a:string>cscript.exe ".\Resources\VisioPro2010\VisioPro_2010.vbs"</a:str
ing>
   </UninstallCommandLines>
   <UninstallableApplications xmlns:a="http://schemas.microsoft.com/2003/10/Ser
ialization/Arrays">
      <a:string>Microsoft Visio Premium 2010</a:string>
   </UninstallableApplications>
   <Versions xmlns:a="http://schemas.microsoft.com/2003/10/Serialization/Arrays
">
      <a:string>14.0.6029.1000</a:string>
   </Versions>
 </UninstallableProduct>
</ArrayOfUninstallableProduct>
```

10.3.5.2.6 Log files

Every time the Reclaimer runs it will create a local log file of the process it is doing. The location and name of the log file depends on what task the reclaimer is doing.

Task	Logpath	Notes
Optout	**C:\Users\{USER}\AppData\Local\Temp\ AppClarity.SoftwareReclaimer.log**	Optout mode is normally run under user context so that the user can interact with the dialog.

Task	Logpath	Notes
		This means the log file will be in the users Temp folder within the user profile.
Mandatory	**C:\windows\Temp\AppClarity.SoftwareReclaimer.log**	Mandatory mode is normally set to run under system context, in order to process reclaim uninstall commands. Therefore, the log file will be under the system temp directory.
Reclaim	**C:\windows\Temp\AppClarity.SoftwareReclaimer.MSI.log**	For a mandatory reclaim, if a reclaim occurs using an MSI then an MSI log

Task	Logpath	Notes
		file is also created.

10.3.5.3 Configuration Manager setup

The following assumes you will create one Configuration Manager package, with two deployments. However, an additional two deployments are recommended for initial testing.

10.3.5.3.1 To setup the Software Reclaimer in Configuration Manager

Create a source folder in your Configuration Manager site source folder structure

Copy the AppClarity.SoftwareReclaimer.exe and optionally the two customization files into the source folder

Optionally include other customization files, if required for language support - see customizing the dialogs

> **Tip**
>
> During Tachyon installation, AppClarity.SoftwareReclaimer.exe and the two customization files are copied to : <installation drive>:\ProgramData\1E\SLA Platform

In Configuration Manager console, deploy a new software distribution package, with two programs

In package settings, point the source directory to the source folder where you copied all the files.

For the newly created package, distribute to relevant distribution points.

Create a new collection to be used specifically for the Software Reclaimer.

Create two new programs for the package – one for the mandatory mode and one for the opt-out mode.

Create two deployments – one for each program.

10.3.5.3.2 Collections

We recommend you create at least one new collection specifically for use with the Software Reclaimer. DO NOT reuse an existing collection made for another purpose in case you need to add exclusions at a later date. The collection must contain all the Windows workstations you want to run the Software Reclaimer on. There may be instances where it is advisable to create more than one collection so that you can stagger the times the Software Reclaimer is run within your organization.

10.3.5.3.3 Programs

You must create up two programs for the package – one for opt-out mode and one for mandatory mode.

The parameters you need to set in Configuration Manager when you run it in mandatory mode are:

Parameter	Value
Command line:	`AppClarity.SoftwareReclaimer.exe -mode MANDATORY -service "<server URL>/CoreExternal/api/ReclaimAction/Action"` See Software Reclaimer command-line regarding the **-service** parameter.
Program can run:	Whether or not a user is logged on.
Run mode:	Run with administrative rights. In mandatory mode, the Software Reclaimer requires administrative privileges to run without user intervention and it is advisable to run it when users are not at their computers to avoid interrupting them during working hours. When the application to be uninstalled has been installed in per user mode, i.e. the **only for me** option was selected during installation, the program for the Configuration Manager package must be run with user's rights. If the application has not been installed in per user mode, i.e. the **for everyone** option was selected during installation, the program for the Configuration Manager package must be run with administrative rights.

In opt-out mode, the Software Reclaimer does not require elevated rights and it is advisable to run it at a time when users are most likely at their computers so that they can respond to prompts. The parameters you need to set in Configuration Manager when you run it in opt-out mode are:

Parameter	Value
Command line:	`AppClarity.SoftwareReclaimer.exe -mode OPTOUT -service "<serverURL>/CoreExternal/api/ReclaimAction/Action"` See Software Reclaimer command-line regarding the **-service** parameter.
Program can run:	Only when a user is logged on.
Run mode:	Run with user's rights.
When this program is assigned to a computer:	Run once for every user who logs on.

10.3.5.3.4 Deployments

Each program created (one for opt-out mode and one for mandatory mode) must have its own deployment. Additionally, if you created more than one collection, you must create an advertisement for each collection. The parameters for the deployments are:

Parameter	Value
Mandatory assignments:	Occurs every 1 day(s) effective **<date>** where **<date>** is when the mandatory assignment comes into effect.
Program rerun behavior:	Always rerun program.
Distribution points:	Download content from distribution point and run locally.

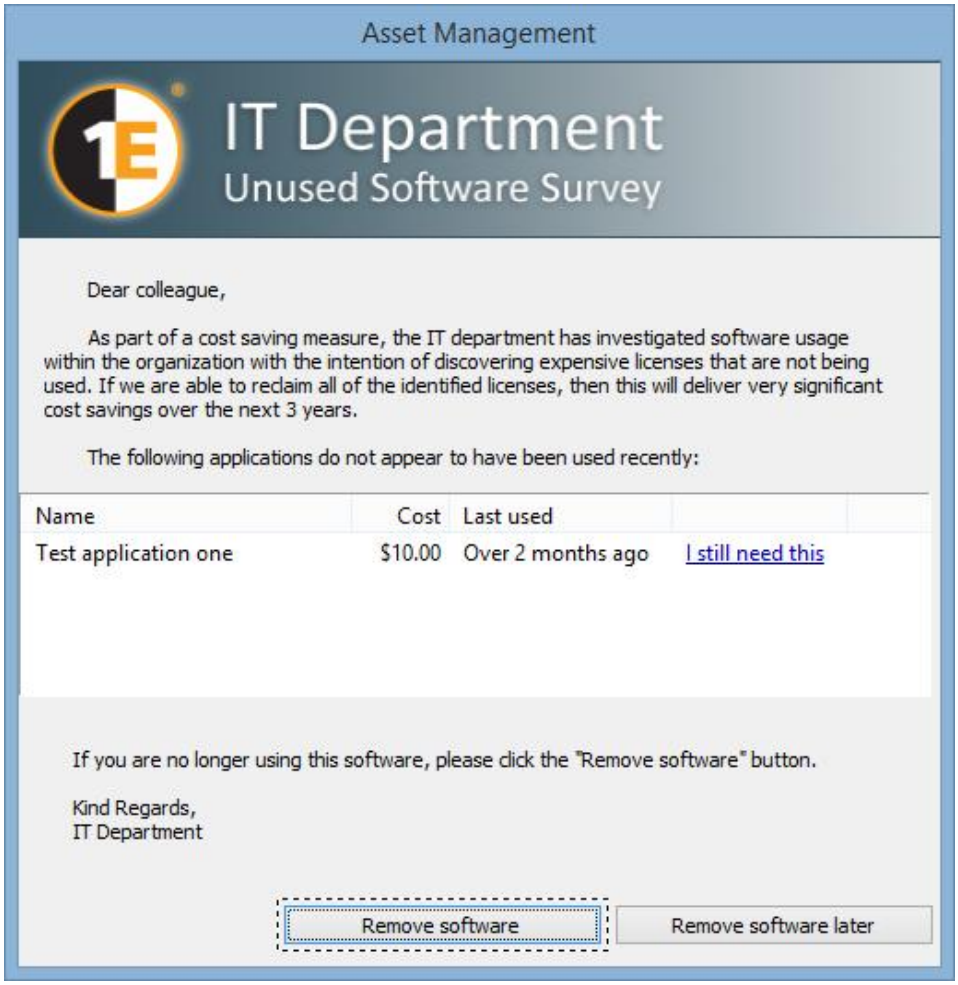
> **Tip**
>
> Mandatory mode is best used at a time when users are not at their computers so that any software uninstall does not disrupt them during working hours.
>
> Mandatory mode should be run at least one hour after optout in order to allow the server to process opt-out responses. Typically, you will configure deployments to run opt-out mode in the morning when the user is logged on, and mandatory mode in the afternoon when the computer is switched on.

10.3.5.3.5 Testing

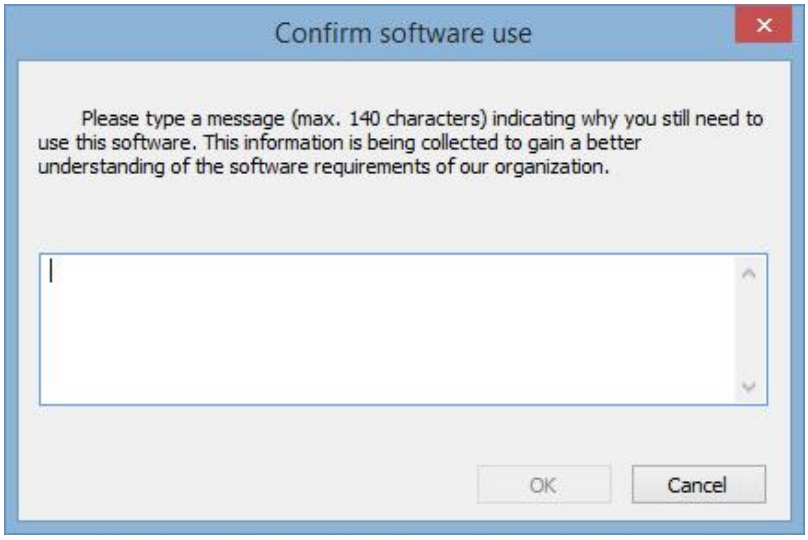
Please refer to Testing Software Reclaimer above.

10.3.5.4 Opt-out dialog and reclaim override management

This dialog is displayed when the Software Reclaimer is run in opt-out mode and only if there is at least one application that is a candidate for un-installation. If there is more than one candidate for removal, it will show up to three items as prioritized by the AppClarity server.



If the end-user selects an **I still need this...** link, a second dialog is displayed prompting them to justify their need for the corresponding application.



To close the main opt-out dialog, the end-user must select either **Remove Software** or **Remove software later**.

The Software Reclaimer closes automatically after 120 minutes if the end-user does not interact with the dialog.

Action by end-user	Response sent back to the server	Action by AppClarity	Next experience for the end-user
No action	None.	None, because the Reclaimer does not send anything back to the server.	The next time the Reclaimer runs in opt-out mode, the opt-out dialog is displayed. The applications listed depend on whether priorities have changed.
Remove software	The Reclaimer sends back a response with: end-user's choice details of any justification reasons the end-user has entered	The policy for each of the displayed applications is converted from optional to mandatory, except for applications where the end-user has given a reason using **I still need this...**. If an administrator rejects the user's reason, then the policy for that application is converted to mandatory.	The next time the Reclaimer runs in opt-out mode, the opt-out dialog is displayed only if there are further applications with optional policies. Each time the Software Reclaimer runs in mandatory mode, the Reclaimer uninstalls the top priority application that has a mandatory policy.
Remove software later	The Reclaimer sends back a response with: end-user's choice details of any justification reasons the end-user has entered	They defer the decision of whether or not to uninstall all the displayed applications. The opt-out dialog is not displayed on that machine for the next seven days even if the Software Reclaimer is run in opt-out mode on that machine within the seven-day window. When an end-user defers the decision for the first time, they must choose **I still need this...** within the next 21 days or it will be scheduled for uninstallation and not be displayed in the opt-out dialog again.	The next time the Reclaimer runs in opt-out mode, the opt-out dialog is displayed only if there are further applications with optional policies. The opt-out dialog is only shown again if there are further applications with optional policies. Next time the Software Reclaimer runs in

Action by end-user	Response sent back to the server	Action by AppClarity	Next experience for the end-user
		If an administrator rejects the user's reason, then the policy for that application is converted to mandatory.	mandatory mode, the Reclaimer uninstalls the top priority application.

When a policy for an application is converted from optional to mandatory, then the application will be handled the same as any other application that has a mandatory policy. The mandatory policies for the machine are prioritized by the AppClarity server, and the next time the Software Reclaimer runs in mandatory mode, the application with the highest mandatory policy will be uninstalled. The Software Reclaimer uninstalls only one application each time it runs.

Reclaim overrides

When a user chooses to opt out of a reclaim, their reason is displayed in Reclaim override management under the Policy tab. Administrators then have an option whether to accept or reject the end-user's reason. The end-user is not informed of the administrator's decision. Please see Opt-out dialog and reclaim override management for more information.

Administrator actions

If an administrator accepts the reason, the application policy for the end-user's machine is de-activated (is neither an optional nor mandatory policy) and the application starts again with the normal usage assessment that may cause re-activation at a later date

If an administrator rejects the reason, the policy for the application is converted from optional to mandatory.

User actions

If the user selects **Remove software**, then all applications in the list will be scheduled for un-installation. The actual un-installation is reassessed on the next mandatory-mode software reclaim run and prioritized along any other candidates for mandatory uninstall.

If the user selects **Remove software later**, they defer the decision of whether to uninstall the applications. The opt-out dialog is not displayed on that machine for the next seven days even if the Software Reclaimer is run in opt-out mode on that machine within the seven-day window.

When a user defers the decision for the first time, they must choose I still need this... within the next 21 days or it will be scheduled for uninstallation and not be displayed in the opt-out dialog again.

When a policy for an application is converted from optional to mandatory, then the application will be handled the same as any other application that has a mandatory policy. The mandatory policies for the machine are prioritized by the AppClarity server, and the next time the Software Reclaimer runs in mandatory mode, the application with the highest mandatory policy will be uninstalled. The Software Reclaimer uninstalls only one application each time it runs.

10.3.5.5 Site Settings affecting the Software Reclaimer

The Sofware Reclaimer has the following settings in the SLA databases, which directly relate to the behaviour of the Reclaimer. There are other settings in the same database tables which relate to usage policies and other behaviour of the system, some are described in Usage categories

Warning

The following is for information only, to help understand how the Reclaimer process works. Do not make changes to any settings unless advised by 1E.

Setting	Default	Purpose
uss_AutomaticUninstallRetryLimit	5	Number of times an uninstall is retried if a status is returned indicating that the uninstall failed but a retry is permitted. The retries must complete within the time window given by the setting uss_minimumResendCompletedPolicy_Days (by default, 14 days). After this the policy is recorded as having failed for the device in question
uss_AutomaticUninstallMaxItemsCount	1	Do not change this setting.
uss_AutomaticUninstallOptOutTimeoutMins	120	This is the number of minutes for which the Software Reclaimer opt-out dialog is displayed. If the user has not interacted with the dialog after this time period, it automatically closes. No default user action is associated with this closure.
uss_AutomaticUninstallOptOutMaxLimit_Days	28	This defines the length of time for which a user can continually defer the decision with regard to software reclaim, when presented with the opt-out dialog. After this time period elapses, if the user has not either requested approval for the software to be retained, or acceded to its removal, then a mandatory policy to uninstall it will be activated. The time period

Setting	Default	Purpose
		commences when the user first defers the decision from the opt-out dialog.
uss_AutomaticUninstallOptOutInterval_Days	7	The number of days before the Reclaimer opt-out dialog is redisplayed to the user, if previously the end-user responded to the dialog in any way.
uss_AutomaticUninstallOptOutMaxItemsCount	3	Do not change this setting.
uss_MinimumResendActivePolicy_Days	2	The number of days before an active policy is re-sent to a machine.
uss_MinimumResendCompletedPolicy_Days	14	The number of days before a completed policy (either successfully completed or failed) can be re-sent to a machine.
uss_AutomaticUninstallRemoveComponentProducts	1	If set, indicates that, if a software reclaim policy is associated with a product which is a suite (e.g Microsoft Office Professional Plus), then any component products associated with that suite (e.g Excel) will also be uninstalled.
uss_AutomaticUninstallKeepInterval_Days	60	The number of days before an active policy is re-sent to a machine If a user has requested that a software item not be reclaimed, and the request has not already been approved or rejected, then this is the number of days that must elapse before the user will again be prompted as to what action should be taken.
uss_ReclaimOptOutInfoDetails_MaxRows	100	Do not change this setting.

Warning

Do not make changes to any settings unless advised by 1E.

The settings exist in **[SLA-Shared].[dbo].[ProjectSetting]** table, which gets copied to **[SLA-Data].[dbo].[InstanceSetting]** when a new Inventory repository is created. Each Inventory repository will have its own group of settings in the InstanceSetting table. You can edit **[SLA-Data].[dbo].[InstanceSetting]** to change the settings for an existing repository. If that repository contains reclaim policies, the new settings will take effect and update the policies after an action is run on the repository.

Use the following SQL script to view settings in both tables.

```
SELECT * for [SLA-Shared]

SELECT * FROM [SLA-Data].dbo.InstanceSetting AS ISG
JOIN [SLA-Data].dbo.InstalledProject AS IP ON IP.ProjectID=ISG.ProjectID
JOIN [SLA-Data].dbo.Instance AS I ON I.InstanceID=ISG.InstanceID
WHERE IP.Title='Compliance' AND I.IsArchived=0
```

10.3.5.6 Customizing the dialogs

Either or both of these dialogs can be customized:

For the main (Asset Management) dialog, all text plus the header logo can be customized

For the confirmation (Confirm software use dialog), all text can be customized

Dialogs are customized by using one or more locale specific XML files to override any or all parts of the two dialogs. Locales and XML search order, are discussed in more detail below under Per-locale customization.

Although you can have multiple XML files for different languages, you cannot use multiple files to independently configure either dialog. The first XML file which is considered applicable will always be used, to the exclusion of any other files.

The XML files

must be included in the same folder as the Reclaimer executable

can have any name but we recommend a convention such as **AppClarity.SoftwareReclaimer(locale).xml**

10.3.5.6.1 Customizing the logo in the main dialog

The built-in header logo used in the main dialog can be replaced using an image file called **logo.png** which must exist in the same folder as the Reclaimer executable.

For best results, this image should be **500x90 pixels**.

There can be only one logo file, because the filename is hard-coded in the software reclaimer, and is not referenced in any XML files.

10.3.5.6.2 Sample XML customization file

A sample XML file is shown below, which includes all the element names for text strings that are configurable. Any element included in an XML file will override the default built-in both dialogs for

all target locales. If the element is missing then the built-in default text will be used, as decribed below under Partial customization.

Note

The use of the CDATA sections ensures that text containing special XML characters, such as **<**, **>** and **&**, does not need to be specially escaped.

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <dialogResourceStrings>
    <mainDialog>
      <title>Asset Management(No LANGUAGE)</title>
      <instructions><![CDATA[
        Dear colleague,
        As part of a cost saving measure, the R&D department has investigated s
oftware usage within the organization with the intention of discovering expensi
ve licenses that are not being used. If we are able to reclaim all of the ident
ified licenses, then this will deliver very significant cost savings over the n
ext 3 years.

        The following applications do not appear to have been used recently:
      ]]></instructions>
      <footnote><![CDATA[
        If you are no longer using this software, please click the <Remove soft
ware> button.

        Kind Regards,
        IT Department
      ]]></footnote>
      <button1><![CDATA[Remove software]]></button1>
      <button2><![CDATA[Remove software later]]></button2>
      <header1><![CDATA[Name]]></header1>
      <header2><![CDATA[Cost]]></header2>
      <header3><![CDATA[Last used]]></header3>
      <unknown><![CDATA[Unknown]]></unknown>
      <overOneYearAgo><![CDATA[Over a year ago]]></overOneYearAgo>
      <overNYearsAgo><![CDATA[Over %d years ago]]></overNYearsAgo>
      <overOneMonthAgo><![CDATA[Over a month ago]]></overOneMonthAgo>
      <overNMonthsAgo><![CDATA[Over %d months ago]]></overNMonthsAgo>
      <overOneWeekAgo><![CDATA[Over a week ago]]></overOneWeekAgo>
      <overNWeeksAgo><![CDATA[Over %d weeks ago]]></overNWeeksAgo>
      <yesterday><![CDATA[Yesterday]]></yesterday>
      <overNDaysAgo><![CDATA[Over %d days ago]]></overNDaysAgo>
      <today><![CDATA[Today]]></today>
      <stillNeeded><![CDATA[I still need this]]></stillNeeded>
    </mainDialog>
    <confDialog>
      <title><![CDATA[Confirm software use]]></title>
      <instructions><![CDATA[
        Please type a message (max. 140 characters) indicating why you still ne
```

```
ed to use this software. This information is being collected to gain a better u
nderstanding of the software requirements of our organization.
      ]]></instructions>
      <button1><![CDATA[OK]]></button1>
      <button2><![CDATA[Cancel]]></button2>
    </confDialog>
  </dialogResourceStrings>

  <appSettings>
    <appClarityReclaimerServiceUrl>http://SCCM.QA.LOCAL:8080/CoreExternal/api/R
eclaimAction/Action/</appClarityReclaimerServiceUrl>
    <activeEfficiencyUrl>http://%AESERVERNAME%/ActiveEfficiency</activeEfficien
cyUrl>
        <publicKey></publicKey>
  </appSettings>
</configuration>
```

10.3.5.6.3 AppSettings

The **<appSettings>** section of the XML file can be ignored or removed if you are using the **-service** parameter on the Software Reclaimer command-line.

If you are not using the **-service** parameter, then you must ensure that all XML files contain the correct value for **appClarityReclaimerServiceUrl**.

The **<activeEfficiencyUrl>** section is not used, and can be deleted.

The **<publicKey>** section is used to support the optional SSL pinning feature. Please contact 1E for more details about this feature.

10.3.5.6.4 Partial customization

For a partial customization, exclude elements from the XML file. This will cause the hard-coded default values embedded in the Reclaimer executable to be used. For example, if you exclude the

```
<button1><![CDATA[Remove software]]></button1>
```

element in the **<mainDialog>** section, the Remove software button will take the default value. However, any other elements which override hard-coded defaults would still take effect.

If the element corresponding to the entire dialog is omitted, then that dialog reverts to its hard-coded defaults. For example, omitting the **<confDialog>** element and its children will result in the main dialog being customized and the confirmation dialog reverting to its hard-coded defaults.

10.3.5.6.5 Per-locale customization

Locales are specified by two attributes, using the Microsoft locale name format:

The first attribute is the language associated with the locale, for example, **de** for German

The second attribute is the geographical region associated with the locale, for example, **at** for Austria

In this example **de-at** represents German (Austria). Another example is **en-us** which represents English (United States).

You can specify either the first attribute, or both attributes, when creating a customization XML file. The example XML file below specifies both attributes: *<configuration xml:lang="de-at">*. A customization file that specifies only the first attribute, for example de, would specify the language attribute as such: *<configuration xml:lang="de">*.

When the Software Reclaimer runs, it reads the Windows user locale and uses the following search order to select the first applicable customization XML file:

Region - the first XML file found whose language attribute exactly matches the full locale e.g. **<configuration xml:lang="de-at">**

Language - the first XML file found whose language attribute matches the language of the locale e.g. **<configuration xml:lang="de">**

Global default - the first XML file found that does not specify a language attribute i.e. **<configuration>**

Built-in default - otherwise use the internal hard-coded default text

The selection is then used for both dialogs. Although you can have multiple XML files for different regions and languages, you cannot use multiple files to independently configure either dialog. The first XML file which is considered applicable will always be used, to the exclusion of any other files. If the selected XML file has partial customization, the built-in default text will be used for the omitted elements.

The example XML below is a full customization of the text in both dialogs for the locale **de-at**.

```
<?xml version="1.0" encoding="utf-8"?>
<configuration xml:lang="de-at">
  <dialogResourceStrings>
    <mainDialog>
      <title><![CDATA[Vermögensverwaltung(de-at)]]></title>
      <instructions>
        <![CDATA[
        Lieber Kollege,

        Im Rahmen eines Kostensenkungsmaßnahme, die IT-Abteilung hat die Softwa
renutzung innerhalb der Organisation mit dem Ziel, die Entdeckung teure Lizenze
n, die nicht verwendet werden untersucht. Wenn wir in der Lage, alle identifizi
erten Lizenzen zurückfordern, dann wird dies sehr deutliche Kosteneinsparungen
über die nächsten 3 Jahre zu liefern.

        Die folgenden Anwendungen werden nicht angezeigt, bis vor kurzem verwen
det haben:
      ]]></instructions>
      <footnote><![CDATA[
        Wenn Sie keine Folge mit dieser Software sind, bitte klicken Sie auf di
e <Entfernen-Software> -Taste.

        Kind Regards,
        IT Department
      ]]></footnote>
      <button1><![CDATA[Entfernen Sie die software]]></button1>
      <button2><![CDATA[Entfernen Sie die Software später]]></button2>
```

```
      <header1><![CDATA[Namen]]></header1>
      <header2><![CDATA[Kosten]]></header2>
      <header3><![CDATA[Zuletzt vervendet]]></header3>
      <unknown><![CDATA[Unbekant]]></unknown>
      <overOneYearAgo><![CDATA[vor mehr als ein Jahr]]></overOneYearAgo>
      <overNYearsAgo><![CDATA[vor mehr als %d Jahre]]></overNYearsAgo>
      <overOneMonthAgo><![CDATA[vor mehr als 1 Monat]]></overOneMonthAgo>
      <overNMonthsAgo><![CDATA[Vor über %d Monaten]]></overNMonthsAgo>
      <overOneWeekAgo><![CDATA[mehr als vor einer Woche]]></overOneWeekAgo>
      <overNWeeksAgo><![CDATA[mehr als %d Wochen]]></overNWeeksAgo>
      <yesterday><![CDATA[gestern]]></yesterday>
      <overNDaysAgo><![CDATA[Vor über %d Tage]]></overNDaysAgo>
      <today><![CDATA[heute]]></today>
      <stillNeeded><![CDATA[Ich muss noch diese]]></stillNeeded>
    </mainDialog>
    <confDialog>
      <title><![CDATA[Bestätigen Sie Software verwenden]]></title>
      <instructions><![CDATA[
        Bitte geben Sie eine Nachricht (max. 140 Zeichen), das anzeigt, warum S
ie noch brauchen, um diese Software zu nutzen. Diese Informationen werden gesam
melt, um ein besseres Verständnis für die Software-Anforderungen unserer Organi
sation zu gewinnen.
      ]]></instructions>
      <button1><![CDATA[OK]]></button1>
      <button2><![CDATA[Stornieren]]></button2>
    </confDialog>
  </dialogResourceStrings>

  <appSettings>
    <appClarityReclaimerServiceUrl>http://%ACSERVERNAME%:8335/appclarity/servic
es/softwareReclaimer/</appClarityReclaimerServiceUrl>
    <activeEfficiencyUrl>http://%AESERVERNAME%/ActiveEfficiency</activeEfficien
cyUrl>
  </appSettings>
</configuration>
```

10.3.5.7 Demo mode

Demo mode allows you to run the Software Reclaimer dialogs without the need for a server or policies, so that you can:

simply demonstrate what it looks like out of the box

validate customizations, including logo, text and locale, as described Customizing the dialogs.

Note

Demo mode does not test connection to the server, nor does it test reclaim policies.

If not using demo mode, you would need all the following in order to demonstrate or test the Reclaimer optout dialog.

Full SLA Platform infrastructure installed and working, with a Configuration Manager connector

Applications installed on your test machine

Optional policies configured that match your test machine.

The following is a way that you can run the Reclaimer as many times as you want using optout mode without requiring policies or affecting anything already configured.

Download **AppClarity.SoftwareReclaimer.Demo.xml**

Make modifications to the **OptionalUninstall** applications

You can specify from 1 up to 3 applications.

Copy the following into a test folder on your computer

AppClarity.SoftwareReclaimer.exe

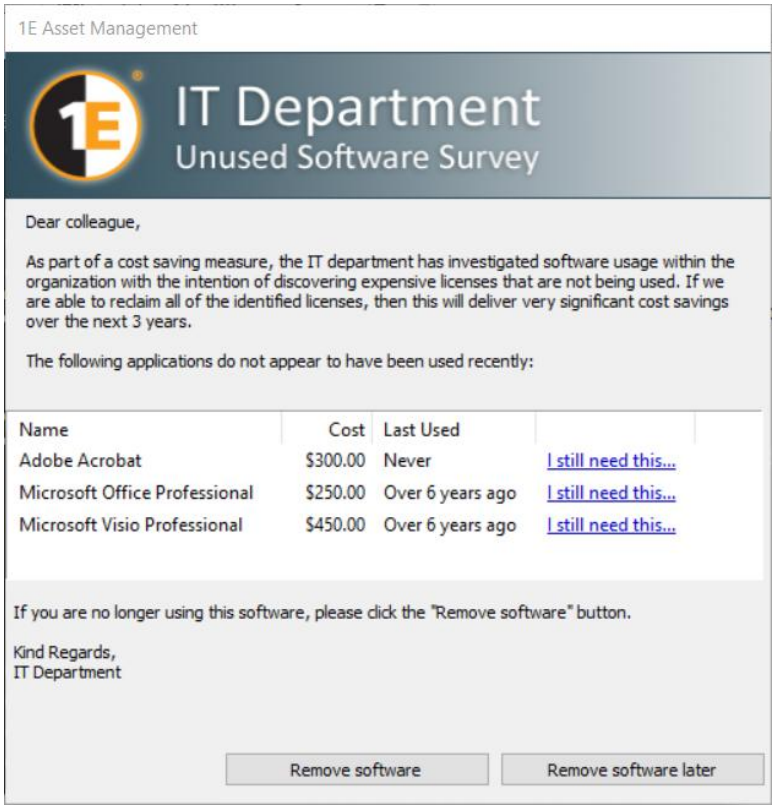
Your copy of **AppClarity.SoftwareReclaimer.Demo.xml**

Any custom XML files and logo.png that you wish to test.

From a command prompt run the following:

```
AppClarity.SoftwareReclaimer.exe -mode OPTOUT -nowait
```

The dialog is displayed showing the optional uninstall applications, with a new logo and customized dialog text from other custom XML files



Click on **I still need this...** to show the second dialog with its text customization

To close the window select one of the buttons

in demo mode these buttons do not send opt-out responses back to the server

You can then make further changes to your custom XML files, and repeat testing until you are happy with the customizations

When done, copy the custom XML files to your deployment package for deployment testing (do not include the Demo XML file).

Download AppClarity.SoftwareReclaimer.Demo.xml ...

AppClarity.SoftwareReclaimer.Demo.xml Expand source

```
<?xml version="1.0" encoding="utf-8"?>
<OptionalUninstalls>
  <!--
    name is required
    cost is optional
    if lastUsedDate is given, it must be of the form "YYYY-MM-DDTHH:MM:SSZ" (ex
ample: 2011-03-10T10:53:12Z)
    if lastUsedDate is not given, the application will be shown as "never" used
  -->
  <OptionalUninstall name="Adobe Acrobat" cost="$300" />
  <OptionalUninstall name="Microsoft Office Professional" cost="$250" lastUsedD
ate="2011-03-10T10:53:12Z" />
  <OptionalUninstall name="Microsoft Visio Professional" cost="$450" lastUsedDa
te="2011-03-10T10:53:12Z" />
</OptionalUninstalls>
```

Tip

You do not need to specify **-service** in the command line because demo mode does not use the server. Even if specified, the parameter is ignored in demo mode.

For the same reason you do not need to configure the **<appClarityReclaimerServiceUrl>** setting in the **<appSettings>** section of any XML files, or the publicKey for HTTPS.

10.3.5.8 Digital signing certificates

10.3.5.8.1 Certificate limitations - signing certificates missing

On Windows computers, the installation MSI files, and binary executable and DLL files of 1E software are digitally signed. The 1E code signing certificate uses a timestamping certificate as its countersignature. 1E occasionally changes its code signing certificate, and uses it for new releases and patches for older versions, as shown in the table(s) below.

Root Certificate Authorities are implicitly trusted to validate certificates, and their certificates must be correctly installed to do this. Your computers should already have the necessary **root CA** certificates installed, however this may have been prevented by your organization's security policies, or inability to connect to the Internet, or they are legacy OS. In general this is not an issue because by default Windows allows software to be

installed and run without validation, although you may see a warning or experience a delay. However, you *must* have relevant CA certificates installed if you are using 1E Client (which self-validates its own files), or your organization has applied more secure polices (for example UAC, AppLocker or SmartScreen).

Typical reasons for issues with signing certificate are:

If your organization has disabled **Automatic Root Certificates Update** then you must ensure the relevant **root CA** certificates are correctly installed on each computer

If computers do not have access to the Internet then you must ensure the relevant **root and issuing CA** certificates are correctly installed on each computer, numbered in the table(s) below.

The signature algorithm of the 1E code signing certificate is SHA256RSA. In most cases, the file digest algorithm of an authenticode signature is SHA256, and the countersignature is a RFC3161 compliant timestamp. The exception is on legacy OS (Windows XP, Vista, Server 2003 and Server 2008) which require the file digest algorithm of an authenticode signature to be SHA1, and a legacy countersignature.

The table below applies to software and hotfixes released in 2020.

2020	**Signing certificate**	**Timestamping certificates**
Certificate	1E Limited	TIMESTAMP-SHA256-2019-10-15 ***and*** DigiCert Timestamp Responder
Issuing CA	**DigiCert EV Code Signing CA (SHA2)** Thumbprint: 60ee3fc53d4bdfd1697ae5beae1cab1c0f3ad4e3	**DigiCert SHA2 Assured ID Timestamping CA** Thumbprint: 3ba63a6e4841355772debef9cdcf4d5af353a297 ***and*** **DigiCert Assured ID CA-1** Thumbprint: 19a09b5a36f4dd99727df783c17a51231a56c117
Root CA	**DigiCert High Assurance EV Root CA** Thumbprint: 5fb7ee0633e259dbad0c4c9ae6d38f1a61c7dc25	**DigiCert Assured ID Root CA** Thumbprint: 0563b8630d62d75abbc8ab1e4bdfb5a899b24d43

10.3.5.8.2 Certificate limitations - expired root certificates

Ensure that your Root CA Certificates are up-to-date on clients and servers. The **Automatic Root Certificates Update** feature is enabled by default, but its configuration may have been changed or restricted by Group Policy **Turn off Automatic Root Certificates Update**.

If this GPO is enabled, then you will see *DisableRootAutoUpdate = 1 (dword)* in *HKLM\Software\Policies\Microsoft\SystemCertificates\AuthRoot.*

10.4Using AppClarity

How SAM users use AppClarity to view software inventory and usage, handle software reclaim, manage entitlements and view effective license positions, compliance and calculate license demand.

10.4.1 AppClarity user roles

AppClarity supports Role Based Access Control (RBAC). RBAC allows a Tachyon Administrator to allocate specific AppClarity based roles to different users, thereby enabling access and actions to the screens those users need to carry out their roles. This avoids unwanted access being permitted to SAM team members outside of their role, ensuring data security and improving governance.

There are pre-defined roles with sets of permissions aimed at particular SAM user types. Tachyon Administrators can assign any of these AppClarity based roles to any AD domain user.

Typically you would install AppClarity using the the Tachyon installation account. This role has purposefully limited permissions, but is able to add new Tachyon users and assign roles to those users. So after installing AppClarity one of the first steps would be to add the **AppClarity Administrator** role to an existing or new Tachyon user and then continue with the verification steps to confirm that AppClarity has been successfully installed. Please refer to Verifying for more details.

After the AppClarity installation has been verified you would then have the ongoing task of identifying your SAM users adding them as Tachyon users and assigning their AppClarity roles to allow them to carry out their SAM duties.

> **Note**
>
> AppClarity permissions are granted on a module level (for example, Entitlement, Reclaim or Compliance) and not at per screen level (such as **Entitlement→Summary Report** or **Reclaim→Savings**), for example:

A Tachyon Administrator has a request for a Reclaim Viewer to only view the **Entitlement**→Summary Report.

The Tachyon Administrator assigns the role of **Entitlement Administrator** to the Reclaim Viewer.

The Reclaim Viewer would be able to view all screens under Entitlement module, not just the requested screen, **Entitlement**→Summary Report.

10.4.1.1 Pre-defined AppClarity roles

The pre-defined roles are:

Role	Actions
AppClarity Administrator	Create, update, delete and view AppClarity Compliance, Entitlement, License Demand and Reclaim - view and export Inventory - view, edit, delete and export Associations
Reclaim Administrator	Create, update, delete and view AppClarity Reclaim - view and export Inventory - view, edit, delete and export Associations
Reclaim Viewer	View only AppClarity Reclaims
Entitlement Administrator	Create, update, delete and view AppClarity Entitlement - view and export Inventory - view, edit, delete and export Associations
Compliance Administrator	Create, update, delete and view AppClarity Compliance, Entitlement and License Demand - view AppClarity Reclaim - view and export Inventory - view, edit, delete and export Associations
Compliance Viewer	View only AppClarity Compliance, Entitlement and License Demand

10.4.1.2 AppClarity screen access and actions per role

In this section we will define the screens and actions that each Role will be able to access, and what actions are available, the actual function of each screen and action is detailed in the later pages.

10.4.1.2.1 AppClarity Administrator

This user is not able to assign roles in the settings application

Screen	Actions	View only
Entitlements - Summary Report	Refresh Report	Yes
Entitlements - Licenses / Maintenances	New License, New Maintenance, Edit, Publish, Clone, Move to Draft, Delete, Components, Export, Refresh Report	No
Entitlements - Licenses / Maintenances - Links popup	No actions possible on this screen	Yes

Screen	Actions	View only
Entitlements - Licenses / Maintenances - Vendor popup	No actions possible on this screen	Yes
Entitlements - Licenses / Maintenances - New License	Publish, Save Draft, Cancel	No
Entitlements - Licenses / Maintenances - New Maintenance	Publish, Save Draft, Cancel	No
Entitlements - Licenses / Maintenances - Edit License	Publish, Save Draft, Cancel	No
Entitlements - Licenses / Maintenances - Clone	Publish, Save Draft, Cancel	No
Entitlements - Licenses / Maintenances - Components	No actions possible on this screen	No
Entitlements - Agreements	New Agreement, Edit, Publish, Clone, Move to Draft, Delete, Export, Refresh Report	No
Entitlements - Agreements - Links popup	No actions possible on this screen	Yes
Entitlements - Agreements - New Agreement	Publish, Save Draft, Cancel	No
Entitlements - Agreements - Edit	Publish, Save Draft, Cancel	No
Entitlements - Agreements - Clone	Publish, Save Draft, Cancel	No
Entitlements - Contracts	New Contract, Edit, Delete, Export, Refresh Report	No
Entitlements - Contracts - New Contract	Publish, Save Draft, Cancel	No

Screen	Actions	View only
Entitlements - Contracts - Edit	Save, Cancel	No
Compliance - License Summary	Add License, Add Reclaim Policy, Export, Refresh Report	No
Compliance - License Summary - Summary by Installs (visible by clicking on Compliance Category bar)	Export	No
Compliance - License Summary - Add License	Publish, Save Draft, Cancel	No
Compliance - License Summary - Add Reclaim Policy	Evaluate, Save Draft, Publish, Cancel	No
Compliance - License Position	Export, Compliance Details, Refresh Report	No
License Demand	View Report, Refresh	No
License Demand - Microsoft Core License Demand	Show Detailed Report	No
License Demand - Microsoft Core License Demand - Detailed Report	Export	No
License Demand - IBM Processor Value Unit (PVU) License Demand	Show Detailed Report	No
License Demand - IBM Processor Value Unit (PVU) License Demand - Detailed Report	Export	No
License Demand - Oracle Processor License Demand	Show Detailed Report	No

Screen	Actions	View only
License Demand - Oracle Processor License Demand - Detailed Report	Export	No
License Demand - Red Hat Socket License Demand	Show Detailed Report	No
License Demand - Red Hat Socket License Demand - Detailed Report	Export	No
Reclaim - Usage Summary	Add Policy, Export, Refresh Report	No
Reclaim - Usage Summary - New Policy	Evaluate, Save Draft, Publish, Cancel	No
Reclaim - Reclaim History	Export, Refresh Report	No
Reclaim - Policies	New Policy, Edit, Publish, Clone, Move to Draft, Delete,Manage Associations, Export, Refresh Report	No
Reclaim - Policies - New Policy	Evaluate, Save Draft, Publish, Cancel	No
Reclaim - Policies - Edit Policy	Evaluate, Save Draft, Publish, Cancel	No
Reclaim - Policies - Cloned Policy	Evaluate, Save Draft, Publish, Cancel	No
Reclaim - Policies - Manage Associations	Opens the Inventory - Manage Associations - Product to CM Screen with the Reclaimable filter selected Add Association, Edit Association and Remove Association Buttons are disabled unless a Reclaim has been created	No
Reclaim - Savings	Export, Refresh Report	No

10.4.1.2.2 Reclaim Administrator

This user is not able to assign roles in the settings application

Screen	Actions	View only
Reclaim - Usage Summary	Add Policy, Export, Refresh Report	No
Reclaim - Usage Summary - New Policy	Evaluate, Save Draft, Publish, Cancel	No
Reclaim - Reclaim History	Export, Refresh Report	No
Reclaim - Policies	New Policy, Edit, Publish, Clone, Move to Draft, Delete, Manage Associations, Export, Refresh Report	No
Reclaim - Policies - New Policy	Evaluate, Save Draft, Publish, Cancel	No
Reclaim - Policies - Edit Policy	Evaluate, Save Draft, Publish, Cancel	No
Reclaim - Policies - Cloned Policy	Evaluate, Save Draft, Publish, Cancel	No
Reclaim - Policies - Manage Associations	Opens the Inventory - Manage Associations - Product to CM Screen with the Reclaimable filter selected Add Association, Edit Association and Remove Association Buttons are disabled unless a Reclaim has been created	No
Reclaim - Savings	Export, Refresh Report	No
Compliance - License Summary - Add Reclaim Policy	Add Policy	No

10.4.1.2.3 Reclaim Viewer

This user is not able to assign roles in the settings application

Screen	Actions	View only
Reclaim - Usage Summary	No actions possible on this screen	Yes
Reclaim - Reclaim History	No actions possible on this screen	Yes
Reclaim - Policies	Manage Associations	No
Reclaim - Policies - Manage Associations	Opens the Inventory - Manage Associations - Product to CM Screen with the Reclaimable filter selected No actions possible on this screen	Yes
Reclaim - Savings	No actions possible on this screen	Yes

10.4.1.2.4 Entitlement Administrator

This user is not able to assign roles in the settings application

Screen	Actions	View only
Entitlements - Summary Report	Refresh Report	No
Entitlements - Licenses / Maintenances	New License, New Maintenance, Edit, Publish, Clone, Move to Draft, Delete, Components, Export, Refresh Report	No
Entitlements - Licenses / Maintenances - Links popup	No actions possible on this screen	Yes
Entitlements - Licenses / Maintenances - Vendor popup	No actions possible on this screen	Yes
Entitlements - Licenses / Maintenances - New License	Publish, Save Draft, Cancel	No
Entitlements - Licenses / Maintenances - New Maintenance	Publish, Save Draft, Cancel	No

Screen	Actions	View only
Entitlements - Licenses / Maintenances - Edit License	Publish, Save Draft, Cancel	No
Entitlements - Licenses / Maintenances - Clone	Publish, Save Draft, Cancel	No
Entitlements - Licenses / Maintenances - Components	No actions possible on this screen	No
Entitlements - Agreements	New Agreement, Edit, Publish, Clone, Move to Draft, Delete, Export, Refresh Reports	No
Entitlements - Agreements - Links popup	No actions possible on this screen	Yes
Entitlements - Agreements - New Agreement	Publish, Save Draft, Cancel	No
Entitlements - Agreements - Edit	Publish, Save Draft, Cancel	No
Entitlements - Agreements - Clone	Publish, Save Draft, Cancel	No
Entitlements - Contracts	New Contract, Edit, Delete, Export, Refresh Reports	No
Entitlements - Contracts - New Contract	Save, Cancel	No
Entitlements - Contracts - Edit	Save, Cancel	No

10.4.1.2.5 Compliance Administrator

This user is not able to assign roles in the settings application

Screen	Actions	View only
Entitlements - Summary Report	Refresh Report	No

Screen	Actions	View only
Entitlements - Licenses / Maintenances	New License, New Maintenance, Edit, Publish, Clone, Move to Draft, Delete, Components, Export, Refresh Report	No
Entitlements - Licenses / Maintenances - Links popup	No actions possible on this screen	Yes
Entitlements - Licenses / Maintenances - Vendor popup	No actions possible on this screen	Yes
Entitlements - Licenses / Maintenances - New License	Publish, Save Draft, Cancel	No
Entitlements - Licenses / Maintenances - New Maintenance	Publish, Save Draft, Cancel	No
Entitlements - Licenses / Maintenances - Edit License	Publish, Save Draft, Cancel	No
Entitlements - Licenses / Maintenances - Clone	Publish, Save Draft, Cancel	No
Entitlements - Licenses / Maintenances - Components	No actions possible on this screen	No
Entitlements - Agreements	New Agreement, Edit, Publish, Clone, Move to Draft, Delete, Export, Refresh Report	No
Entitlements - Agreements - Links popup	No actions possible on this screen	Yes
Entitlements - Agreements - New Agreement	Publish, Save Draft, Cancel	No
Entitlements - Agreements - Edit	Publish, Save Draft, Cancel	No

Screen	Actions	View only
Entitlements - Agreements - Clone	Publish, Save Draft, Cancel	No
Entitlements - Contracts	New Contract, Edit, Delete, Export, Refresh Report	No
Entitlements - Contracts - New Contract	Publish, Save Draft, Cancel	No
Entitlements - Contracts - Edit	Save, Cancel	No
Compliance - License Summary	Add License, Add Reclaim Policy, Export, Refresh Report	No
Compliance - License Summary - Summary by Installs (visible by clicking on Compliance Category bar)	Export	No
Compliance - License Summary - Add License	Publish, Save Draft, Cancel	No
Compliance - License Summary - Add Reclaim Policy	Evaluate, Save Draft, Publish, Cancel	No
Compliance - License Position	Export, Compliance Details, Refresh Report	No
License Demand	View Report, Refresh	No
License Demand - Microsoft Core License Demand	Show Detailed Report	No
License Demand - Microsoft Core License Demand - Detailed Report	Export	No
License Demand - IBM Processor Value Unit (PVU) License Demand	Show Detailed Report	No

Screen	Actions	View only
License Demand - IBM Processor Value Unit (PVU) License Demand - Detailed Report	Export	No
License Demand - Oracle Processor License Demand	Show Detailed Report	No
License Demand - Oracle Processor License Demand - Detailed Report	Export	No
License Demand - Red Hat Socket License Demand	Show Detailed Report	No
License Demand - Red Hat Socket License Demand - Detailed Report	Export	No
Reclaim - Usage Summary	No actions possible on this screen	Yes
Reclaim - Reclaim History	No actions possible on this screen	Yes
Reclaim - Policies	Manage Associations	No
Reclaim - Policies - Manage Associations	Opens the Inventory - Manage Associations - Product to CM Screen with the Reclaimable filter selected Add Association, Edit Association and Remove Association Buttons are disabled unless a Reclaim has been created	No
Inventory - Manage Associations - Product to CM	Add Association, Edit Association, Remove Association	No
Reclaim - Savings	No actions possible on this screen	Yes

10.4.1.2.6 Compliance Viewer

This user is not able to assign roles in the settings application

Screen	Actions	View only
Entitlements - Summary Report	No actions possible on this screen	Yes
Entitlements - Licenses / Maintenances	No actions possible on this screen	Yes
Entitlements - Licenses / Maintenances - Links popup	No actions possible on this screen	Yes
Entitlements - Licenses / Maintenances - Vendor popup	No actions possible on this screen	Yes
Entitlements - Agreements	No actions possible on this screen	Yes
Entitlements - Agreements - Links popup	No actions possible on this screen	Yes
Entitlements - Contracts	No actions possible on this screen	Yes
Compliance - License Summary	No actions possible on this screen	Yes
Compliance - License Summary - Summary by Installs (visible by clicking on Compliance Category bar)	No actions possible on this screen	Yes
Compliance - License Position	No actions possible on this screen	Yes
License Demand	View Report	No
License Demand - Microsoft Core License Demand	No actions possible on this screen	Yes
License Demand - IBM Processor Value Unit (PVU) License Demand	No actions possible on this screen	Yes

Screen	Actions	View only
License Demand - Oracle Processor License Demand	No actions possible on this screen	Yes
License Demand - Red Hat Socket License Demand	No actions possible on this screen	Yes

10.4.2 Running your first Compliance License Summary

The first time you start AppClarity it's advisable and helpful to start with viewing the **License Summary** for the situation where you have no entitlements defined in the selected compliance repository, refer to the Repositories page for more information.

This gives you an established baseline to work with, where you can see what AppClarity is reporting to you without involving entitlements. It also lets you get familiar with the way that the information gets into the **License Summary** for a particular compliance repository.

10.4.2.1 Default repositories and permissions needed

The compliance screens in AppClarity rely on selecting a compliance repository that has been associated to both entitlement and inventory repositories. When you installed AppClarity, this created two new default repositories in **Settings**→Configuration→Repositories to add to the existing default inventory making three:

Default Inventory.

Default Entitlement.

Default Compliance.

To run a Compliance Report, an AppClarity user must have any of the following roles:

Full Administrator

AppClarity Administrator

Compliance Administrator.

Logged-in users with any of the following roles can view the **AppClarity→Compliance→License Summary** screen:

Full Administrator

AppClarity Administrator

Compliance Administrator

Compliance Viewer.

10.4.2.2 Associating the default repositories

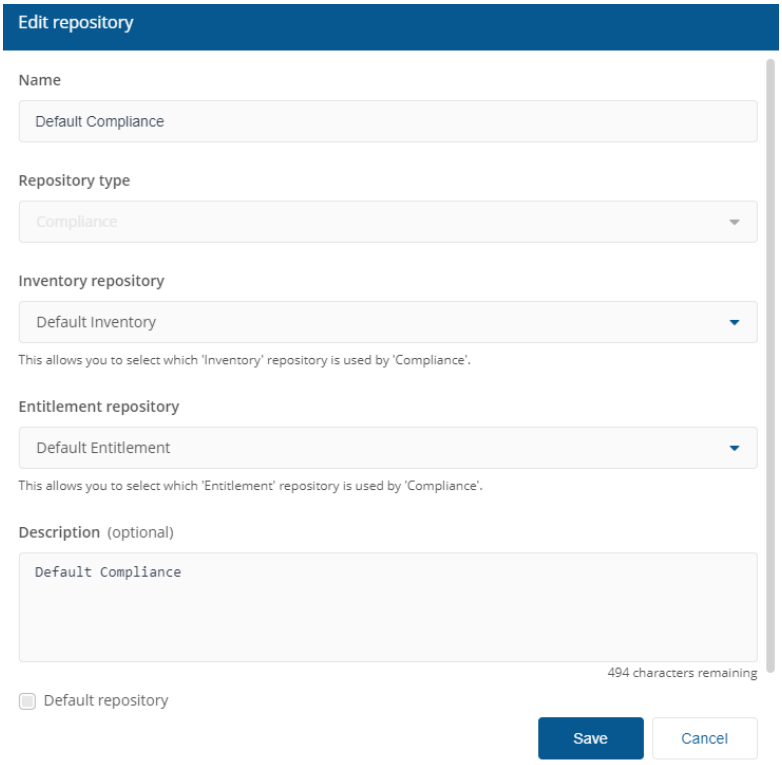
The first time you browse to the AppClarity pages the only repositories available are the default ones. To run the **AppClarity→ Compliance→License Summary** you will use the **Default Compliance** repository, it will already be associated with the **Default Inventory** but you'll also need to associate it with the **Default Entitlement** repository. Switch to **Settings→Configuration→Repositories**:

Check the checkbox for the **Default Compliance** repository, and click **Edit**.

Once the **Default Compliance repository** opens in edit mode, select the **Default Inventory** and **Default Entitlement** repositories.

Optionally enter a description.

Click **Save**.



10.4.2.3 Viewing the Compliance License Position

Before viewing the Compliance License Position, ensure **License Demand Compliance (LDC)** reports for Microsoft Core, Oracle Processor, IBM PVU and RedHat Socket have been refreshed.

To run and view License Demand Compliance (LDC) reports :

Switch to **AppClarity→License Demand**.

On the **License Demand Calculation Report** screen, select your compliance repository from the dropdown list.

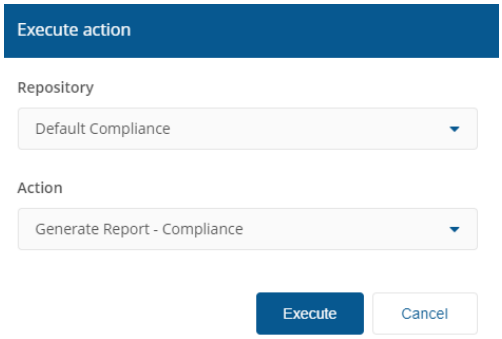
Click **Refresh** for each report.

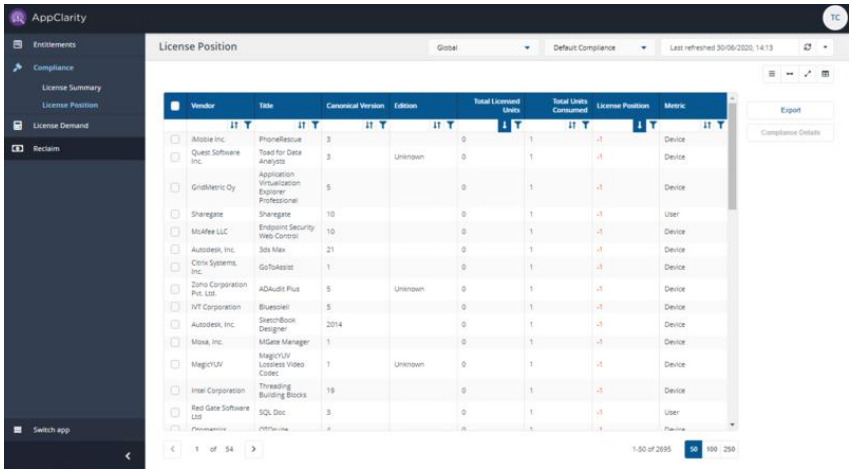
Once the report refresh shows as complete, click **View Report**.

When you have refreshed the LDC reports, refresh the Compliance Report and view License Position for Compliance using the **Refresh reports** icon on the top right of the page.

The screen should now display the information derived from the reports we just refreshed. Here we can see entries for each product, including the **Vendor**, **Title** and **Edition** and the most significant value, which is in the **License Position** column.

This shows the status of the licenses for each of those products, as there are no entitlements defined, they'll show negative values. The numbers indicate how many licenses are needed in order to make that product compliant. The **License Metric** column at the end of the row shows how the licenses are calculated, either by **Device**, **User**, **Core** or by **Processor**.





10.4.2.4 Viewing Compliance License details

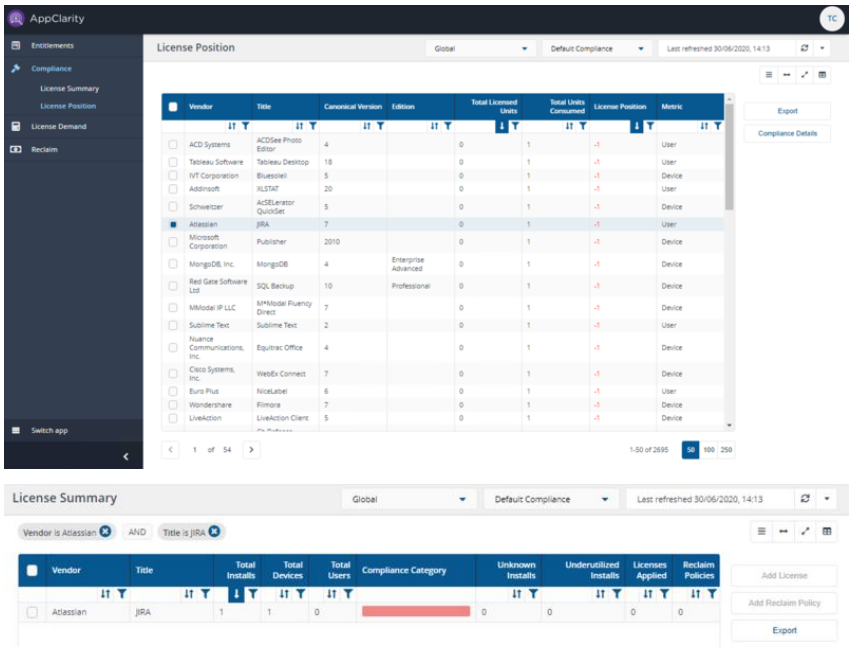
To view the **Compliance Details** for any of the products displayed:

On the **License Postion** page check the checkbox one or more products and click **Compliance Details**.

The License Summary for the selected product or products. From here you can further explore the **Compliance Category** for a particular product by clicking on the colored **Compliance Category** bar.

In the License Summary by Installs, you can review the license position for that software and filter a detailed table, for example by **Status**, **Machine Name** or by **Primary User**.

You've just created your first report in AppClarity and had a quick glance at your compliance position, without any entitlements set, showing what types of software are installed in your network and how many licenses must be created in order to make that software compliant.



Note

The Effective License Position (ELP) shows details for the installation title for product titles where they differ, for example:

SQL Server Master Data Services, SQL Server Data Quality Services, SQL Server Integration Services etc. - mapping with the demand for SQL Server

RedHat Linux Server installation on VMs - mapped with demand of RedHat Enterprise Linux for Virtual Datacenters.

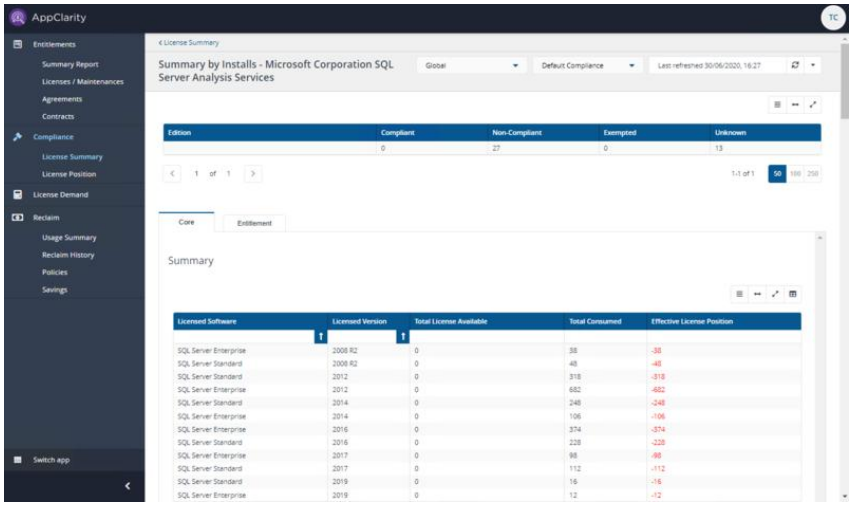
In the example shown, the **License Summary** page has been filtered to show results with the title, SQL Server Analysis Services (SSAS), then clicking on **Compliance Category** color bar for SSASshows the ELP for this product. SSAS is now matched with mapped with SQL Server, this means the complete ELP position is shown for SQL Server.

In addition, the ELP for the licensed and mapped titles remain the same for a given Management Group, for example:

If there are 100 installs of SSAS in the Global Management Group and 10 in Management Group 1

100 installs of SQL Server in Global and 70 in Management Group 1.

A selection of either SSAS or SQL Server would show a license position of SQL Server for Management Group 1 based on the combined 70 installs of SQL Server and 10 of SSAS.



10.4.2.5 Refreshing reports for your repositories

You can refresh reports from individual AppClarity screens, as well as using the Settings App, by using the refresh icon next to the **Last Refreshed** box:

Clicking the dropdown icon next to the refresh icon shows you the last report that was run, a link to the **Settings→Monitoring→Process Log** and a **Status**:

Green tick - indicates a successful refresh

Triangle exclamation - indicates a failed refresh.

You can refresh reports from the following pages:

Title page	Sub-Page	Report
Entitlements	Entitlement Summary	Entitlement Consolidation
License / Maintenance	Entitlement Consolidation	
Agreement	Entitlement Consolidation	
Contract	Entitlement Consolidation	
Compliance	License Summary	Compliance
Compliance Summary by Installs	Compliance	

Title page	Sub-Page	Report
License Position	Compliance	
License Demand	License Demand Calculation Summary report - first page	License Demand Calculation report
License Demand - Detailed Report	License Demand Calculation report	
Reclaim	Usage Summary	Reclaim Product Usage
Reclaim History	Reclaim Reporting	
Policies	Reclaim Consolidation	
Savings	Reclaim Reporting	

10.4.2.5.1 Refresh reports using Settings

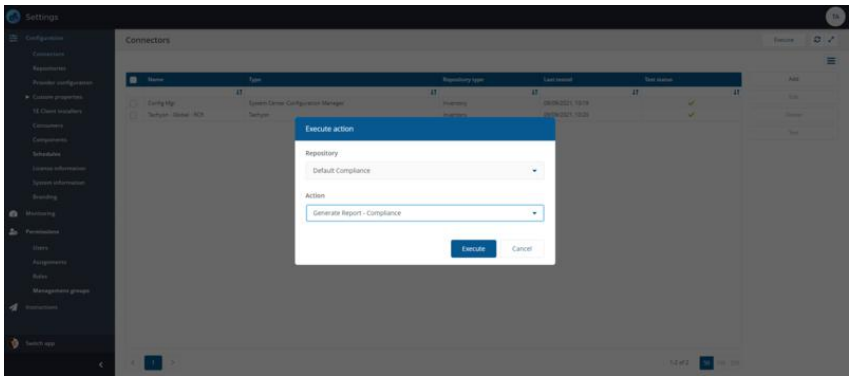
You can also refresh reports using the **Settings** app, for example:

Switch to **Settings**→**Configuration**→**Connectors** and click **Execute**.

In the **Execute action** popup from **Repository** select **Default Compliance** and **Action** as **Generate Report - Compliance**, and click **Execute**.

To monitor the progress of the new action navigate to **Settings**→**Monitoring**→**Process log** to view the **Generate Report** action running.

When the **Generate Report** action has completed, switch app to **AppClarity**→**Compliance**→**License Position**.



10.4.2.5.2 Scheduling a report refresh for a repository

Toautomaticallyrefresh a report for a repository you can set up a schedule:

Under the **Settings**→Configuration→Schedules and click **Add**.

In the Add schedule screen for:

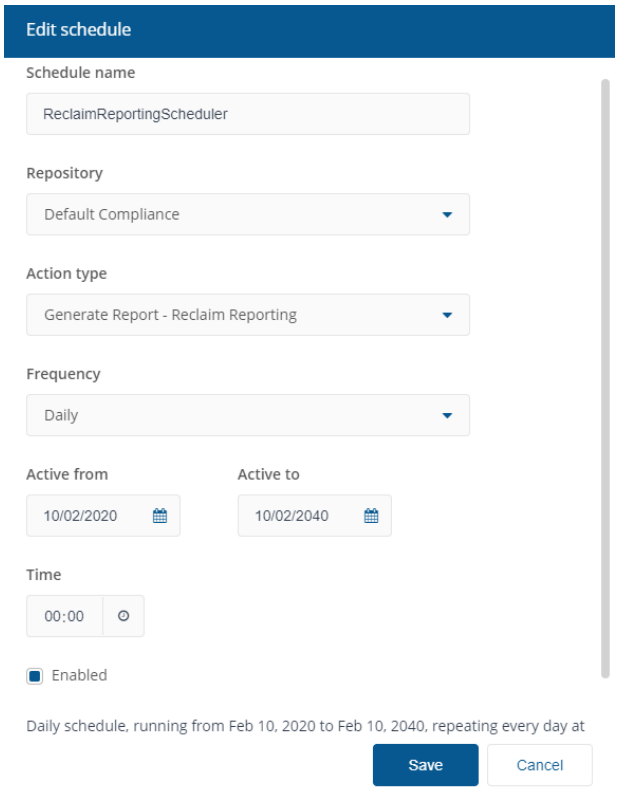
Schedule name - enter a logical name for the new schedule.

Repository - select your repository from the dropdown menu.

Action type - select the associated action type you want to schedule.

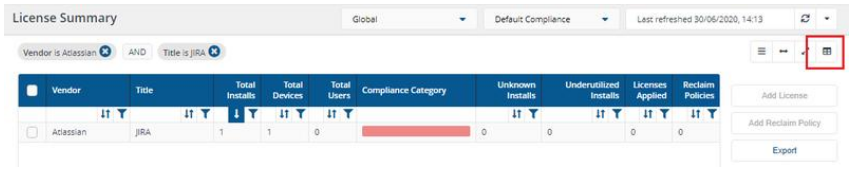
Frequency - select the frequency.

> **Note**
>
> For any entitlement repository, when a new entitlement is created (which triggers an entitlement consolidation) a **Schedule** called **EntitlementConsolidationScheduler** is created for this repository by default, it's set to run on a 24 hrs frequency (daily basis).



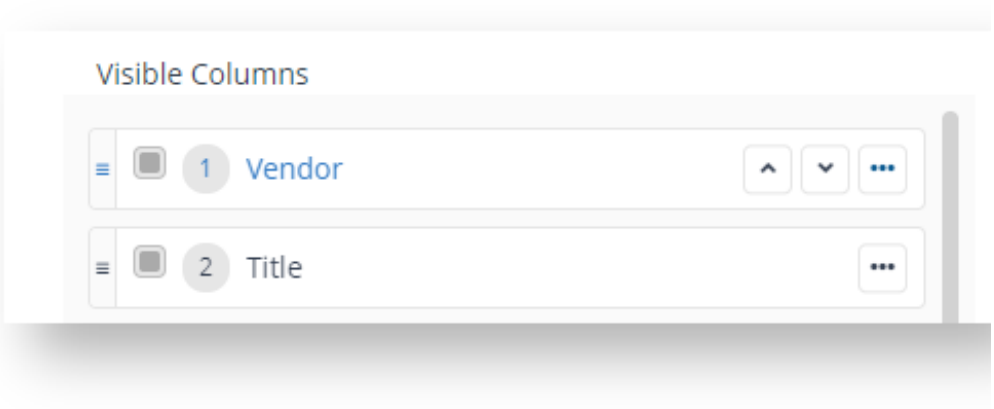
10.4.2.6 Choosing the columns displayed in reports

You can choose which columns are displayed in AppClarity detail tables to increase readability. On the pages where you can pick the displayed columns you'll see the control highlighted in the example.



When you click on the **Choose columns** control it opens a popup displaying every column on the current screen, the controls are:

Control	Explanation
Available Columns	Columns which are by default hidden from display on screen. You can still include any of them to display on screen.
Visible Columns	Displays the list of columns displayed on screen. Mandatory Columns cannot be excluded, the selection controls for these items are disabled. They can still be moved up or down. **Tip** Some pages have mandatory columns and a set of default hidden columns.
Arrow buttons	To move up or move down, exclude or include any column, clicking on the ellipsis displays these additional controls.
Drag and drop	You can drag and drop columns to change how they are displayed.
Exclude columns	Exclude column button allows you to select columns to exclude from the current display.



For example, in Viewing License Compliance Details we viewed the**License Summary**, using the **Choose columns** control you can pick which columns are displayed in the table. On this page, the default columns are:

Vendor

Title

Total Installs

Total Devices

Total Users

Compliance Category

Unknown Installs

Underutilized Installs

Licenses Applied

Reclaim Policies.

Each page also has some mandatory columns which cannot be excluded from display. When you click the **Choose columns** icon the excluded columns are greyed out and cannot be removed.

For example, in License Summary you cannot remove these columns:

Vendor

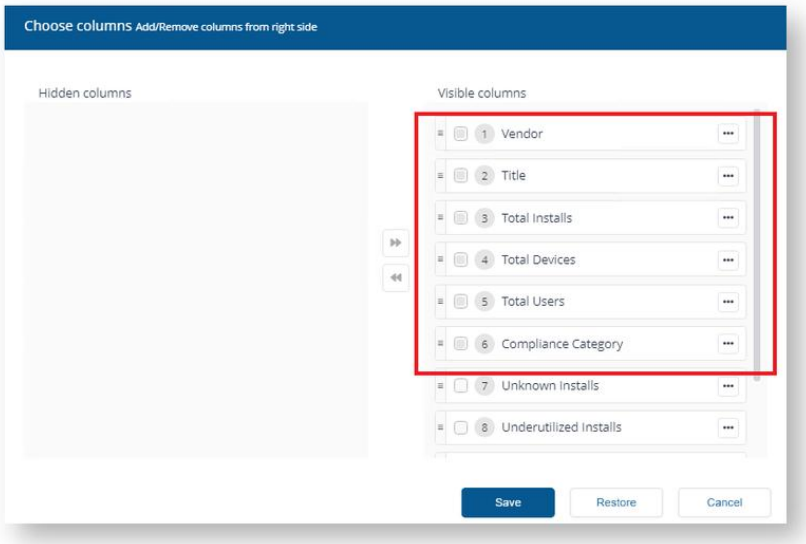
Title

Total Installs

Total Devices

Total Users

Compliance Category



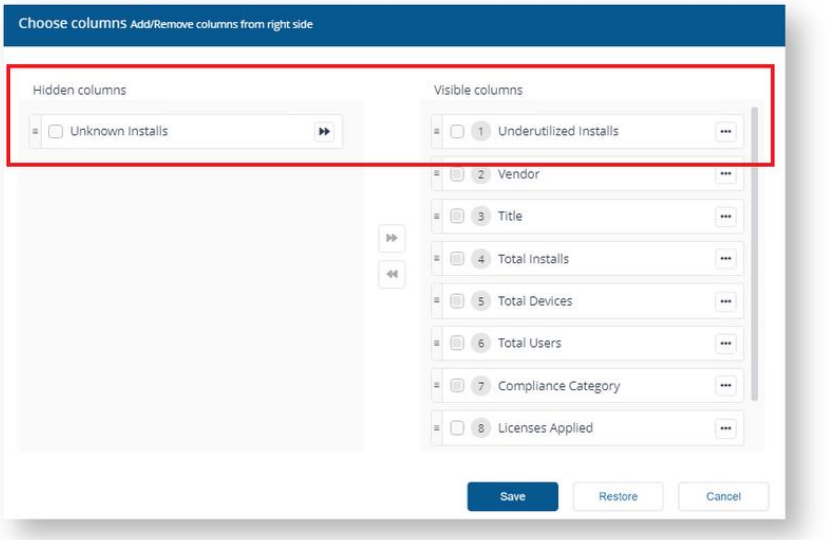
From this screen we chose to exclude **Unknown Installs** and move **Underutilized Installs** to the top of the list.

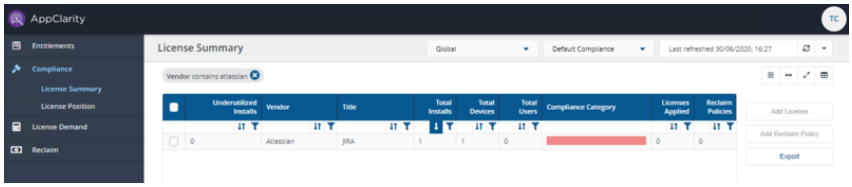
To apply this view to the current report, click **Save**.

You can also choose **Restore** to reset the column chooser UI or **Cancel** to cancel your changes and exit the **Choose columns** control.

Note

When you refresh reports on a page where you have amended the displayed columns, the report view will reset back to its default view once the refresh completes and the page reloads.





10.4.3 Viewing software install counts across all devices

The AppClarity reports are fundamentally based on inventory provided by Tachyon. The inventory shows what software is installed on what devices. If you're a user interested in the software reclaimer aspects of AppClarity you can focus on the software you want to reclaim. Or, if you're a S AM user interested in license compliance, you can focus on the software you want to be compliant on.

To view software install counts across all devices you can use the inventory **by Product** and **by Device** screens, which are both accessible using the Inventory app, to focus on the software and devices you are interested in.

You can view software installation counts using two screens in the Inventory app by using **Switch app** to navigate to **Inventory→SLA Inventory** and using the following two screens:

By Product - shows the inventory organized according to the software titles installed in your enterprise

By Device - shows the inventory organized according to the devices in your enterprise.

10.4.3.1 Using the Inventory By Product screen

Navigate to **Switch apps→Inventory→SLA Inventory→ By Product**

This displays the **Products By Vendor** screen. This screen shows:

A bar showing the distribution of **Licensable** (orange) and **Non licensable** (green) products

A chart showing the top 5 **Vendors by product count**, that is the vendors who sell the most installed products on your enterprise, divided into vendors according to their licensable and non-licensable installed products

A chart showing the top 5 **Products by edition count**, that is the product titles that have the most installed editions on your enterprise, divided into licensable and non-licensable installed titles

A chart showing the top 5 **Product editions by install**, that is the editions that have the most installations on your enterprise, divided into licensable and non-licensable installed editions

> Each of the blocks of color in bar at the top, the **Vendors by product count** and **Products by edition count** charts is an interactive filter that filters all the other components on the screen

For example, clicking on the licensable block of color on the bar at the top filters the three charts to show the top 5 licensable installed products and editions. Notice how the **FILTER BY** field now displays a **License Required Equals true** filter.

Clicking on one of the vendors displayed in the **Vendors by product count** chart filters the screen to just display information related to that vendor. In our example we click on the **Microsoft Corporation** vendor and the **FILTER BY** field now shows **License Required Equals true AND Vendor Equals Microsoft Corporation** filters.

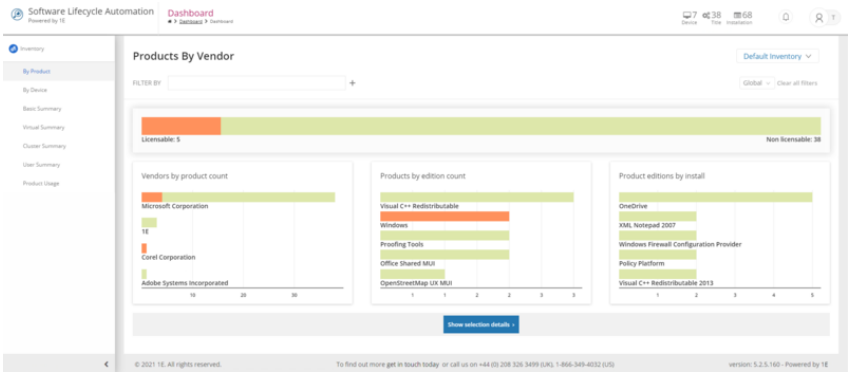
Clicking on one of the products displayed in the **Products by edition count** chart filters the screen to just display information related to that product. In our example we click on **Office 365** and a filter for that also gets added to the **FILTER BY** field.

The **Product editions by install** chart works slightly differently. Clicking on one of the licensable editions, instead of just adding a new filter to the page, it displays the **Product Details** for that installed edition. In our example we click on the **Office 365 ProPlus** edition and the screen changes to a table with the details for **Office 365** displayed. The columns displayed on this screen are described in the following table:

Column heading	Description
Vendor	The vendor who sells the installed software title. For example **Microsoft Corporation** is the vendor for **Office 365**.
Title	The title name for the installed software title. For example the title for Microsoft Office 365 can be **Office 365**.
Colloquial Version	Any associated informal name for the version of the installed software title. For example the Colloquial Version for Microsoft Office 365 could be **2016**.
Edition	The specific edition of the installed software title. For example the Edition for Microsoft Office 365 could be **ProPlus**.
Version	The specific version for the installed software title. For example the specific version for Microsoft Office 365 could be **16.0.10228.20080**.

Host	The host where the software title is installed. For example **Acme-win1002**.
Host Computer Name	The computer name for the host where the software title is installed.
Computer Type	The type of the computer where the software title is installed. For example **Workstation**, **Server** or **Virtual Machine**.
OS	The Operating System where the software title is installed. For example **Windows 10 Pro**.

The **Host** column contains a link to the device where the software title is installed. Clicking on the link displays the details for the host machine with a table showing all the software titles installed on that machine, as well as highlighting above the table the host's OS, machine type and how many processors it has.



10.4.3.2 Using the Inventory By Device screen

Navigate to **Switch apps**→**Inventory**→**SLA Inventory**→ **By Device**

This displays the **Products By Device** screen. The columns on this screen are described in the following table:

Column heading	Description
Host Name	The name for the device. This is a link that navigates to the Product Details table for the selected device.
Last Inventory Date	The date when inventory information was lastreturned for the device.
Computer Type	The type of the device. For example **Workstation**, **Desktop**, **Laptop**, **Server** or **Virtual Machine** etc.
Device Model	The model for the device. For example: **Virtual Machine**, **Surface Pro 3**, **Optiplex 910** etc.

OS	The Operating System installed on the device. For example **Windows 10 Pro**.
Number of Unnormalized Software Records	The number of unnormalized software records associated with the device, i.e. the number of installed software titles on the device that couldn't be automatically matched by 1E Catalog. This is formatted as a link, click to match the records to the catalog.
Number of Normalized Software Records	The number of normalized software records associated with the device, i.e. the number of software titles installed on the device that were matched by 1E Catalog.

You can filter the devices displayed in the table by clicking the **+** at the end of the **FILTER BY** field.

The filter builder contains three sections:

The FIELD section, where you specify what column you want to filter on

The OPERATOR section, where you specify the comparison you want to make

The VALUE section, where you specify the value you want to compare the column against

In our example we set:

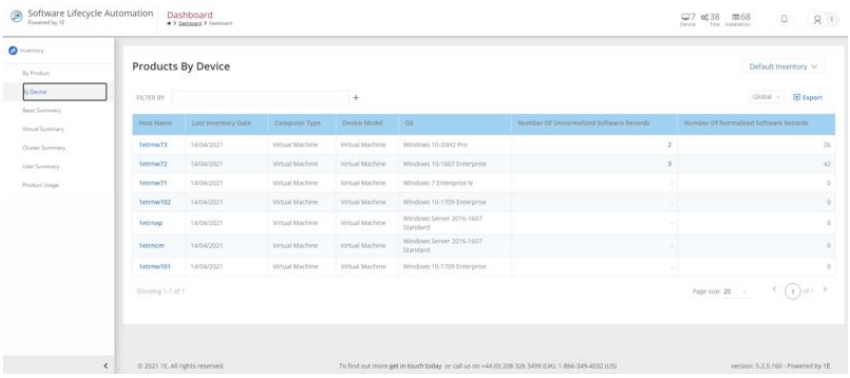
FIELD to Host Name

OPERATOR to Contains

VALUE to win10

This will filter the table to only show devices with **win10** in their host name.

Clicking on the link in the **Host Name** column for any device navigates to the **Product Details** table for that device. Where you can see the same information for the device as shown when navigating via the **By Product** screen.



10.4.4 Viewing product usage

The inventory information retrieved by Inventory from sources such as Configuration Manager and Tachyon includes data on how often products are being used on particular devices. If you're a user interested in the software reclaimer aspects of AppClarity you can focus on reclaiming software based on its usage. There are two ways of viewing product usage in AppClarity:

To view product usage information across all servers and workstations in your network switch to**Inventory**→**SLA Inventory**and then **Inventory**→ **ProductUsage**to investigate the products you are interested in.

To view usage information for reclaimable software, i.e. software installed on workstations not on servers, switch to**AppClarity**→**Reclaim**→**Usage Summary**. By default, that page also contains a filter to show licensable products only, but you can remove that if you're interested in reclaiming any type of software on workstations.

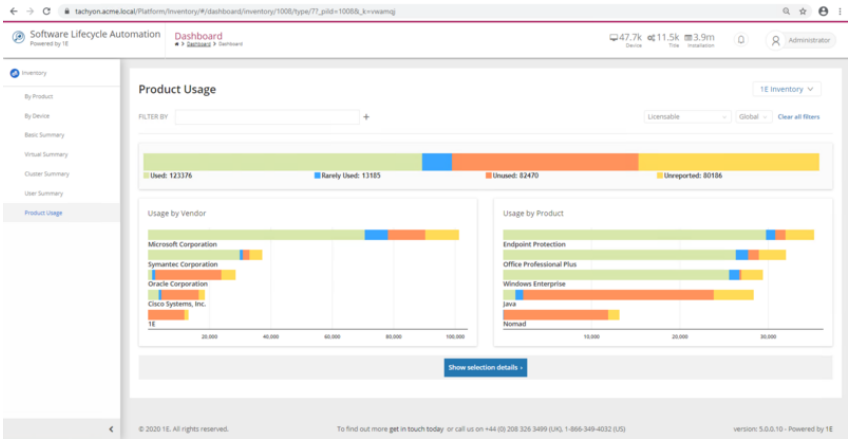
> **Note**
>
> The reclaimer does not work on server OS. From AppClarity 7.1 software reclaimer works for any device where Server OS does not contain "Server" (ie. only client OS) or Server OS is not NULL. Other types of device are removed from the reclaim reports.

Product usage information is reported through the inventory repository when connected to a Microsoft System Center Configuration Manager or Tachyon data source. If you're interested in the possibilities of reclaiming unused software and thereby reducing license waste and costs, AppClarity provides a way of navigating the products installed on your system and seeing how much they are being used. These investigations can then be used as the basis for defining reclaim policies that will target the right software.

There are two views on product usage. One is in Inventory and the other, geared more towards software reclaim, is in AppClarity.

10.4.4.1 Inventory Product Usage page

Switch to **Inventory**→**SLA Inventory**→**Product Usage** . This page displays usage information on both Servers and Workstations.



Here you'll see three charts displaying products organized according to their usage categories. The main chart that spans the width of the page displays the overall usage categories and the counts of software in each.

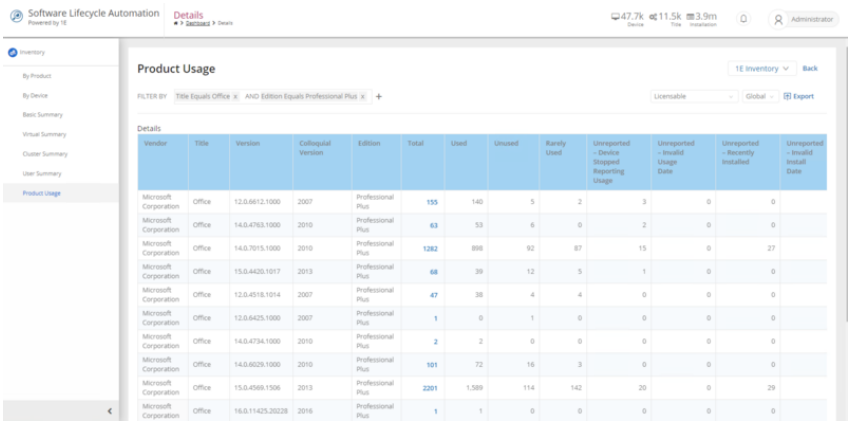
The **Usage by Vendor** chart on the left shows the vendors that have the most installed products in the environment. For example, **Microsoft Corporation**, **Symantec Corporation** and **Oracle Corporation**.

The **Usage by Product** chart on the right displays the top five products with the most installations. In our example **Endpoint Protection**, **Office Professional Plus**, **Windows Enterprise, Java** and **Nomad**.

Hovering over one of the color blocks in the chart displays information for that usage type. For example the blue color block on the **Office Professional Plus** product shows that there are **1394** rarely used installations the red color block for that product shows that there are **1204** unused installations of **Office Professional Plus**.

Clicking on a block in the **Usage by Product** chart drills down to the details for that particular product. In our example by clicking on a block in the **Office Professional Plus** product.

Doing this displays the **Product Usage** table for that product. Here you can see the vendor, title, version, colloquial version and edition for the product alongside a total that shows the number of installations for the product. There are also four columns for each of the usage categories. In our example **Office Professional Plus** version 12.0.6612.1000 has **155**installations, **5** of which are unused and **2** are rarely used.



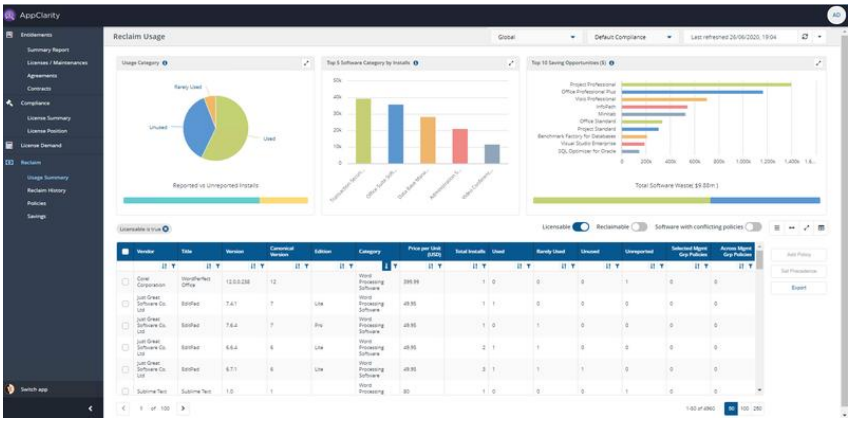
The total column contains a link that, when clicked, displays the **Product Details** table for the product's installations. In our example we can see that this version of **Office Professional Plus** is installed on **162** computers. This will be significant later when we compare the **Inventory Product Usage** page with the **AppClarity Product Usage** page.

Clicking on the name for a device displays detailed information and all the installations for that device.

We then click **Back** a few times to return to the top-level **Inventory Product Usage** page. Fix the totals on this page in your mind to compare them with the **AppClarity Product Usage** page. In our example there are **140** used, **2** rarely used, **5** unused products.

10.4.4.1.1 AppClarity Usage Summary page

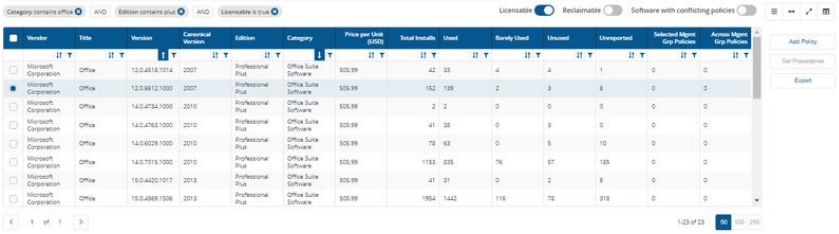
Switch to **AppClarity→Reclaim→Usage Summary**. There's a filter set by default only showing information for the selected management group and only products which are licensable.



This page also displays**Usage Category and Reported Vs UnReported Installs**, **Top 5 Software Category by Installs** and **Top 10 Saving Opportunities ($) and Total Software Waste** charts and a table showing vendor, title, version, colloquial version and edition for the product alongside a total that shows the number of installations for the product. There are also four columns for each of the usage categories **Used**, **Rarely Used**, **Unused** and **Unreported**.

To filter the table by **Usage Category**, **Top 5 Software Category by Installs** or byTop 10 Saving Opportunities click on the color bar for the category you're interested in, for example in our case there's 1,711 records in **Unused** software in **Usage Category.**

In our example let's investigate **Office Professional Plus** for example you could do this by filtering the table view by **Category** containing **Office** and by **Edition** containing **Plus** or if you know the version, by filtering on **Version**.



Now notice how there are different values for the usage categories. In our example on this page there are 139 **Used**, 2 **Rarely Used**, 3 **Unused** products. The difference between the two pages is down to the fact that this page displays just the reclaimable software, i.e. the software installed on workstations, and is filtered to display only licensable software on those workstations, whereas the **Inventory→SLA Inventory→Product Usage** page showed all the software installed on both workstations and servers.

In our example this shows us 3 prime candidates for reclaiming **Office Professional Plus**. To find out how you can reclaim these, refer to Reclaiming a product based on its usage.

In this example we've investigated product usage data and seen the differences between the **SLA Inventory Product Usage** and **AppClarity Product Usage** pages. We've also seen how we can focus on a particular product and investigate its rarely used and unused installations.

> **Note**
>
> You can change the default displayed currency from USD to a currency of your choice, refer to Changing the default currency in AppClarity for details.

10.4.5 Viewing product compliance

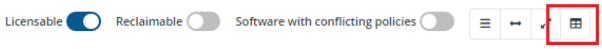
You can view your compliance position focusing on the products installed on your system. From here you can also add entitlements for a specific product.

> **Note**
>
> Before viewing the Compliance → License Summary, please ensure that License Demand reports for SQL Core, IBM PVU, Oracle Processor and RedHat Socket has been successfully refreshed for the Default Compliance repository.

This example assumes that you have associated your chosen compliance repository with your chosen entitlement repository, this example uses **Default Compliance** and **Default Entitlement** and you have run the **Compliance** report on your chosen compliance repository.

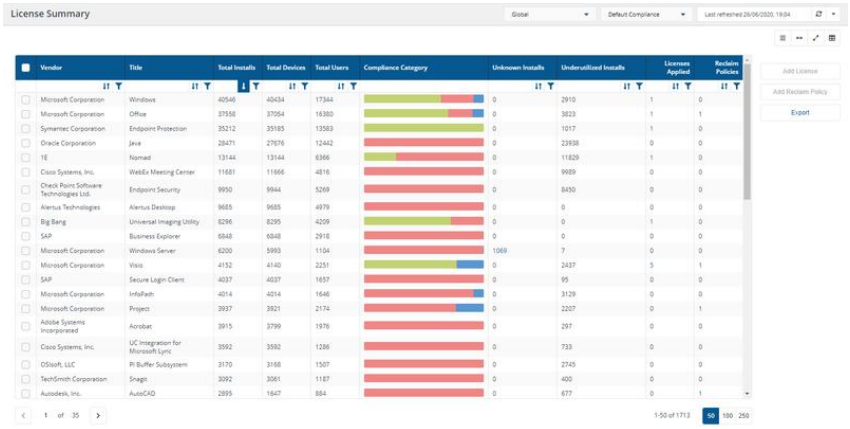
Please refer to Running your first Compliance License Summary for steps that show how to do this.

To view product compliance and interact with the products to create new licenses and improve your compliance:

> **Note**
>
> You can choose which columns are displayed in Inventory and AppClarity detail tables to increase readability. On pages where you can pick the displayed columns you'll see a new control like the one highlighted below:
>
> 
>
>
> To find out more about this feature refer to Running your first Compliance License Summary: Choosing the columns to display in reports.

Navigate to **AppClarity→Compliance→License Summary**. Here you'll see a summary of your compliance position. The displayed table shows compliance information about all your products.

This displays the License Summary page, for more details on the fields on this page please refer to License Summary page.



Following a defaulter install, there are no entitlements so all the products are showing as red in the **Compliance Category** because they're non-compliant.

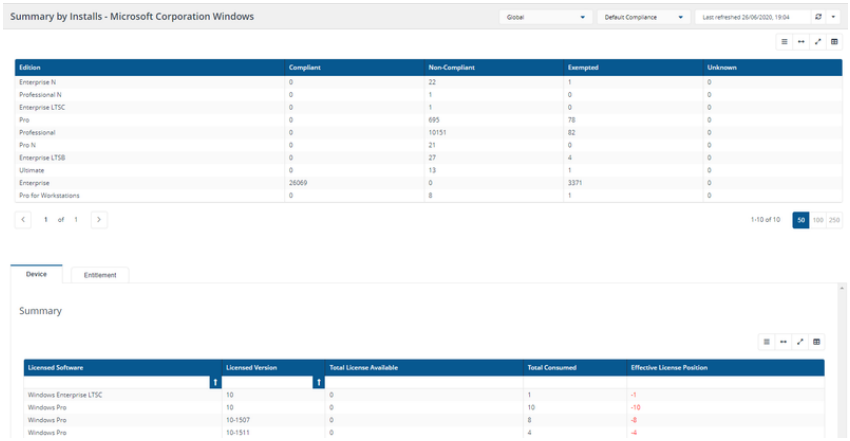
To view Compliance Information about a specific product click directly on the colored bar in the **Compliance Category**. Also, on mouse hover, it displays 3 categories as below and also display hover tool top %

Compliant (green) - Total no of compliant counts

Non Compliant (red) - Total no of non compliant counts

Exempted (blue) - Total no of exempted counts

This displays the compliance **Summary by Installs** page, for more details on the fields on this page please refer to Summary by Installs page.



10.4.6 Viewing your effective license position

AppClarity can take Inventory and combine that with your entitlements to show your current compliance position, or the license position. The compliance position shows the result of matching up your current installations with your currently defined entitlements so that you can tell whether your entitlements are deficient, sufficient or surplus to your installations.

In this example, we will show how to use the **License Summary** and **License Position** pages to identify license deficits and how you can work to quickly implement the entitlements you need to change the deficits into

surpluses. Before viewing License Summary, please ensure all**License Demand**reports have refreshed to get the correct numbers for complex metric based products.

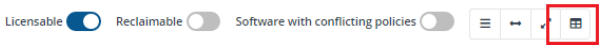
10.4.6.1 Viewing your license position

Your license position contrasts with your product compliance position, as shown in the previous Viewing product compliance example, in that it not only shows you license deficiencies it also shows your surplus licenses. This lets you work towards the ideal position where you roughly balance the two, so that you are completely compliant but have not drastically overspent on your licenses - some slight excess may be desirable to cater for future demand.

Navigate to the **AppClarity→Compliance→License Position** page. For more details on the fields in this page please refer to License Position page.

In our example, on this page in the **License Position** column we can see the **5** excess of licenses implemented for the **Microsoft Visio** product.

Scanning down the products we can see a **-8** deficit for **Microsoft Project**. Based on **10** licenses we have purchased for Microsoft Project we'd like to turn this now into a similar excess of **5** licenses.

> **Note**
>
> You can choose which columns are displayed in Inventory and AppClarity detail tables to increase readability. On pages where you can pick the displayed columns you'll see a new control like the one highlighted below:
>
> 
>
>
> To find out more about this feature refer to Running your first Compliance License Summary: Choosing the columns to display in reports.

The quickest way of doing this is to navigate to the **AppClarity→Licenses / Maintenances** page, we then set a filter to get directly to the Microsoft Project installations:

Click the filter at the right-hand under the **Title** Column header.

Construct the **filter Contains Project**.

Click **Apply** to set the filter.

In our example select the row with **Microsoft Project** and a Type of **License** click the **Edit** button when it becomes enabled.

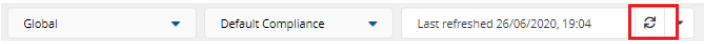
In the **Edit License** page prefilled with the details for **Microsoft Project** we set:

Quantity to **24**

Unit cost to **$400**.

> **Note**
>
> You can change the default displayed currency from USD to a currency of your choice, refer to Changing the default currency in AppClarity for details.

Then click **Publish** to publish the new entitlement and then refresh the necessary**Compliance**report to make the new entitlement count against our installations, using the **Refresh reports** icon on the top right of the page.

> **Note**
>
> You can refresh reports from individual AppClarity screens as well as using the **Settings** App. You can do this by using the refresh icon next to the**Last Refreshed**box, for example:
>
> 
>
>
> For a complete list of the specific reports you can run from particular pages refer to Running your first Compliance License Summary: Refresh Reports.

The multiexcerpt named '**RefreshReportsUsingSettings**' was not found. Please check the page name and MultiExcerpt name used in the MultiExcerpt Include macro.

Having made the entitlement count we now navigate back to the **AppClarity**→**Compliance**→**License Position**page where in our example we can see that the deficit of **-8** for **Microsoft Project** is now a surplus of **5**.

In this example we've seen how to view the license position for each product. We've identified a deficit of **-8** for **Microsoft Project** and used the **License Summary** page to add additional Microsoft Project licenses. We've then browsed back to the **License Position** and seen the deficit turn into a surplus.

10.4.7 Creating a license entitlement

Entitlements are key components for determining your compliance position, also known as the license position. The license entitlements you create are taken into account against the installations on your enterprise, you can then create various reports to show exactly what your effective license position is.

There are three types of entitlement you can create in AppClarity:

Licenses

Maintenance

Agreement.

You may see when you create an entitlement that there is a fourth type called **Contract**. Contracts are really just placeholders for documentary evidence of ownership and may be associated with

any of the three types of entitlement. In our example, we show how a contract can be associated with a license.

By combining these types, you can model a wide range of complex entitlements that you may have in your enterprise, allowing these to convert easily into AppClarity.

In this example

In this example, we introduce entitlements by creating a simple license for Microsoft Visio, and show how that is processed by AppClarity and taken into account against the software installed on our example network.

At the end of this example, you will have created one license entitlement in AppClarity. You will also have created a contract, which is a placeholder for any document, link or written evidence as proof of ownership for the license, the contract will then be linked to the license.

To carry out the actions described below, your user will require either the Entitlement Administrator, Compliance Administrator or Full Administrator role.

It is generally a good idea if the license, maintenance, and agreement entitlements you create have at least one associated contract. It's not mandatory, but it makes sense if the entitlements you create have proof that you own the particular license, maintenance, or agreement. For example, the contract may contain an enterprise agreement, a scan of a proof of purchase, a .PDF of an order or a paid purchase order. You create the contract and link to or load the associated proof into it. After saving, it may then be linked to the license, maintenance, or agreement you want it associated with. Subsequently, when auditing your licenses, AppClarity holds the proof of ownership linked to the entitlements that cover your installations.

10.4.7.1 Creating a simple entitlement

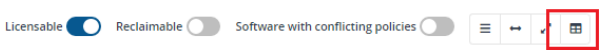
This example shows how a license deficit for a Microsoft Visio installation can be turned into a surfeit by creating a license entitlement. It assumes that you already have inventory data and that you've run the Compliance report.

Navigate to the **AppClarity**→**Compliance**→**License Position** page.

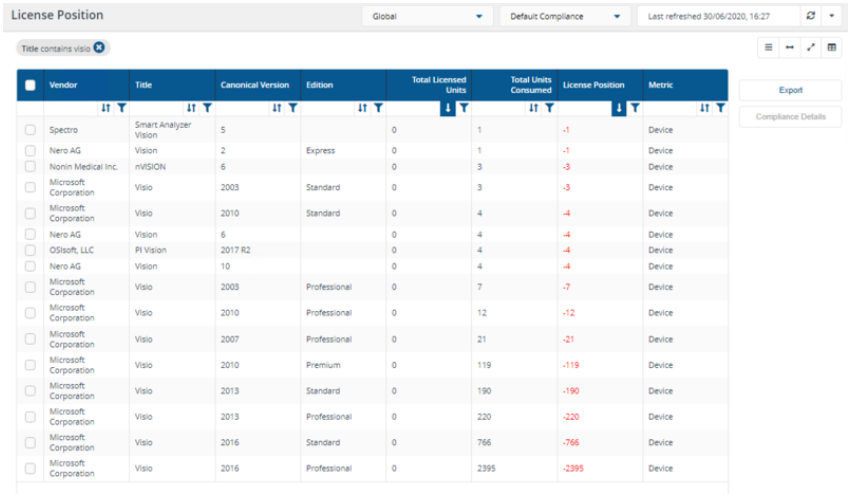
Click on the in the **Title** Column and enter **contains** in the dropdown and Visio in the next field, click **Apply**.

Note

You can choose which columns are displayed in Inventory and AppClarity detail tables to increase readability. On pages where you can pick the displayed columns you'll see a new control like the one highlighted below:

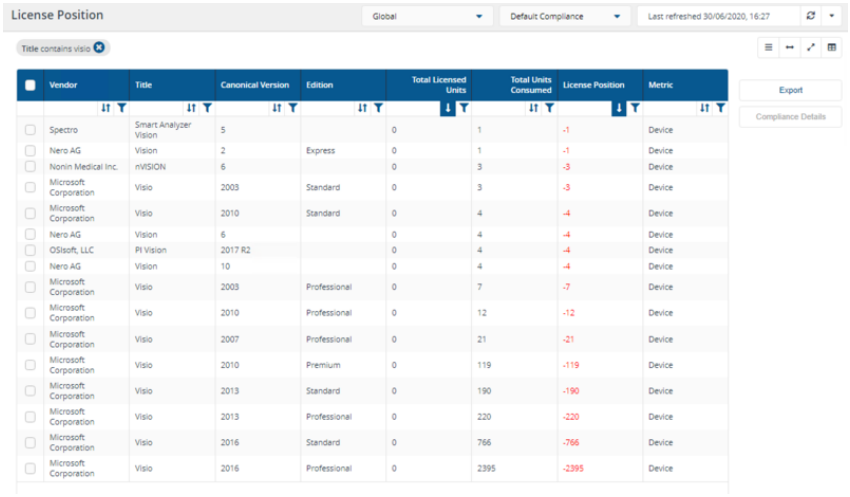


To find out more about this feature refer to Running your first Compliance License Summary: Choosing the columns to display in reports.



In our example you can see that there are multiple entries with the **Title contains Visio** including those with the **Canonical Version** of 2013 and on 2016, both are the Professional Edition.

By selecting either of those listed the **Compliance Details** button becomes enabled, click **Compliance Details**.



This opens the **License Summary** page, filtered on Microsoft Corporation and Visio.

Displayed is the consolidated Summary for all versions of Visio.

It's also possible to achieve the same result directly from the **License Summary** page and adding filters there.

10.4.7.1.1 Creating a simple license

To create our example license, we know the following information about the license:

Vendor: **Microsoft Corporation**

The units per license (**1 unit** per device in case of **Device** Metric**)**

Title: **Visio**

Edition: **Professional**

Version: **2016**

The cost per unit for the license, in this case **$150**

> **Note**
>
> You can change the default displayed currency from USD to a currency of your choice, refer to Changing the default currency in AppClarity for details.

To create and publish a license entitlement:

Select the displayed product and click **Add License**, located just to the right.

In the **New License** page we will choose a specific set of options to show how this page works. For more details on all the fields in this page please refer to New License page.

There are lots of fields on the page, but only a few are mandatory. The mandatory fields have an * next to their name.

The page is split into a number of sections, we will start in the **Basic Information** section.

The **Management Group** is the first mandatory field, it's set by default to Global, but it can be changed to any of your existing Management Groups, in this example we will leave it at **Global**.

The next mandatory item is the **Vendor** field. As we have opened this page after selecting a product, any known fields are prepopulated. Where they are not then as you start to type information suggestions are shown which are bought in from 1E Catalog.

Now we set:

Title: Visio

Version Type: Colloquial (need to set this, so we can specify the **Version** as **2016**)

Version: 2016

Edition: Professional

Metric Type: Device (this is the default)

Quantity: 65 (For other more complex metric types you will need to adjust the **Quantity** accordingly.

Entitlement Type: Perpetual

Start date: to the date the license started, or is due to start on. In our example, it's set to the default of the current date

Duration set the duration of the license, this will be required if the license is not Perpetual

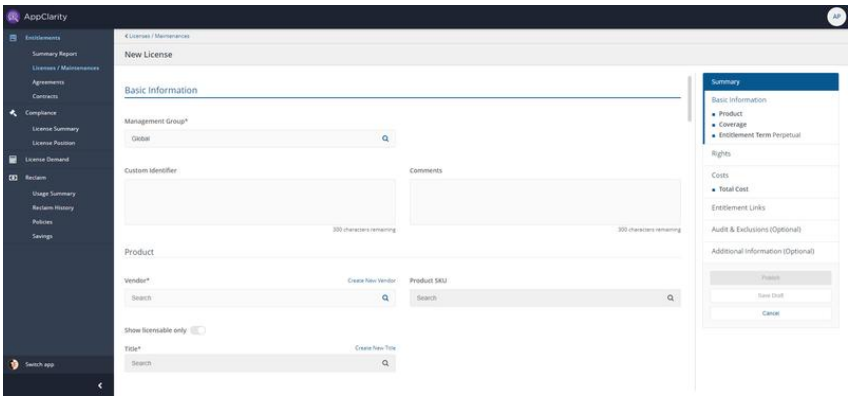
Version Downgrade: We now ensure that the both **Available** and **Persistent** checkboxes under the **Rights** section are checked, as it should be by default. This will confirm that this license can be applied to versions of Visio earlier than 2016.

Costs: 150

Currency: is already set to **USD** by default. AppClarity then calculates the total cost of the 65 licenses as **$9750.00**.

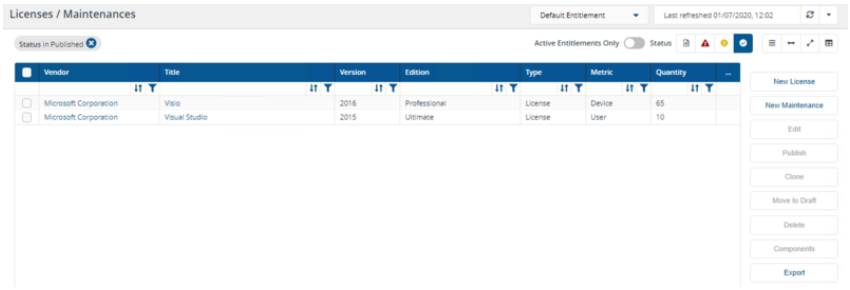
Now everything is set how we want it lets make this license entitlement take effect. To do this we click the **Publish** button at the bottom of the page. We could have clicked **Save draft**, if we were in the middle of making changes and didn't want to make the license active and the license would have been saved as draft in the **Licenses / Maintenances** page.

> **Note**
>
> These steps can also be carried out directly on the **Entitlements - Licenses/Maintenances** page and clicking on **New License**, but the prefilled information will not be there, and you will need to enter that yourself.



Having published the license entitlement an entry now appears in the **Licenses / Maintenances** page.

Click the green tick published icon to show the License we just published.

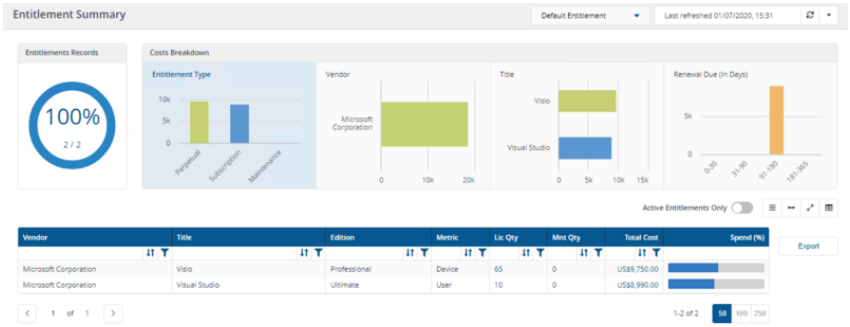


On publishing an entitlement, the **Entitlement Consolidation** report is refreshed. Once this is done, data can be seen on the **Entitlement Summary** page.

> **Note**
>
> You can download a .tsv report of the Entitlement Summary for your organization.
>
> Click **Export** to download a file in the format EntitlementSummary_currentdate.tsv

Note

The **Active Entitlements Only** control has been added to the **Entitlement Summary** page. The control adds a filter when it's turned on that filters the table to only display the entitlements that have been published and not the ones that are in draft.



To make a published license entitlement take effect you have to run the **Compliance** report:

Navigate to the **Settings**→**Connector** page and click on the **Execute** button.

The **Execute** action popup is displayed, enter the following:

Repository: Default Compliance

Action: Generate Report - Compliance

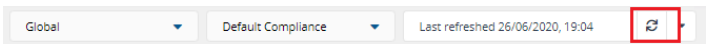
Navigate to **Settings**→**Monitoring**→**Process Log** and wait for the action to complete, this will be **Compliance** and will have a green tick in the **Status** column when complete.

Navigate to the **AppClarity**→**Compliance**→**License Position** page.

In our example you can see that **Visio** with **Edition** of **Professional** now has a **License Position** of **5.** This indicates that the installations of the software title are now licensed and there are **5** spare licenses for **Visio**.

Note

You can refresh reports from individual AppClarity screens as well as using the **Settings** App. You can do this by using the refresh icon next to the **Last Refreshed** box, for example:



For a complete list of the specific reports you can run from particular pages refer to Running your first Compliance License Summary: Refresh Reports.

10.4.7.1.2 Creating a contract

In our example we will create a new contract and load a scan of the proof of purchase for **Visio**.

To create a new contract:

Navigate to the **AppClarity**→**Entitlements**→**Contracts** page.

Click the **New Contract** button, located just to the right of the page.

In the **New Contract** page set the details for the contract. In our example we make the following settings:

Name: Visio

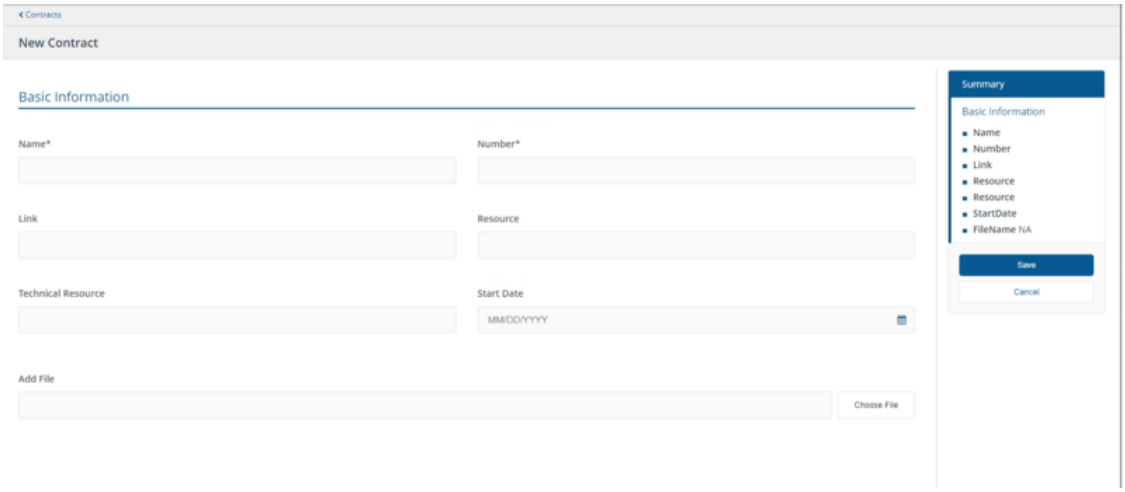
Number:11

Start date: 03/01/2018

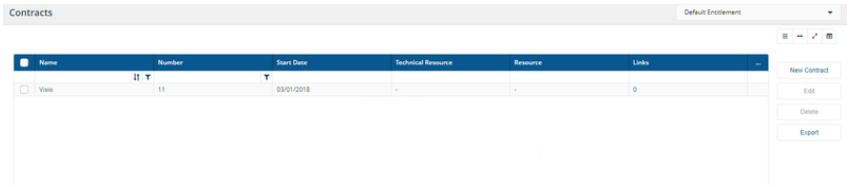
On this page you could set a link to the contract (if the contract is online), specify the name of the person or role who manages the agreement, specify the name of the person or role who knows the technical detail of the license. In our example we will just add an attachment of a scan of the proof of purchase for **Visio**.

Clicking **Choose File** displays a system **Open** dialog, here you can browse to and select the file you want to attach. In our example the file is in **C:\AppClarity\Contract Scans** and is called **Visio20180607.png**. When the file is selected click **Open** to attach the file.

Once all the settings have been made on the screen click **Save contract**.



The newly created contract is now added to the **Contracts** page.



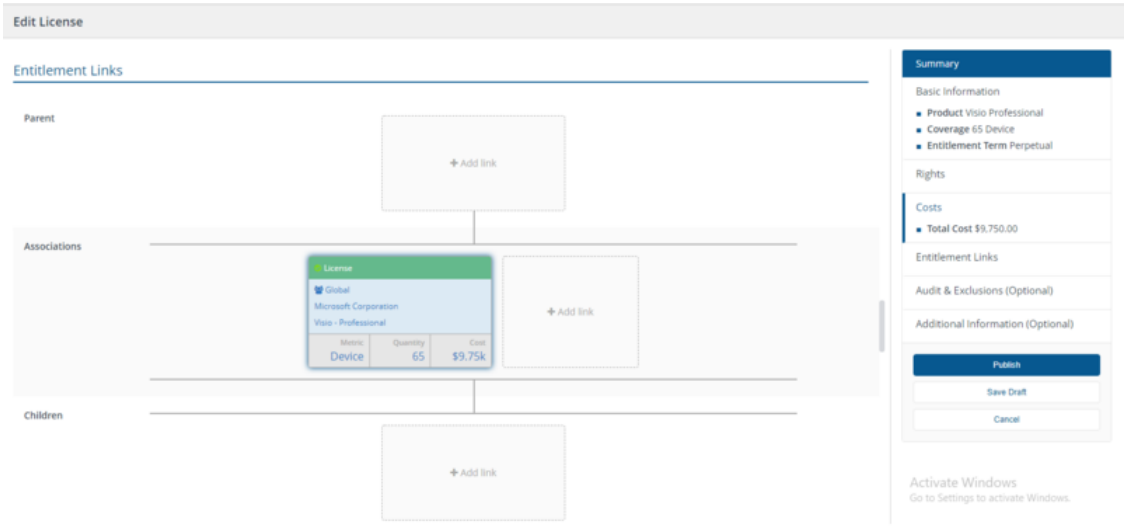
10.4.7.1.3 Linking the license to the contract

Once the new contract has been saved you can now link it to a license, maintenance or agreement entitlement.

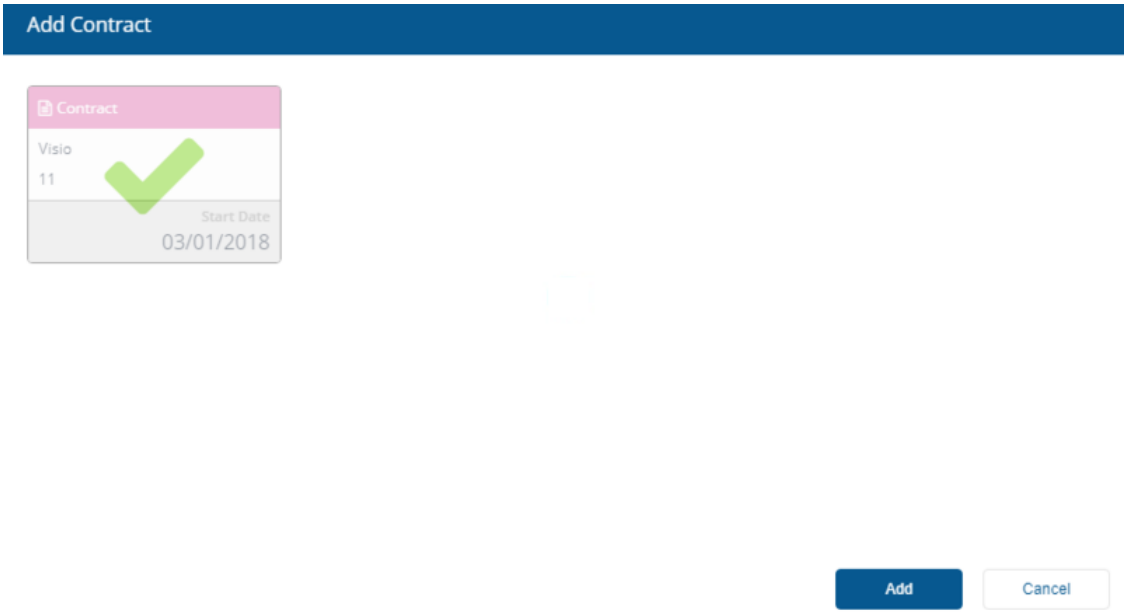
To link a contract:

On the **AppClarity**→**Entitlements**→**License / Maintenances** screen locate the entitlement you want to link the contract to. At the right-hand end of the entitlement's entry click on the **Edit** link. In our example we click on the **Edit** link for the **Visio** license entitlement we created earlier.

On the **Edit License** page scroll to the **Entitlement Links** section and click the **+ Add Link** in the **Associations** area.



On the **Add Contract** popup subsequently displayed, locate the contract created earlier. In our example this was called **Visio**, and click the contract, a green tick will appear and click **Add**.

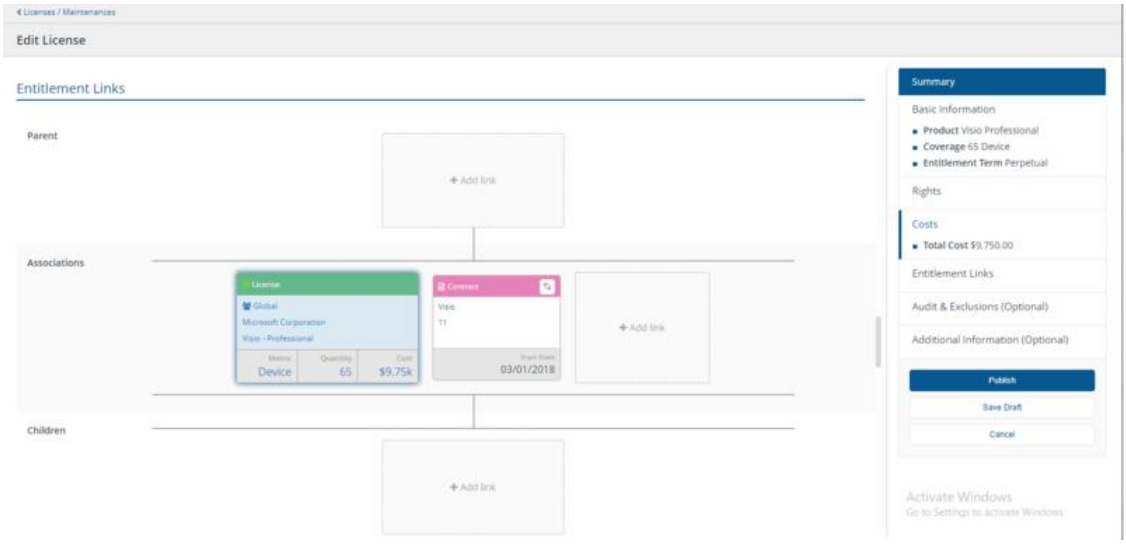


The **Edit License Entitlement Links** will be updated.

Click on **Publish**, this returns to the **Licenses / Maintenances** screen, and a 1 will now appear in the **Links** column for this entitlement.

If you click on the 1 in the **Links** column this will open the **Entitlement Links** page in view mode showing the **Associations**.

Congratulations! You have now created your first license entitlement and your first contract and linked one to the other.

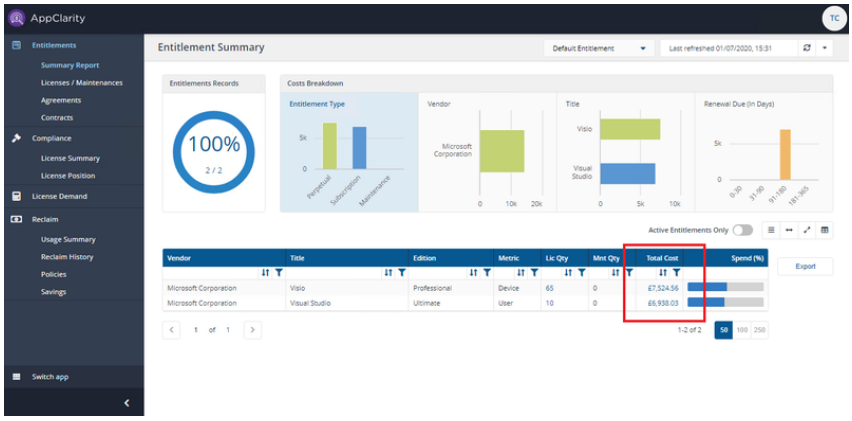


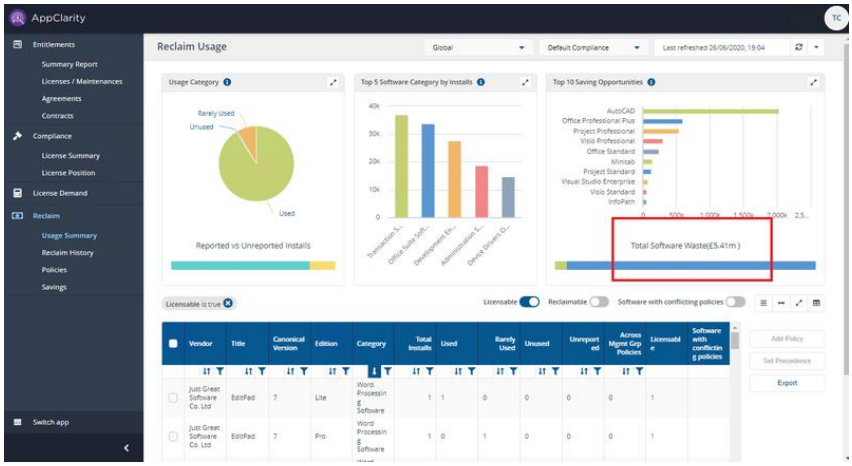
10.4.7.2 Changing the default currency in AppClarity

You can change the default currency (USD) along with the appropriate currency symbol and name from USD to a currency of your choice. For example, if you set the default currency to GBP then all cost values should be displayed in GBP after currency conversion (if required) along with the correct currency symbol (in case of graphs).

You can change the cost values displayed on the following pages, costs will show the default currency name and graphs will reflect cost values with default currency name and symbol.

Title page	Sub-page	Sub-page
Entitlements	Summary Report	n\a
Reclaim	Usage Summary	n\a
Policies	New Policy	
Edit Policy		
Savings	n\a	





10.4.7.2.1 Setting the default currency

The default currency is set to USD by default, you can change this using an SQL script run against your SLA-Shared database. For example to change the default currency to GBP, you would run the following query:

Changing the default currency

```
USE [SLA-Shared]

UPDATE Setting

SET [Value] = 'GBP'

WHERE [Key] = 'DefaultCurrency'
```

You can view all the currencies available in AppClarity by running the query against SLA-Shared database:

Display available currencies

```
SELECT * FROM Currency
```

Running *SELECT * FROM Currency* returns these results:

CurrencyID	Name	DisplayName	Symbol
1	USD	NULL	$
2	EUR	NULL	€
3	GDP	NULL	£
4	JPY	NULL	¥
5	CAD	NULL	C$
6	AUD	NULL	A$
7	CNY	NULL	¥
8	CHF	NULL	Fr.
9	SGD	NULL	S$
10	HKD	NULL	HK$
11	ZAR	NULL	R$

Note

You can only set the default currency to a value which exists in the Currency table. If the default currency value does not exist in Currency table, then USD will be used as the default currency and all cost values will be displayed in USD.

However the currency symbol and currency may not be in USD and will be same as entered by you when setting default currency, when you set the default currency value, it should be in upper case.

10.4.7.2.2 Updating Currency Conversion Rates

To convert cost values from one currency to another currency, you should maintain a conversion table based on the latest conversion rate. Because all cost values are stored in USD, you will need to update the conversion rate from USD to DefaultCurrency and DefaultCurrency to USD. You can use the following SQL queries to do this.

For example, if you have set the default currency to GBP, you will need to set the conversion rate for converting USD -> GBP and GBP -> USD.

Converting USD to GBP

```
UPDATE cc

SET cc.Rate =  0.77175 -- Take the latest conversion rate

FROM CurrencyConversion cc

JOIN Currency fromCurrency ON cc.FromCurrencyID = fromCurrency.CurrencyID

JOIN Currency toCurrency ON cc.ToCurrencyID = toCurrency.CurrencyID

WHERE fromCurrency.Name = 'USD' and toCurrency.Name = 'GBP'
```

Converting GDP to USD

```
UPDATE cc

SET cc.Rate =  1.295756 -- Take the latest conversion rate

FROM CurrencyConversion cc

JOIN Currency fromCurrency ON cc.FromCurrencyID = fromCurrency.CurrencyID

JOIN Currency toCurrency ON cc.ToCurrencyID = toCurrency.CurrencyID

WHERE fromCurrency.Name = 'GBP' and toCurrency.Name = 'USD'
```

After updating then to view the changes reports on the following screens will require refreshing: Entitlements - Summary, Reclaim - Usage Summary, Reclaim - Policies and Reclaim - Savings

10.4.8 Creating and linking a maintenance entitlement

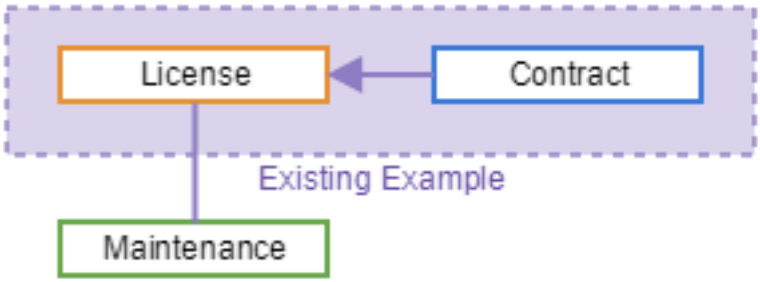
A Maintenance entitlement type in AppClarity specifies the rights and limitations for an organization to install and/or use updated versions of software defined in a license. For example you could specify a maintenance entitlement for Microsoft Visio 2016 to cover all new versions from the current date for the next 3 years.

A maintenance entitlement can be linked as a child of an agreement, a license or another maintenance entitlement. Maintenance entitlements can also have other child maintenance entitlements. As with all the entitlements, maintenance can also have one or more associated contracts.

In this example

In this example we extend the example described in Creating a license entitlement by creating an additional maintenance entitlement for Microsoft Visio to extend the licensing for that product to include all future versions for the next three years.

At the end of this example you will have created a new maintenance entitlement in AppClarity and linked it to the existing Microsoft Visio license entitlement from the Creating a license entitlement example.



To create our example maintenance we know the following information about the license:

Vendor: **Microsoft Corporation**

The units per license, in this case **10** units each covering 1 device

Title: **Visio**

Duration: How long the maintenance period lasts in months, in our example **36** months (3 years)

The cost per unit for the license, in this case **$50** (maintenance at 1/3 of the basic license cost).

10.4.8.1 Creating the maintenance entitlement

To create and publish a maintenance entitlement:

Navigate to **AppClarity→Entitlement→Licenses / Maintenances**. This displays the **Entitlement Repository** page for the repository selected in the top-right of the screen. In our example this is the **Default Entitlement** repository, you can see in our example that **Visio** has a green tick on this page, this is the entitlement that results from having just followed the Creating a license entitlement instructions.

Select **Visio** and click on the **New Maintenance** button, located just to the right of the screen.

The **New Maintenance page** opens. For more details on all the fields in this page please refer to New Maintenance page.

There are lots of fields on the page but a few are mandatory. The mandatory fields have an * next to their name.

The page is split into a number of sections, we will start in the **Basic Information** section.

The **Management Group** is the first mandatory field, it's set by default to **Global**, but it can be changed to any of your existing Management Groups, in this example we will leave it at **Global**.

Now we set the following fields and click **Publish**:

Vendor: Microsoft Corporation

Title: Visio

Edition: Professional

Quantity: 10

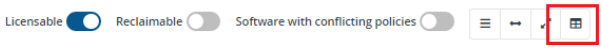
Entitlement Type: For maintenance entitlements defaults to **Subscription**, (which requires that both the **Duration** and **End date** fields are set. The **End date** is automatically determined by the combination of the **Start date** and **Duration** fields)

Duration: 36. which has automatically set the **End date** to 36 months after the **Start date**.

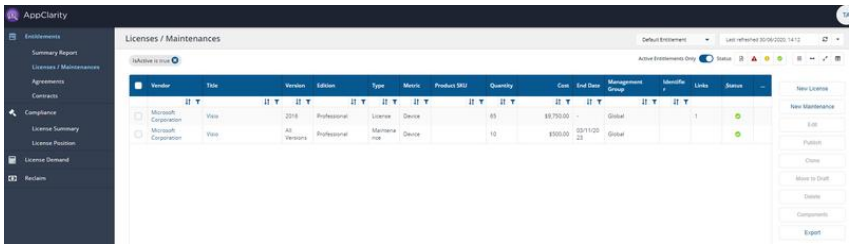
Unit Cost: $50, the **Currency** is already set to **USD** by default. AppClarity then calculates the total cost of the 10 maintenance additions as **$500.00**.

> **Note**
>
> You can change the default displayed currency from USD to a currency of your choice, refer to Changing the default currency in AppClarity.

The new maintenance entitlement now appears in the **Licenses / Maintenances screen**. It is listed as a new entry with the type listed as **Maintenance** and is row two on the screenshot to the right.

> **Note**
>
> You can choose which columns are displayed in Inventory and AppClarity detail tables to increase readability. On pages where you can pick the displayed columns you'll see a new control like the one highlighted below:
>
> 
>
>
> To find out more about this feature refer to Running your first Compliance License Summary: Choosing the columns to display in reports.

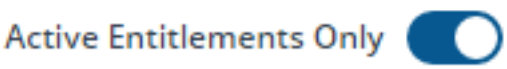
> **Note**
>
> You can download a .tsv report of the Licenses / Maintenances for your organization.
>
> Click **Export** to download a file in the format LicensesMaintenances_currentdate.tsv
>
> This button takes the filters currently applied to the table into account, but not the sorting or the current selection.



10.4.8.2 Linking the maintenance entitlement

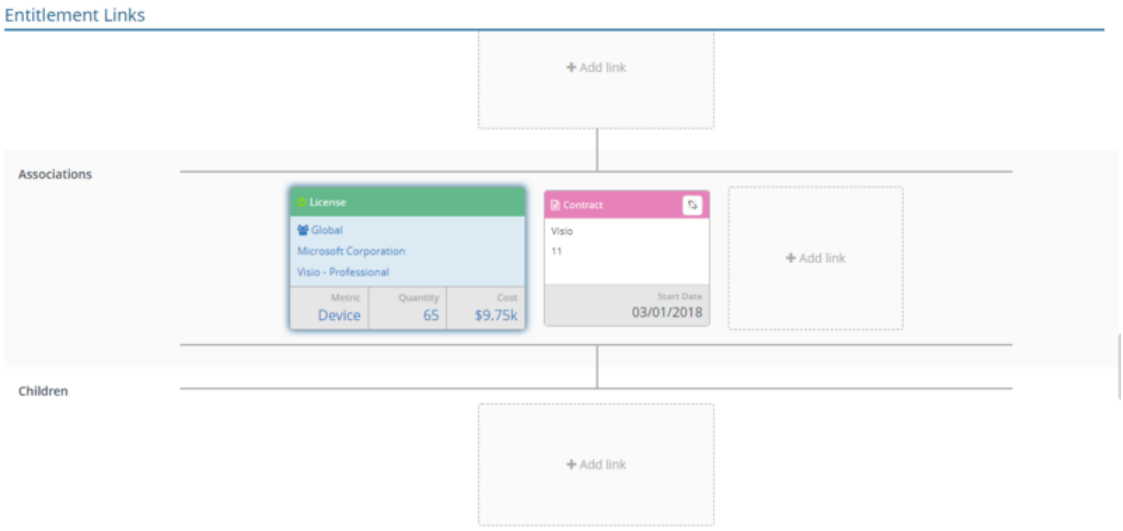
To link a maintenance entitlement to a previously created license entitlement:

On the **AppClarity**→**Entitlements**→**Licenses / Maintenances** page locate the entitlement you want to link the maintenance to. If you toggle the



toggle then this will reduce the number of entitlements displayed and will make finding the relevant one simpler. In our example we click on the **Edit** link for the **Visio** license entitlement we created earlier in Creating a license entitlement.

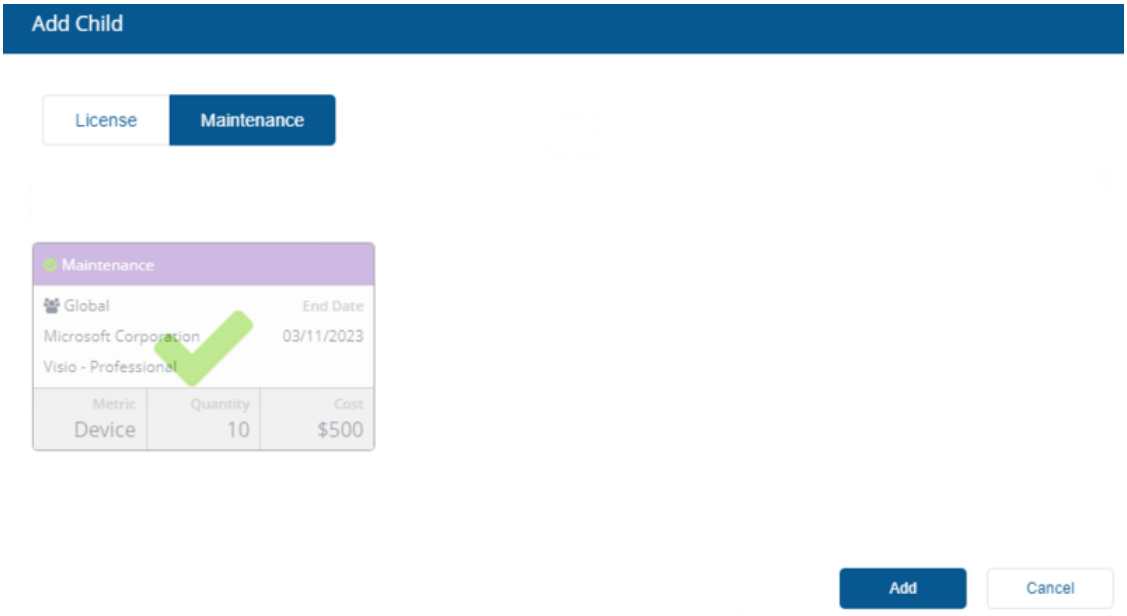
On the **Edit License** page scroll to the **Entitlement Links** section and click in the **Children +Link** area.



In the **Add Child** screen, select **Maintenance**, and click on the displayed **Maintenance**, a green tick will appear.

Click **Add**.

Click **Publish** to save the entitlement and keep it in effect. And you will be returned to the **Licenses / Maintenance** screen.



The maintenance is now linked to the license entitlement.

10.4.8.3 Refreshing the data

To make this immediately count against your compliance position, you should then refresh the following:

Navigate to the **Settings**→**Connector** page and click on the **Execute** button.

The **Execute action** popup is displayed, enter the following:

Repository: Default Compliance

Action: Generate Report - Compliance

Navigate to **Monitoring**→Process Log and wait for the action to complete, this will be **Compliance** and will have a green tick in the **Status** column when complete.

The new maintenance entitlement will now be in force for any new versions of Microsoft Visio that's installed during the next 3 years.

10.4.9 Creating an entitlement using a SKU

Stock Keeping Unit (SKU) codes can be used in some cases to help quickly fill out the details for an entitlement, they can even automatically create and link additional entitlements to model associated maintenance details. AppClarity will retrieve the information for a SKU from 1E Catalog.

Note

A SKU (pronounced 'skue') is an identification, usually alphanumeric, of a particular product that allows it to be tracked for inventory purposes. In AppClarity, via the 1E Catalog, a SKU is associated with the license metrics and use rights associated with a particular software product purchase.

SKUs are in widespread use throughout the software industry, where publishers refer to their software using a SKU. The SKU gets added to most purchase orders to indicate the software or package being bought. Even small differences between two software titles are indicated by different SKUs. The SKU also indicates the license metrics and maintenance terms associated with the purchase and any additional use rights covered by the purchased license.

AppClarity uses the SKU data to automatically:

Prefill the settings in an entitlement with the product details, license metrics, and basic maintenance terms that are indicated by the SKU

Set the additional use rights that are part of the license indicated by the SKU

In this example

In this example, we show how the previous example of a license and maintenance entitlement for Microsoft Visio can be done in a single operation using a SKU number to fetch the details from 1E Catalog.

By the end of this example, you will have created a license entitlement in AppClarity and used a SKU to populate its fields for a Microsoft Visio license and automatically create and link an associated 36 month maintenance for Microsoft Visio.

Let's take a step back now and look at the entitlements we've created so far. The first simple license entitlement covered installations for the Microsoft Visio product, and we had to add the details for the Vendor, License Type, Metric details, Product title, Version Type, Version and Edition. Along the way we also created a contract and attached this to the license. We then created a maintenance entitlement that defined a 3-year subscription and attached that to the license and effectively extended the perpetual license to cover any new versions released during those 3 years.

This example shows how the first and last parts of that sequence can be created in a single step, assuming you know the SKU for Microsoft Visio with a 3-year maintenance. When you use a SKU it must be known by the 1E Catalog, new SKUs from different Vendors are added on a regular basis.

To create an entitlement using a SKU we know the following information in advance:

The vendor of the product, in this case **Microsoft Corporation**

The SKU for the product, in this case for the **Standard** edition of **Visio** this is **D86-03848**

The cost per unit for the license, in this case **$150**

This example assumes that instead of manually creating the two parts of the license and maintenance separately, we start from scratch and instead create and publish a license and maintenance entitlement using a SKU.

> **Note**
>
> You can change the default currency (USD) along with the appropriate currency symbol and name from USD to a currency of your choice, for more details refer to Creating a license entitlement: Changing the default currency in AppClarity

10.4.9.1 Creating the maintenance entitlement from the SKU

To create and publish a license entitlement:

Navigate to the **AppClarity→Entitlements→Licenses / Maintenances** page and click on **New License**.

In the **New License** page we will choose a specific set of options to show how this page works. For more details on all the fields in this page please refer to New License page.

There are lots of fields on the page, but a few are mandatory. The mandatory fields have an * next to their name.

The page is split into a number of sections, we will start in the **Basic Information** section.

The **Management Group** is the first mandatory field, it is set by default to **Global**, but it can be changed to any of your existing Management Groups, in this example we will leave it at **Global**.

The next mandatory item is the **Vendor** field. We know that the vendor for **Visio** is **Microsoft Corporation**, so we start by typing **Micros** into the field and select **Microsoft Corporation** from the dropdown list of suggestions.

This time the **Product SKU** field is the next one we have to fill out. So we start typing the SKU, after entering the first few characters matching SKUs are displayed. We select the matching **D86-03848** from the dropdown list of suggestions.

Note, the page title has now changed to **Edit LicensePlusMaintenance**

Notice how after selecting the SKU the **License Type**, **Metric Type**, **Duration**, **End date**, **Product title** and **Edition** fields are now filled out.

Now we set the following fields and click **Publish**, we could have clicked **Save draft**, if we were in the middle of making changes and didn't want to make the license active and the license would have been saved:

Quantity: 10

Units: 1

Unit Costs: 150

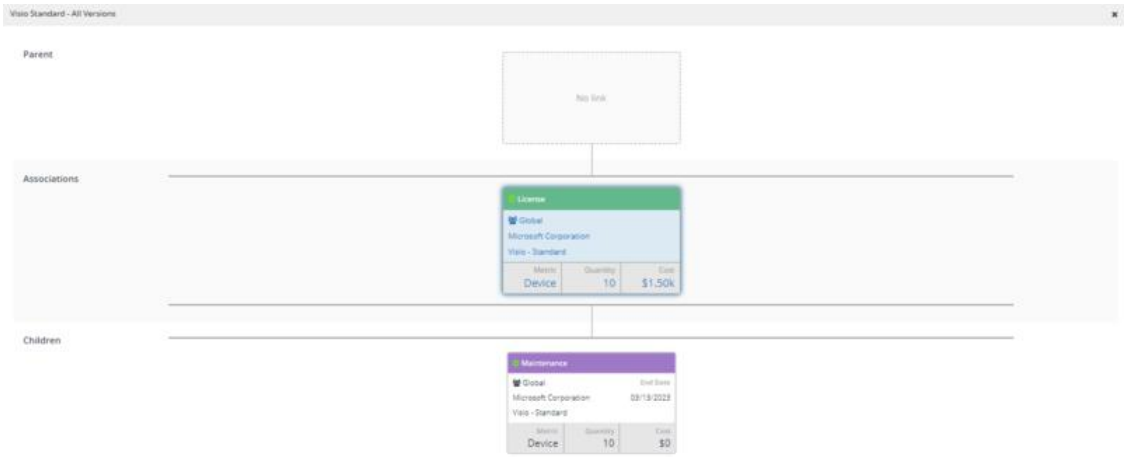
Currency: is already set to **USD** by default. AppClarity then calculates the total cost of the 10 licenses as **$1500.00**

Confirm the Entitlement is created:

Having published the license entitlement an entry now appears in the **Licenses / Maintenances** page. For **Visio Standard** Edition, with the **Product SKU** populated with the previously entered values.

To check this further click on the **1** in the **Links** column for the Entitlement.

In the popup you'll see the entitlement linked to the **Children Maintenance**.



To make a published license entitlement take effect you have to run the **Compliance** report:

Navigate to the **Settings**→**Connector** page and click **Execute**.

The **Execute action** popup is displayed, enter the following:

Repository: Default Compliance

Action: Generate Report - Compliance.

Navigate to **Monitoring**→**Process Log** and wait for the **Action** to complete, this will be **Compliance** and will have a green tick in the **Status** column when complete.

Navigate to the **AppClarity**→**Compliance**→**License Position** page.

In our example you can see that**Visio** with **Edition** of **Standard** now has a **License Position** of **10.** This indicates that the installations of the software title are now licensed and there are **10** spare licenses for **Visio**.

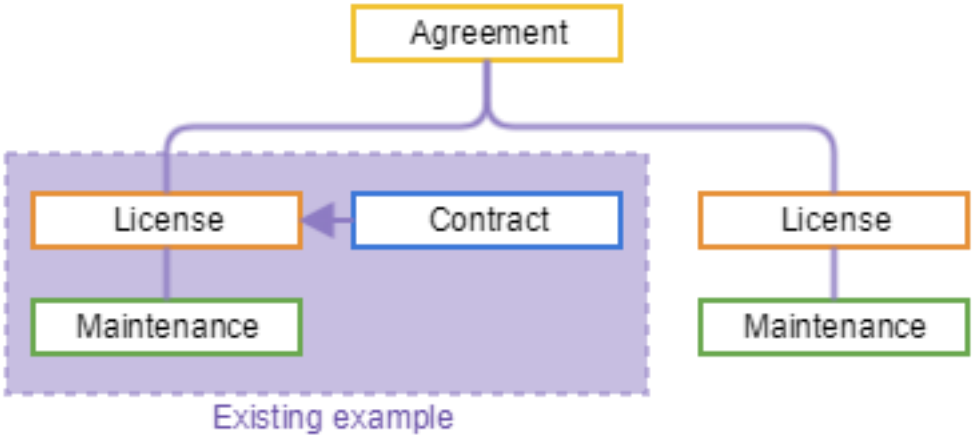
10.4.10 Creating an agreement entitlement

Agreement entitlements provide a way of grouping and organizing entitlements together to model the agreement structures in place between your organization and a vendor of a specific software title. Agreements can act as containers for license, maintenance, and even other agreement entitlements.

In this example

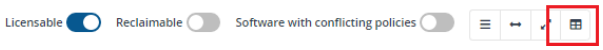
In this example we will extend the Microsoft Visio license and associated maintenance and contract created in Creating a license entitlement and Creating and linking a maintenance entitlement.

By the end of this example you will have created a new Microsoft Product agreement entitlement and linked the existing Visio license to it. You will also have created a new Microsoft Project license and associated 36 month maintenance and then linked that to the new agreement.



10.4.10.1 Check we have a deficit

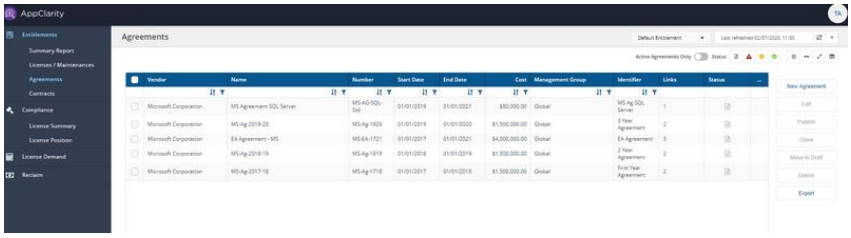
To the right we have navigated to **AppClarity→Compliance→License Position** page and filtered the **Title** on Project which shows that we have an installation for **Microsoft Project** and that has a total license deficiency of **-19**.

> **Note**
>
> You can choose which columns are displayed in Inventory and AppClarity detail tables to increase readability. On pages where you can pick the displayed columns you'll see a new control like the one highlighted below:
>
> 
>
>
> To find out more about this feature refer to Running your first Compliance License Summary: Choosing the columns to display in reports.

Selecting any of the displayed products and then **Compliance Details** opens the **License Summary** page, this display can also be accessed directly and filtered, but you should know there are multiple ways to access the page.

10.4.10.2 Add a New Agreement

To add a new **Microsoft Products** agreement entitlement, navigate to the **Entitlements→Agreements** page and click on **New Agreement**, located just to the right.



To add a new **Microsoft Products** agreement entitlement:

Navigate to the **Entitlements**→Agreements screen and click **New Agreement**, located just to the right.

In the **New Agreement** page we will choose a specific set of options to show how this page works. For more details on all the fields in this page please refer to New Agreement page.

There are lots of fields on the page but a few are mandatory. The mandatory fields have an * next to their name.

The page is split into a number of sections, we will start in the **Basic Information** section.

The **Management Group** is the first mandatory field, it is set by default to **Global**, but it can be changed to any of your existing Management Groups, in this example we will leave it at **Global**.

The next mandatory item is the **Vendor** field. We know that the vendoris **Microsoft Corporation**.

Now we set the following fields and click **Publish**. We could have clicked **Save draft**, if we were in the middle of making changes and didn't want to make the agreement active, the draft agreement would then be saved.

Name to **Microsoft Product Agreement** - this should be the name of your agreement

Number to **Ag123456** - this is not mandatory, but should be the Agreement Number

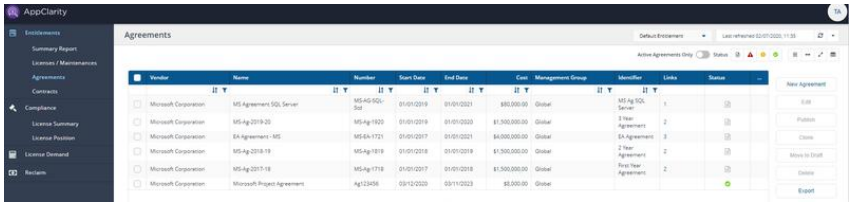
Entitlement Term Start Date defaults to today's date, but should be set to the date your agreement starts, in the example we will use today's date

Duration to **36**

Total Cost to **$8000**

> **Note**
>
> You can change the default currency (USD) along with the appropriate currency symbol and name from USD to a currency of your choice, for more details refer to Creating a license entitlement: Changing the default currency in AppClarity

The **Agreements** page will update and the new agreement will be listed, with the **Status** column having a green tick to show it is published.



We will now link the new **Agreement** to our existing **License** for **Microsoft Visio**.

After the actions above, we are returned to the **Entitlements - Agreements** screen.

Select the **Agreement** just created and click **Edit**.

Scroll to the **Entitlements Links** section and click **+ Add link** in the **Children** section.

Scroll to find the **Visio Professional License,** and then click on this and the green tick we have previously seen will appear.

Click **Add**.

Click **Publish**.

Now we'll add a new license for **Microsoft Project** (refer to Creating a license entitlement for the steps to achieve this, not forgetting to **Publish** once added):

Enter the following details for the license:

Vendor: Microsoft Corporation

Title: Project

Version Type: Colloquial

Version: 2016

Edition: Professional

Metric Type: Device (this is the default)

Quantity: 20

Entitlement Type: Perpetual

Start date: to the date the license started, or is due to start on. In our example it's set to the default of the current date

Costs $200

Adding a new maintenance entitlement for **Microsoft Project**:

Return to the **Licenses / Maintenances** screen. Click the **New Maintenance** button.

We then set the details for the Maintenance click **Publish** when entered:

Vendor: Microsoft Corporation

Title: Project

Edition: Professional

Quantity: 20

Entitlement Type: Subscription (default for maintenance)

Duration: 36

Unit Cost: 50

We will now link the **Microsoft Product Agreement** to our new **License** for **Microsoft Project**.

Navigate to **Entitlements** → **Agreements** screen.

Select the **Microsoft Product Agreement** and click **Edit**.

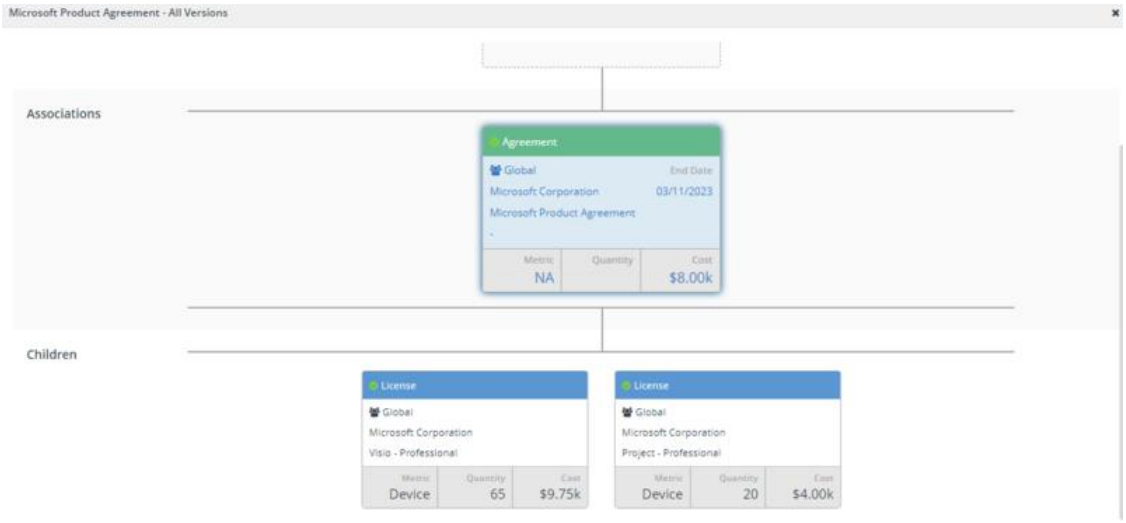
Scroll to the **Entitlements Links** section and Click **+ Add link** in the **Children** section.

Scroll to find the **Project Professional License** click on this and the green tick we have previously seen will appear.

Click **Add**.

Click **Publish**.

That has created the structure for our agreement. To see this click on the **2** in the **Links** column for the **Microsoft Product Agreement**, this will display the screen:



To make a published license entitlement take effect, you have to run the **Compliance** report:

Switch to the **Settings**→**Configuration**→Connectors page and click on the **Execute** button.

The **Execute action** popup is displayed, enter the following:

Repository: Default Compliance

Action: Generate Report - Compliance.

Navigate to **Monitoring**→**Process Log** and wait for the action to complete, this will be **Compliance** and will have a green tick in the **Status** column when complete.

Now that the compliance report has been run, to see the impact of implementing the entitlements:

Switch to the **AppClarity**→**Compliance**→**License Position** page.

In our example you can see that**Visio** with **Edition** of **Professional** now has a **License Position** of **5.** This indicates that the installations of the software title are now licensed and there are **5** spare licenses for **Visio.** And the **License Position** for **Project** is 1.

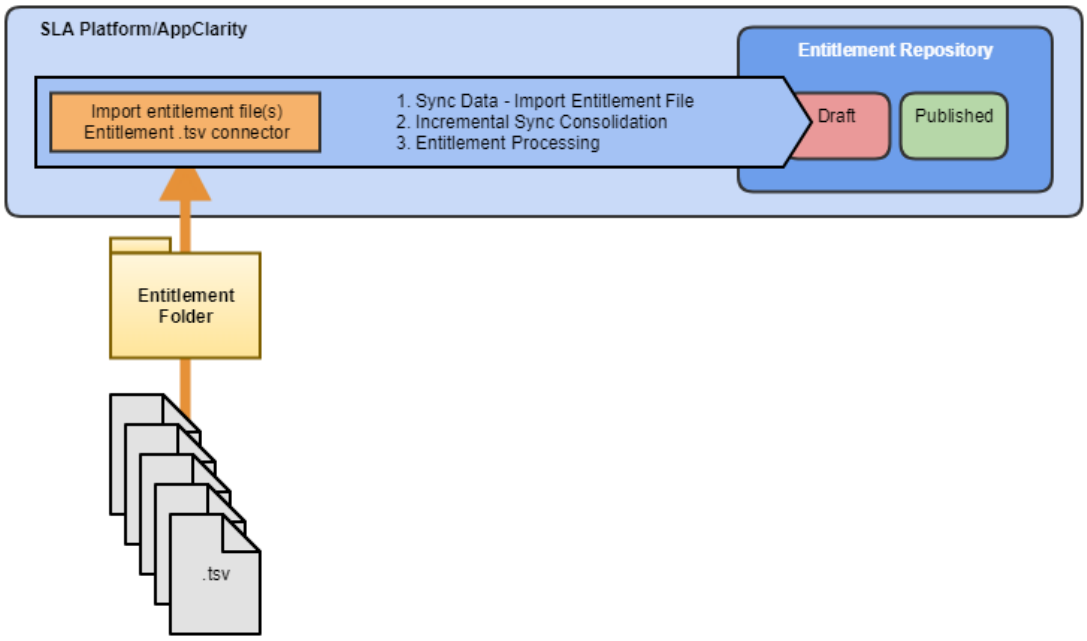
10.4.11 Importing entitlements from a folder

Large organizations may have thousands of entitlements to arrange. For AppClarity to report on your effective license position these need to be defined in AppClarity. To help get your entitlements in place, quickly and effectively AppClarity enables you to import directly from a particular folder. This means you can construct your TSV files as needed, place them in the folder and then import.

After importing the entitlements into AppClarity they are marked as Draft Entitlements. It gives you a chance to view any issues that arose as a result of the import process, and when that's done you can publish all of these entitlements in one go.

In this example

In this example we will show how to create and configure an **Entitlement .tsv** connector to point at a directory where the entitlement files will be placed. We will then show how the entitlement files are imported as **Draft Entitlements** and then the process of removing the imported entitlements with errors.



By the end of this example you will have:

Created a new connector that points at an entitlement directory holding some entitlement files

Added a new entitlements repository that will hold all the imported entitlements

Identified and resolved issues with the imported files

Published some entitlements derived from those files.

10.4.11.1 Importing entitlements from a file

10.4.11.1.1Configuring a connector

Entitlements are imported from .tsv formatted files with a particular schema. The way these files are brought in to AppClarity is using a connector pointing at a directory where the entitlement files are located or will be placed. For more details see Entitlement .tsv connector. The steps for configuring the connector are as follows:

Navigate to **Settings→Configuration→Connectors**.

Click the **Add** button.

In the **Add Connector** popup select the **Entitlement .tsv** connector from the list of connector types.

In the **Connector n ame** field enter a suitable name for the new connector, for a description of suggested naming conventions please refer to Naming conventions. In our example we call the connector **Entitlement File(s) Example**.

In the **Folder or File Location** field enter the folder where you are going to place the entitlement files. In our case we use the folder **C:\AppClarity\File Upload\Example**

Click **Add** to save the new connector.

Click the **Test** to ensure access to the folder with the entitlement files.

If the test is a success you'll see a green tick in the **Test Status** column.

If you see a red triangle, click on it to display its description. Use this information to help resolve the issue, then cycle through resolving and running the test until it's a success.

10.4.11.1.2Add a new entitlement repository

To keep the imported entitlements separate from our default or other entitlement repositories it's useful to create a new entitlement repository to test the import process and resolve any issues in isolation. For more details on adding and configuring repositories please refer to Repositories page. To create a new entitlement repository:

Navigate to the **Settings→Configuration→Repositories** page and click **Add.**

In the **Add repository** popup enter the details for the new repository.

Enter a unique **Name** for the repository that does not match an existing repository. For a description of suggested naming conventions, please refer to Naming conventions. In our example we call the repository **1E Entitlements**.

From the Repository type dropdown menu choose the type, **Entitlement**.

In the **Description** field set a suitable description that will let you know the purpose of the repository at a later stage. In our example this is **Entitlement files in the Example folder can be imported and tested here.**

Leave the **Default repository** checkbox unchecked and click **Add**.

10.4.11.1.3Populating the new entitlement repository

The next step is populating the new entitlement repository using the connector created earlier. To do this:

Navigate to **Settings→Configuration→Connectors** and click **Execute**.

In the **Execute action** popup select your new entitlement repository, In our example this is **1E Entitlements**.

From the **Action** dropdown, choose the **Sync Data** action for your **Entitlement .tsv** connector, and click **Execute.**

To monitor the progress of the new action navigate to **Settings→Monitoring→Process log** to view the **Sync Data** for Entitlement .tsv and dependent actions running.

There are three actions that run when you select the **Sync Data - <connector name>** action:

Sync Data

Incremental Sync Consolidation

Entitlement Processing

The output of each of these three related actions is:

Fetch the entitlement files from the folder pointed at by the connector.

Consolidate and de-duplicate entries in the information.

Process the imported entitlements and place them a draft state in **Entitlements**.

You should make sure these three actions complete successfully before continuing.

10.4.11.1.4Viewing the draft imported entitlements

When the actions have completed you can navigate to the **AppClarity→Entitlements→Licenses / Maintenances** page to view the imported entitlements. After creating a new entitlement repository you need to be aware that it won't initially be selected by default on any of the entitlements pages. To select the new entitlement repository:

On the **AppClarity→Entitlement→**Licenses / Maintenances page click on the entitlement name drop down in the top-right of the page. In our example when we first browse to the **AppClarity→Entitlement→**Licenses / Maintenances page the **Default entitlement** is selected.

From the list of entitlement repositories subsequently displayed in the drop down list, click on the name of the entitlements repository created and populated earlier. In our example this is **1E Entitlements**.

When this is selected, the newly imported entitlements will be visible on the **Licenses / Maintenances** page, in the **Status** column you can see the status of each entry will be set if there are no errors or warnings to **Drafts with no warnings**. If any entitlements have any errors or warnings, they will have an icon to warn of the issue (See the table below for the various statuses)**.**

If an Entitlement has a warning icon then to see the detail of what the issue is, click on the Entitlement title (it's a hyperlink) this will open the detailed page for the Entitlement. Scroll to the bottom section to view any warnings or errors for the entitlement.

10.4.11.1.5Bulk publishing the imported entitlements

Once the entitlements are displaying in the **Licenses / Maintenances** page you can check for and resolve any immediate errors and then bulk publish the imported entitlements. In our basic example the entitlement import into draft hasn't raised any issues, so we can get straight on with the business of publishing.

After reviewing the items and ensuring there are no errors. Scroll to the top of the page and click the **Select all** button. This checks all the boxes in the left-hand column.

Click the **Publish** button. This publishes all the rows where the boxes are checked.

When you publish the imported entitlements you sometimes get additional errors, for example incorrect or missing information or matching related issues. Check the icon's in the **Status** column for any items that do not display a published green tick.

To resolve an issue, where the Vendor, Title and Edition information hasn't completely matched with the catalog you'll need to edit the entitlement. Click **Edit** for the row in question.

In the entitlement edit page the values will be prefilled from the imported entitlement. You then need to check each of the following fields by clicking on the:

Vendor field and select any matching vendor returned from the 1E Catalog.

Title field and select any matching product returned from the 1E Catalog.

Version field and select any matching product version returned from the 1E Catalog.

Edition, if it's been set, and select any matching edition returned from the 1E Catalog.

After checking the vendor, title, version and edition click the **Publish** button to check any changed values.

Now all the imported entitlements have been processed successfully, navigate to the **AppClarity**→**Entitlements**→**Summary Report**→Entitlement Summary page to view all imported entitlements.

You can search for errors in the imported data by using the **Status** filters at the top of the **Licenses / Maintenances** page, by hovering your mouse over the icons you'll see a description for each filter:

Status Icon	Description
	Drafts with no warnings.
	Drafts with errors.
	Drafts with warnings.
	Published.

10.4.12 Managing compliance for user-based licenses

You can view your compliance position by focusing on how licenses are consumed by user as well as by device. From here, you can also add entitlements for a specific product.

10.4.12.1 Viewing product compliance by user

This example assumes that you have associated your chosen compliance repository with your chosen entitlement repository, this example uses**Default Compliance** and**Default Entitlement,** and you have run the **Compliance** report on your chosen compliance repository.

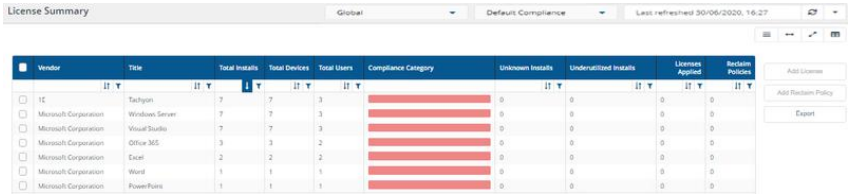
Please refer to Running your first Compliance License Summary for steps that show how to do this.

Our example, shows a simple workflow of how one user who is a primary user on multiple devices and uses the same software on those devices may need only one license for the installs to be compliant. In this example the user **ACME\Paul.Harris** uses 2 **Installations** on 2 **devices** running **Visual Studio Professional**, but would only

need 1 license because user based compliance works across devices, where device based compliance works per individual device.

To view product compliance and interact with the products to create new licenses and improve your compliance:

Navigate to **AppClarity→Compliance→License Summary**. Here you'll see a summary of your compliance position. The displayed table shows compliance information about all your products.



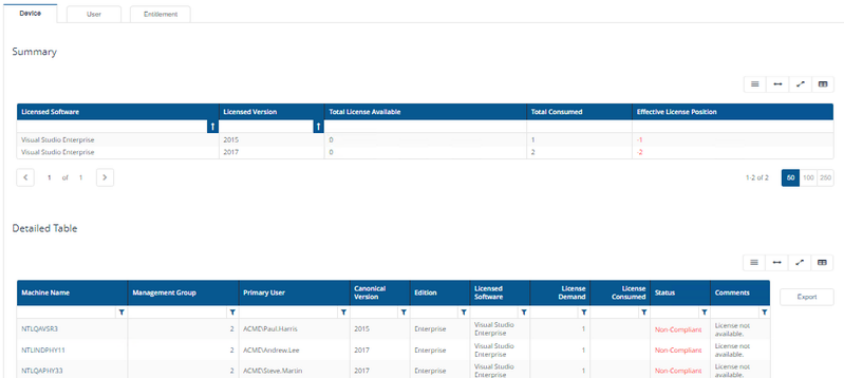
This displays the License Summary page, for more details on the fields on this page please refer to License Summary page. The compliance position for **Visual Studio** shows that **Visual Studio** has **7 installations** on **7 devices**, which are primarily used by **3 Users.** To make **Visual Studio** compliant we could use either of these options:

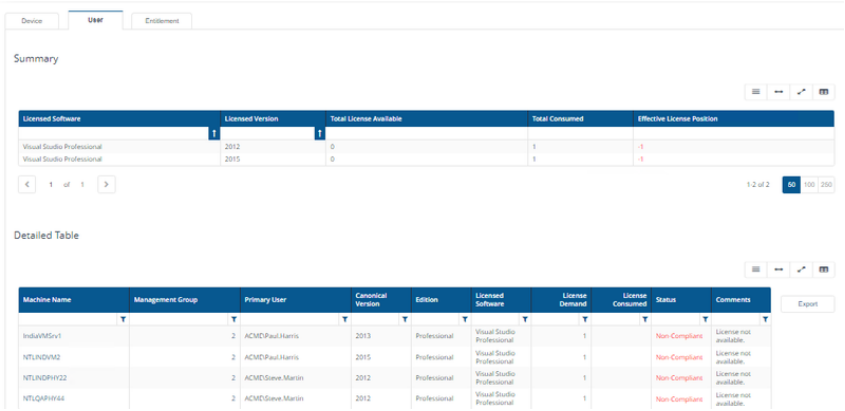
7 Device metric based licenses

3 User metric based licenses.

> This example focuses on setting up a User metric based license for **Visual Studio** to make this product compliant.

Select the product by clicking on the color bar in the **Compliance Category** column you want to add a license entitlement for, in our example this is**Microsoft Corporation**,**Visual Studio**.





10.4.12.2 To create and publish a license entitlement:

This displays the**New License**page, for this example, we set the following fields to create the license entitlement:

> **Note**
>
> These steps can also be carried out directly on the**Entitlements - Licenses /Maintenances**page and clicking on**New License**, but the prefilled information will not be there and you will need to enter that yourself.

Select the displayed product and click**Add License**, located just to the right.

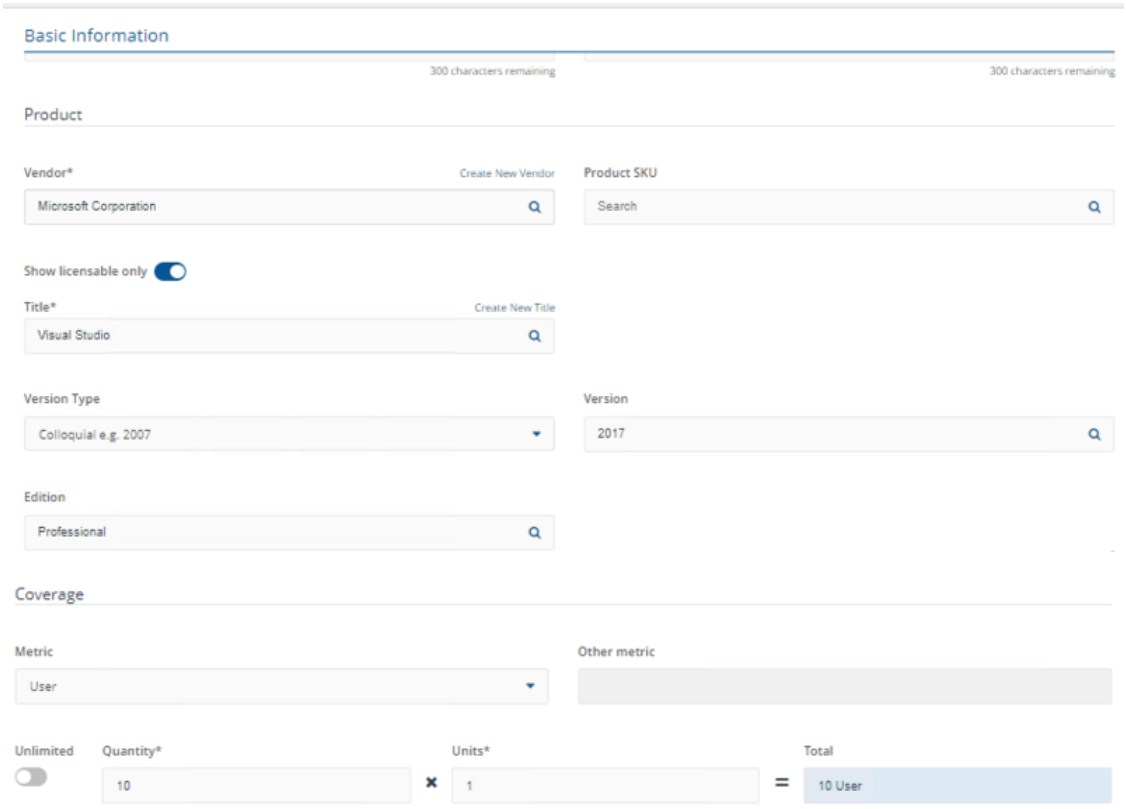
In the **New License** page we will choose a specific set of options to show how this page works. For more details on all the fields in this page please refer to New License page.

There are lots of fields on the page but a few are mandatory. The mandatory fields have an * next to their name.

The page is split into a number of sections, we will start in the **Basic Information** section.

The **Management Group** is the first mandatory field, it's set by default to Global, but it can be changed to any of your existing Management Groups, in this example we will leave it at **Global**.

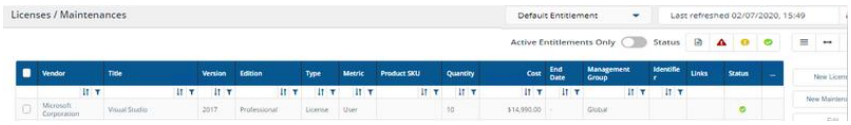
The next mandatory item is the **Vendor** field. As we have opened this page after selecting a product, any known fields are prepopulated. Where they are not, then as you start to type information suggestions are shown which are brought in from 1E Catalog.



Now everything is set how we want it lets make this license entitlement take effect. To do this we click the **Publish** button at the bottom of the page. We could have clicked **Save draft**, if we were in the middle of making changes and didn't want to make the license active and the license would have been saved as draft in the **Licenses / Maintenances** page.

Having published the license entitlement an entry now appears in the **Licenses / Maintenances** page.

The License we just published is shown with a green tick next to it, those in draft have a paper icon next to them.



For this simple example we populated the following fields:

Title: Visual Studio

Edition: Professional

Version Type: Colloquial

Version: 2017

Metric Type: User (Device is default selection)

Quantity: 10 (For other more complex metric types, you will need to adjust the **Quantity** accordingly. For example, Microsoft Office 365 may be purchased in blocks of 5 devices, so if you bought 10 licenses at 5 devices each you would need to enter 50 in the **Quantity** field)

Entitlement Type: Perpetual

Start date: to the date the license started, or is due to start on. In our example, it's set to the default of the current date

Duration set the duration of the license, this will be required if the license is not Perpetual

Version Downgrade: We now ensure that the both **Available** and **Persistent** check boxes under the **Rights** section are checked, as it should be by default. This will confirm that this license can be applied to earlier versions of Windows Server.

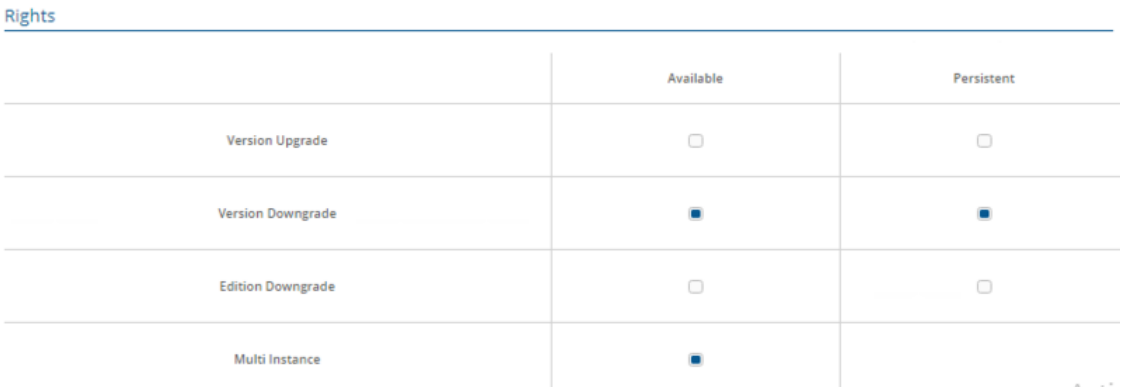
Costs: 150

Multi Instance: you must **ensure this is checked** to set the license as one that applies across multiple devices (In case of **User metric** based licenses, **Multi Instance right is compulsory**)

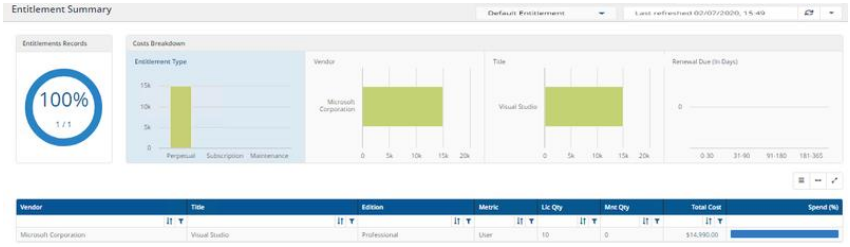
Currency: is already set to **USD** by default. AppClarity then calculates the total cost of the 10 licenses.

> **Note**
>
> **Edition Downgrade** has been improved. For example Visual Studio can have multiple editions like Ultimate, Professional and Enterprise editions. In previous versions of AppClarity if you used Visual Studio Enterprise and in other addition downgraded versions like Visual Studio Professional, the lower version also consumed the same license as Visual Studio Enterprise.
>
> If you only have an entitlement for Visual Studio Enterprise in your Inventory, the Enterprise license will cover Visual Studio Enterprise but also downgraded versions like Visual Studio Professional and Visual Studio Ultimate.

> **Note**
>
> You must ensure you check the **Multi Instance** checkbox to set the license as one that applies across multiple devices, otherwise setting the license by user will not work.

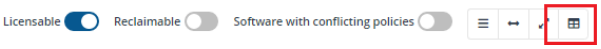


On publishing an entitlement, the **Entitlement Consolidation** report is refreshed. Once this is done, the data can be seen on the **Entitlement Summary** page.



To make a published license entitlement take effect you have to run the **Compliance** report:

> **Note**
>
> You can refresh reports from individual AppClarity screens as well as using the **Settings** App. You can do this by using the refresh icon next to the**Last Refreshed**box, for example:
>
>
>
>
> For a complete list of the specific reports you can run from particular pages refer to Running your first Compliance License Summary: Refresh Reports.

> **Note**
>
> You can choose which columns are displayed in Inventory and AppClarity detail tables to increase readability. On pages where you can pick the displayed columns you'll see a new control like the one highlighted below:
>
> 
>
>
> To find out more about this feature refer to Running your first Compliance License Summary: Choosing the columns to display in reports.

Navigate to the **Settings→Connectors** page and click on the **Execute** button.

The **Execute** action popup is displayed, enter the following:

Navigate to **Settings→Monitoring→Process Log** and wait for the action to complete, this will be **Compliance** and will have a green tick in the **Status** column when complete.

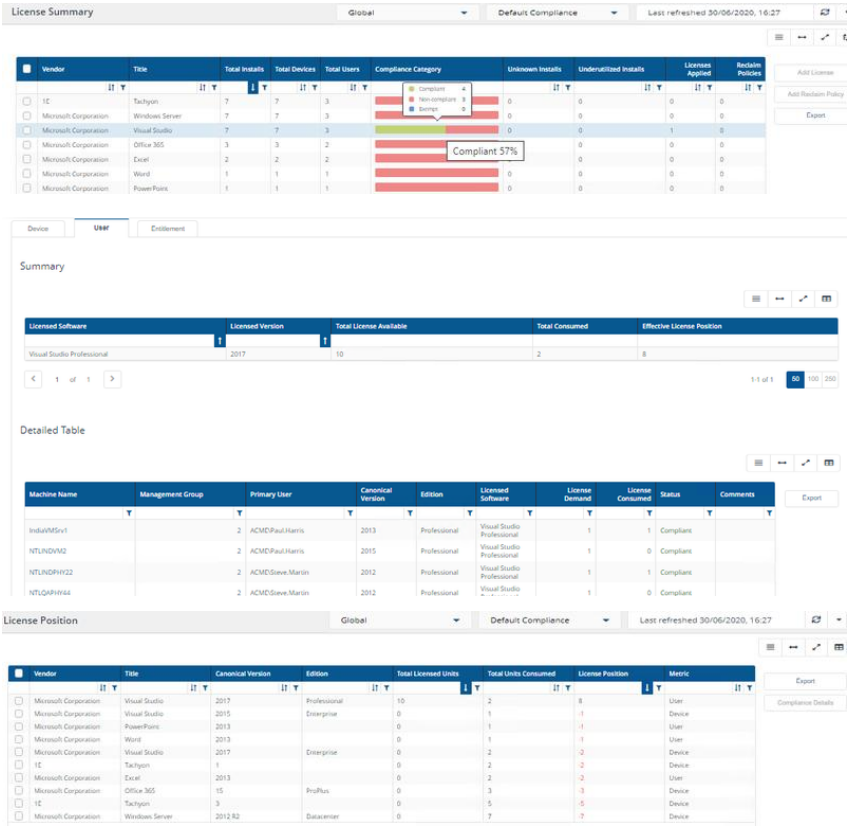
Navigate to the **AppClarity→Compliance→License Position** page.

In this example, you can see that **Visual Studio Professional** is now **Compliant** for 4 devices but with only 2 users**.**

> **Visual Studio Professional** has 4 installations on 4 devices. But, only 2 user metric based licenses were consumed as only 2 users were accessing these 4 devices.

Repository: Default Compliance

Action: Generate Report - Compliance



10.4.13 Calculating license demand

To calculate the license demand, you need to refresh the report you are interested in. In our example we have refreshed all three reports.

> **Note**
>
> The License Demand Compliance (LDC) reports do not take into account any current entitlements set in AppClarity. They are purely for the purpose of determining the overall number of license units that would be required to make the installations compliant. In effect, the LDC reports answer the following question:
>
> If you currently had no licenses how many licenses,in the most efficient arrangement,would you need to procure in order to become compliant?

To run and view License Demand Compliance (LDC) reports :

Switch to **AppClarity→License Demand**.

On the **License Demand Calculation Report** screen, select your compliance repository from the dropdown list.

Click **Refresh** for each report.

Once the report refresh shows as complete, click **View Report**.

The displayed summary table lists **Licensed Software**, the total number of **Installs**, **License Demand** and **Unknown Installs**. You also have the option to select one or multiple titles and then clicking **Show Detailed Report** to further explore and filter the number of selected titles.

You may want to find out the quantity of licenses you would need to purchase or submit into AppClarity in order to make your product compliant. AppClarity provides license demand calculation reports that perform complex licensing calculations to find out what your ideal licensing position should be.

The complex server licensing covers four major reports of different vendors, for the most used and most expensive forms of licensing that occur in customer environments:

Microsoft Core License Demand

IBM Processor Value Unit (PVU) License Demand

Oracle Processor License Demand

Red Hat Socket Demand.

The Microsoft Core License Demand report includes Windows Server OS licensing because it is core-based, and therefore it is now included in our Microsoft Core License Demand.

To view and refresh these reports, the logged-in user must have any of the user roles:

License Demand Calculation Report (LDC) page	Role
View a License Demand Calculation (LDC) pages	Full Administrator
	Compliance Administrator
	Compliance Viewer
Refresh a License Demand Calculation (LDC) Report	Full Administrator
	Compliance Administrator

Refer to AppClarity user roles for more information about Role Based Access Controls (RBAC) in AppClarity. In future versions of AppClarity we plan to extend the number of vendors and products available. This example focuses on the Microsoft Core License Demand report.

10.4.13.1 Summary table

At the top of the page is a summary, where the primary bit of information is what AppClarity has estimated as the license demand. This appears under the **License Demand** column for each product.

The example shows the **Microsoft Core License Demand** for SQL Server (for Standard and Enterprise editions) displaying the unknown (or unparented) installation for its components, for example Reporting Services and Analysis Services.

In the example, both the **SQL Server Integration Services** and **SQL Server Reporting Services** show 0 **Installs** and 248 and 67 **Unknown Installs** respectively:

SQL Server Enterprise - License Demand indicates you would need to buy 1,310 cores licenses to be compliant

SQL Server Standard - License Demand indicates you would need to buy 970cores licenses to be compliant.

The example also shows the **Microsoft Core License Demand** for Windows Server Enterprise and Windows Server Standard, for this calculation:

Windows Server Enterprise - License Demand indicates that you would need to buy 4,192 cores licensesto be compliant

Windows Server Standard - License Demand indicates that you would need to buy 24,130 cores licensesto be compliant.

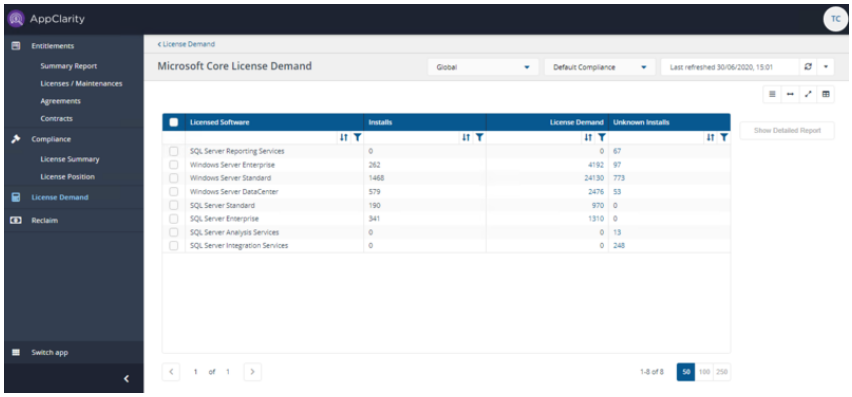
This value is calculated by incorporating all the licensing schemes for SQL Server and Windows Server that Microsoft provides in order to derive the most efficient value. Clicking on one of these values will take you to the rows in the detailed table displaying the installations on devices.

> **Note**
>
> There are some common reasons why **Unknown Installs** prevent License Demand from being calculated:

The host information is unknown to AppClarity

The hardware information (i.e., no of cores) is unknown to AppClarity

Any SQL Server component (For example, SQL Server Integration Services or Reporting Services) does not have a parent installation on any device (i.e., on any device, only the component is installed, and SQL Server installation is missing).



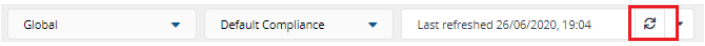
10.4.13.2 Detailed Report table

In the rest of the report, a table is displayed where each row shows the installation for the product on a particular device (Physical servers, physical host with VM's or Clusters). The **License Demand** value for each **Machine Name** row in the table is added together to form the summary **License Demand** value. The table is sorted by the different **Licensed Software** column.

The rows in the table are also organized into clusters containing **Physical Host** containing the physical hosts and the virtual guests they are hosting. It is important to see this relationship as this can sometimes make a significant difference to the license requirements. The table also shows the hardware information which again can make a difference to the license requirements.

Note

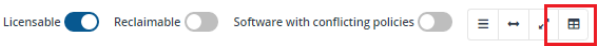
You can refresh reports from individual AppClarity screens as well as using the **Settings** App. You can do this by using the refresh icon next to the**Last Refreshed**box, for example:



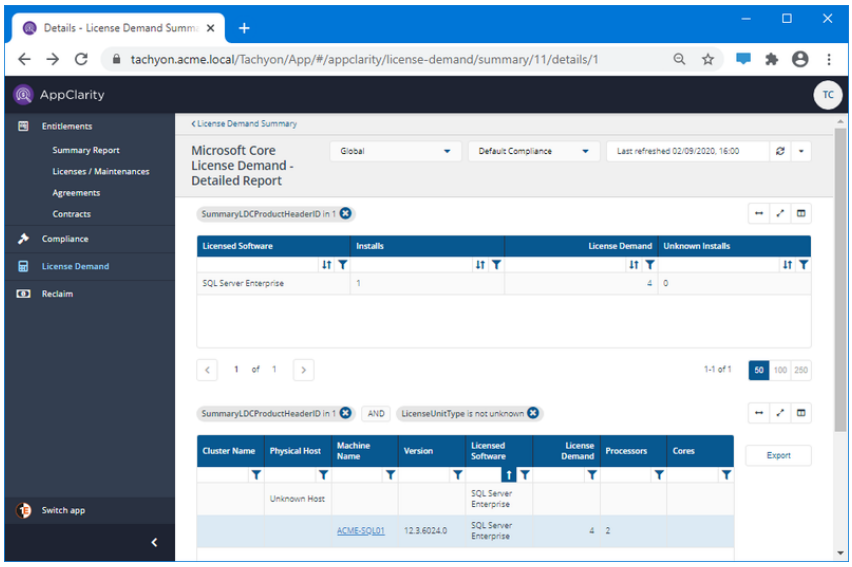
For a complete list of the specific reports you can run from particular pages refer to Running your first Compliance License Summary: Refresh Reports.

Note

You can choose which columns are displayed in Inventory and AppClarity detail tables to increase readability. On pages where you can pick the displayed columns you'll see a new control like the one highlighted below:

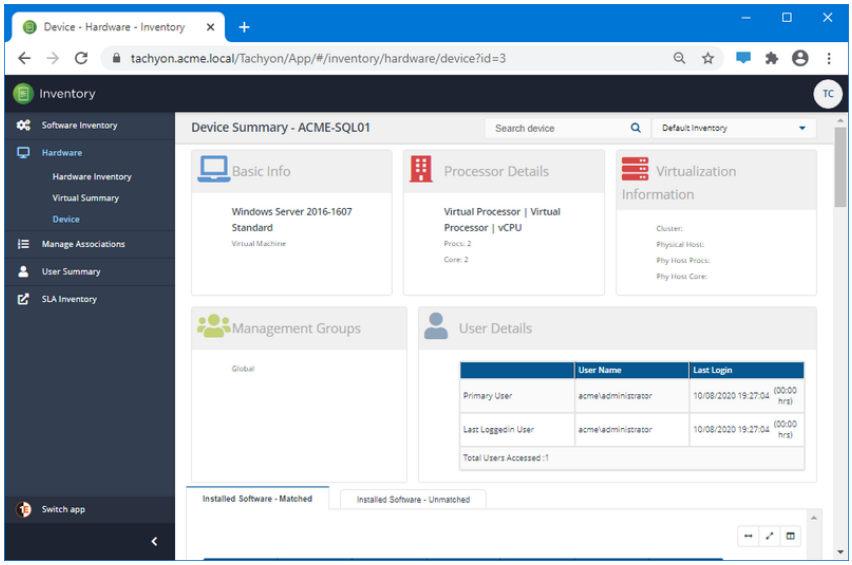


To find out more about this feature refer to Running your first Compliance License Summary: Choosing the columns to display in reports.



Entries in the **Machine Name** column are links to the corresponding **Device Summary** for that machine in the Inventory app.

In our example by clicking on ACME-SQL01 in the **device Name** column we can view the device's associated **Device Summary** in **Inventory**→**Hardware**→**Device**.



To automatically refresh a report for a repository you can set up a schedule:

Under the **Settings**→Configuration→Schedules and click **Add**.

In the Add schedule screen for:

Schedule name - enter a logical name for the new schedule.

Repository - select your repository from the dropdown menu.

Action type - select the associated action type you want to schedule.

Frequency - select the frequency.

> **Note**
>
> For any entitlement repository, when a new entitlement is created (which triggers an entitlement consolidation) a **Schedule** called **EntitlementConsolidationScheduler** is created for this repository by default, it's set to run on a 24 hrs frequency (daily basis).

10.4.14 Excluding devices from License Demand Calculation using Management Groups

It may be required to exclude some groups of machines from LDC or Compliance reporting, as these may be for developer's devices for which an exemption is permitted and therefore the software on those devices should not be considered in the count of licenses. In AppClarity 8.1 this exemption is carried out by adding the machines to a Management Group. The naming convention of the Management group is very specific and care should be taken when creating it, the name is of the format:

License Exemption OR

License Exemption - Vendor name OR

License Exemption - Vendor name "Identifier for Management group"

Each of these has a specific function, the first will exclude all software for the machines in the group from the LDC and Compliance, the others will exclude all software for the specified vendor from the LDC and Compliance.

For the same vendor, two separate management groups could be created as below, and devices falling in either management group would exempt them for SQL Server installations from the Microsoft Core LDC, and in the Compliance Reporting, all installations where the Vendor is Microsoft Corporation will be excluded from the device (this would include, SQL Server, Office 365, Visual Studio etc.).

License Exemption - Microsoft Corporation

License Exemption - Microsoft Corporation "for MSDN licenses".

> **Warning**
>
> Take care when naming Management groups, as any misspelling of the License Exemption, the Vendor or inappropriate spacing will result in the exemption of installations not being applied.

Remember that when being audited for Compliance, you may have to prove that you are entitled to exempt machines from licensing.

10.4.14.1 Create an Exclusion Management Group

The devices to be excluded need to be added to an Exclusion Management Group. This Exclusion group has a specific naming convention mentioned above, and because all products or all products for a specific vendor will be excluded, care should be taken when populating these groups. The creation and population of Management groups are documented here Management Groups page. The user creating the Management group will require the **Group Administrator** role.

10.4.14.1.1Create the Microsoft Corporation exclusion Management group

In this example, we will exclude Microsoft Products from the Development Computers OU:

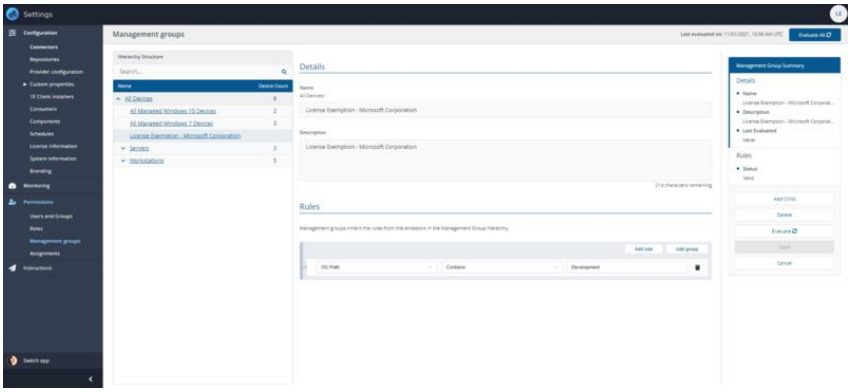
In the **Settings** application, navigate to **Permissions**→**Management groups.**

Create the Management Group with name as **License Exemption - Microsoft Corporation**.

In rules, add the **OU path contains Development**.

Save the Management Group, the screen is shown to the right.

Evaluate the Management Groups by clicking the Evaluate button on the right of the Management groups screen.



10.4.14.2 View the effect of creating the exclusion

The exclusion will take place at the next scheduled refresh/run of the 'Compliance' action against associated compliance repository or refreshing the License Demand report for Microsoft Core License Demand, or it can be run on demand, the following roles have these permissions:

AppClarity Administrator

Compliance Administrator.

To run on demand:

Switch App **Settings**→**Monitoring**→**Process log**

Click **Execute** and select:

Repository: **Default Compliance**.

Action: **Generate Report - Compliance** and then Click **Execute** button.

Monitor the progress in the **Process log**.

10.4.14.2.1View the LDC - Microsoft Core License Demand report

As one of the following users, open AppClarity, and navigate to License Demand:

AppClarity Administrator

Compliance Administrator.

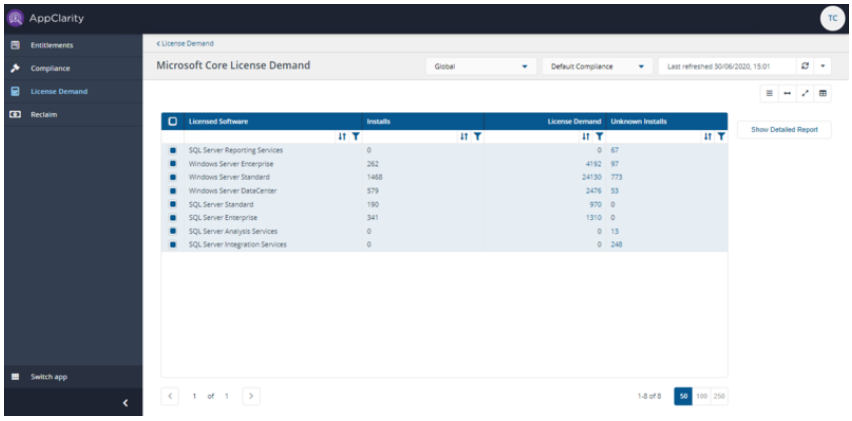
Click on **Refresh** in the Microsoft Core License Demand tile.

When the refresh completes, **Last run: a few seconds ago** shows.

Click on **View Report.**

Select the select all checkbox next to the Licensed Software column title.

Click Show Detailed Report.

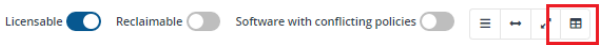


Microsoft Core License Demand - Detailed Report will be displayed. In the example to the right, we have added the Management Group and Comments columns to the default display.

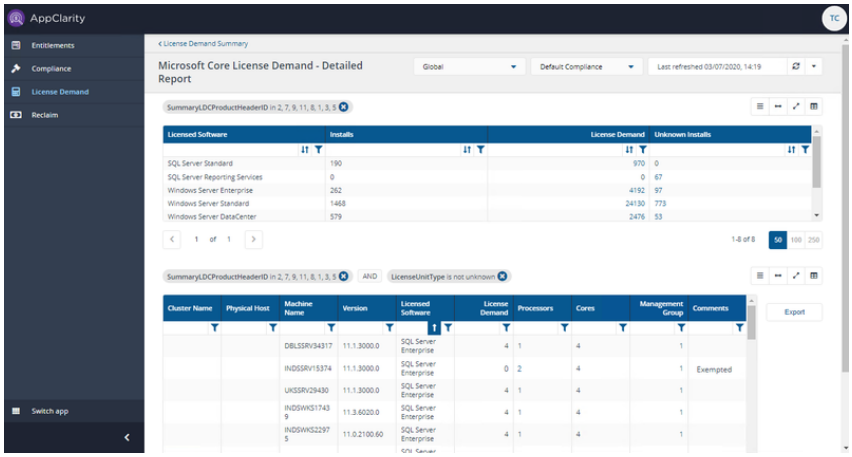
Under column name **Comments**, any installations which had been excluded from license demand calculation, would display the comment as **Excempted**. Also, License Demand value displays as 0 under **License Demand** column.

Note

You can choose which columns are displayed in Inventory and AppClarity detail tables to increase readability. On pages where you can pick the displayed columns you'll see a new control like the one highlighted below:



To find out more about this feature refer to Running your first Compliance License Summary: Choosing the columns to display in reports.



In the Management Group Column, on clicking the value displays the group the machine is a member of, clicking this shows that the machine is a member of 2 groups:

License Exemption - Microsoft Corporation

Global.

Management Group(s)

License Exemption - Microsoft Corporation
Global

10.4.14.2.2View the Compliance - License Summary report

Users with these roles:

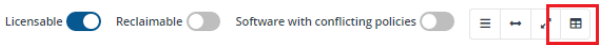
AppClarity Administrator

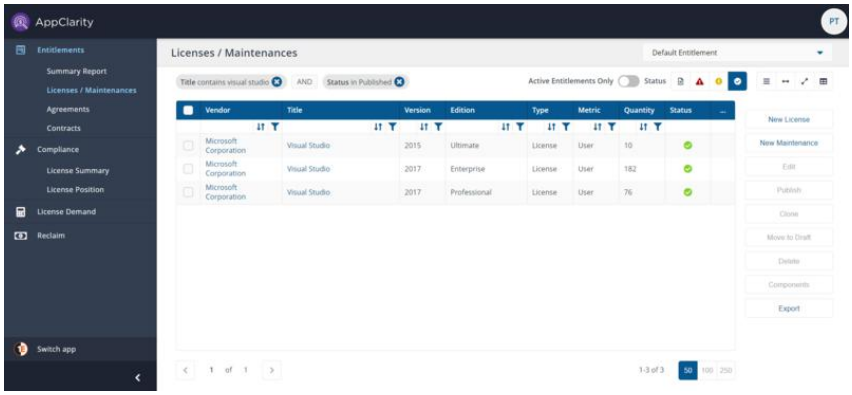
Compliance Administrator

Compliance Viewer.

Can carry out these instructions, open AppClarity, and navigate to **Entitlements - Licenses / Maintenances**. To view results of an exclusion, you MUST have published a License, in this example we will look at Visual Studio.

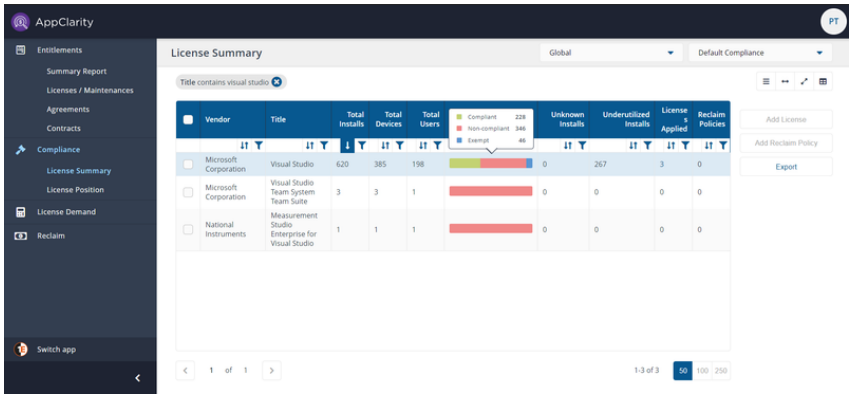
The License for Visual Studio in this example applies to all versions, is User based, there are 100 Licenses and it is published. In this example we have added the Status column to the default displayed columns.

> **Note**
>
> You can choose which columns are displayed in Inventory and AppClarity detail tables to increase readability. On pages where you can pick the displayed columns you'll see a new control like the one highlighted below:
>
> 
>
>
> To find out more about this feature refer to Running your first Compliance License Summary: Choosing the columns to display in reports.



Now we have confirmed we have published a License, navigate to **Compliance - License Summary**.

Viewing the entry for Visual Studio, we can see that the Compliance Category Column has a bar showing Green, Red and Blue, floating over this shows that we have 228 Compliant, 346 Non-compliant and 46 Exempt.



Click on the Compliance Category Column bar for Visual Studio, this opens the Summary by Installs - Microsoft Corporation Visual Studio Page, the page defaults to the Global Management group.

Select **License Exemption - Microsoft Corporation** the page will display as shown.

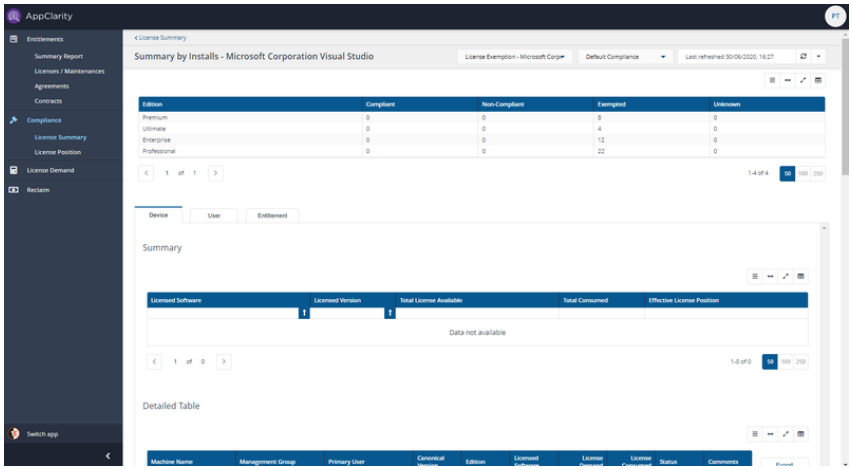
Observe that there are multiple entries for machine DBLSANY19431 and user UserName_33775, however looking at the Canonical Version and Edition we can see that these are all distinct entries for the application.

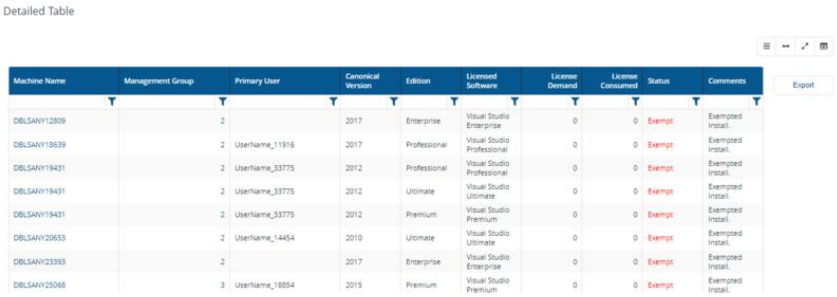
Also, the Status is Compliant, and the Comments show as exempted.

Note

You can refresh reports from individual AppClarity screens as well as using the **Settings** App. You can do this by using the refresh icon next to the**Last Refreshed**box, for example:

For a complete list of the specific reports you can run from particular pages refer to [Running your first Compliance License Summary: Refresh Reports].





We have now looked at the creation of a Management group to add an exemption for Microsoft Corporation, and show how to apply and verify its application. This can be carried out for any Vendor, by amending the Vendor section of the Management Group name.

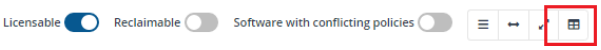
10.4.15 Reclaiming a product based on its usage

Inventory fetches information from its data sources to return details of how products are being used, wherever available. Reclaim Administrators who are interested in reclaiming unused software in order to recycle licenses can use this information to set their reclaim policies.

We'll start with a simple example based on reclaiming unused versions of a software. In this case the policy we set up will be soft (optional) in that it will only trigger a reclaim that allows the user to opt out and keep the software, as long as they provide suitable justification. In this example we use the global management group, more on that later.

This example assumes that you have already run a sync on your selected inventory repository to retrieve inventory data from one or more connector sources. As a result of doing this a number of reports are automatically run. The essential one, particularly for reclaim, is:

Reclaim Product Usage is run on the compliance repository associated with your chosen inventory repository. In our example we use the **Default Compliance** repository (which is automatically associated with the **Default Inventory**).

> **Note**
>
> You can choose which columns are displayed in Inventory and AppClarity detail tables to increase readability. On pages where you can pick the displayed columns you'll see a new control like the one highlighted below:
>
> 
>
>
> To find out more about this feature refer to Running your first Compliance License Summary: Choosing the columns to display in reports.

To view the current product usage and create a reclaim policy for a particular product:

Navigate to the **AppClarity**→**Reclaim**→**Usage Summary**→Reclaim Usage page.

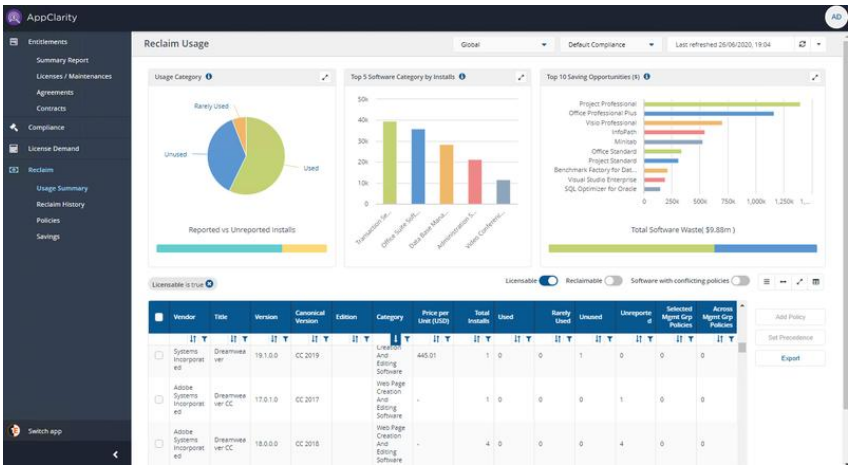
> **Note**
>
> The first thing to notice is how this page displays a chart of software organized according to the four usage categories for software in the inventory. Three categories are for reported usage:, **Used**, **Rarely Used**, **Unused**, and the 4th category is

Unreported. The pie chart shows the proportions of the **reported** categories. The bar underneath shows the proportions of **unreported** and **reported**.

The next thing to notice is that there is a filter set by default that limits the display to the selected management group, in our example the **Global** management group, and another filter that limits the display to licensable products only. You can remove these filters if you don't see the software you want to reclaim. Your charts will only show the categories which your software fall into, and how you apply filters.

Unused software is usually the best candidate for reclaim.

Please refer to Usage categories for a detailed understanding of how usage categories are calculated.



In our example let's investigate **Project Professional** for example, you could do this by filtering the table view by **Title** containing **Project** and by **Edition** containing **Professional** or if you know the version, by filtering on **Version**.

For our example we'll focus on **Project Professional 2013**, notice there are 116 **Total Installs**, 30 **Used**, 16 **Rarely Used**, 45 **Unused** and 25 **Unreported products**. Please refer to Usage Summary page for more details on how this page works and the columns displayed in the table. In our example you can see the usage details for the **Project Professional 2013** product indicating that it has **45** unused installations and there are no reclaim policies currently set for it.

You can click on the **Add Policy** button on the left side of the **Reclaim Usage** page after selecting the product. Doing this displays the **New Policy** page with the details pre-filled with the information related to the selected product, please refer to the New Policy page for more details on how this page works. Here you can see the following information has been set automatically:

Note

Vendor is set to **Microsoft Corporation**

Title is set to **Project**

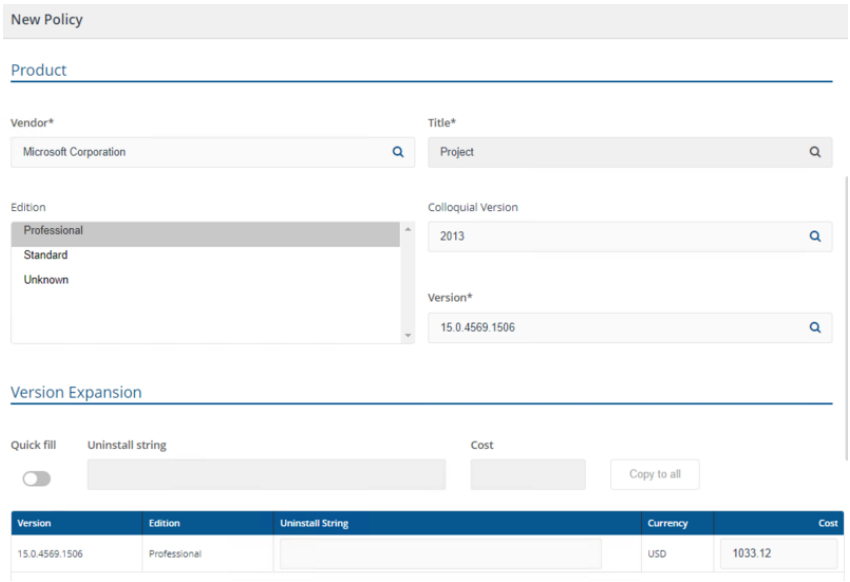
Edition is selected as **Professional**

Colloquial Version is set to **2013**

Version is set to **15.0.4569.1506**

Version Expansion is already expanded to that same version.

> **Note**
>
> There are constraints on the fields when you enter the information manually that you won't necessarily encounter in a pre-filled **New Policy** page like this one. Please refer to the New Policy page for more details on those constraints.



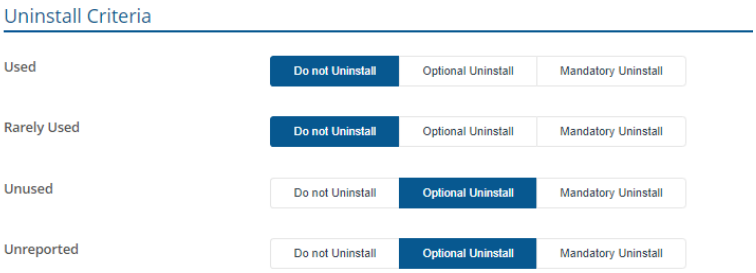
We can now decide which devices where the reclaim policy will run by applying the policy to a management group. You can select the global management group (also known as All Devices) by checking the **Global** checkbox.

We also want to publish the reclaim policy straight away and have it active, so we ensure that the **Enabled** checkbox is checked.

Now we set the reclaim aspects of the policy. There are four **Uninstall Criteria** controls corresponding to each of the software usage categories, where you can select the action to take if the target software is in that category.

In our example we want to leave the **Used** and **Rarely Used** controls at their default of **Do not Uninstall**.

For **Unused** and **Unreported** we want to set both of these to **Optional Uninstall**. This will mean that users on the devices where the targeted software in those states are installed will receive a notification requesting to uninstall the software.



Having set the policy we can now click **Publish** to start the process of making the policy active.

The new reclaim policy now appears on the **Policies** page, it's reported as **Is Enabled = TRUE** and **Status = Published** AppClarity will now make the policy live by automatically running the **Reclaim Consolidation** report.

> **Tip**
>
> When setting up a reclaim policy, for example for Notepad++, if you know **uninstall command line**, then you may enter it inside **Uninstall string** box for the version. Please follow these rules.

Each uninstall command line must be **enclosed** in **double quotes** - for example:

```
"C:\Program Files (x86)\Notepad++\Uninstall.exe"
```

You can use **multiple command lines** for same product version which are tried in succession. Ensure each command line is **enclosed** in **double quotes**, and **separated** by **double pipe character ("||") .** For example:

```
"C:\Program Files (x86)\Notepad++\Uninstall.exe"||"C:\All Softwares\Notepad++\Uninstall.exe"||"C:\Tools\Notepad++\Uninstall.exe"||"D:\Softwares\Notepad++\Uninstall.exe"
```

10.4.15.1 What the end-user sees

Let's suppose there is a device where the target software is installed and it is in the unused usage category. The reclaimer should have been configured to run on each device where reclaim is supported, this is done in two modes:

Is in mandatory mode, usually scheduled to run overnight on the device.

Is in opt-out mode, usually scheduled to run during the day when the end-user is logged on to the device.

When the reclaimer on that device runs in opt-out mode to fetch policies, it will be informed that it needs to start the process of uninstalling the software in opt-out mode. This will mean that an **reclaimer opt out** notification dialog will be displayed to the next end-user that logs on, informing them that a particular software title on their device is reported as not having been used and is therefore due for a reclaim. In more detail:

The dialog shows them:

the name of the software.

the cost that would be recovered by reclaiming the software.

the last time the software was used.

The end-user then has the choice of:

Clicking on the **I still need this** link, and entering a suitable reason why the software should not be reclaimed.

Clicking the **Remove software button**, in which case the software is marked for immediate uninstallation.

Clicking the **Remove software later** button, in which case the software will be scheduled for uninstallation at some point in the future and not for immediate uninstallation.

In our example the end-user chooses to keep the software by clicking on the **I still need this** link and providing a suitable reason. Doing this displays the **Confirm software use** dialog.

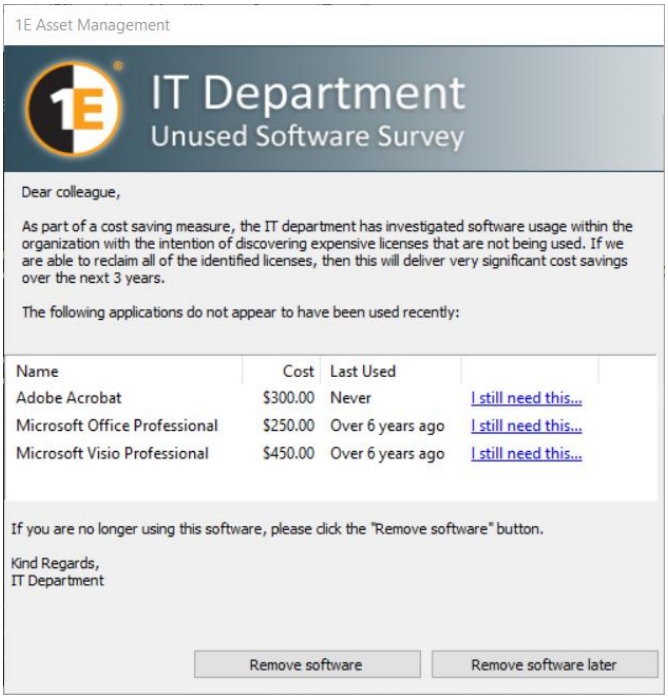
The user enters their reasons for retaining the software and then clicks the **OK** button.

The **Confirm software use** and the **reclaimer opot out** dialogs both close.

The user has provided their reasons, it's now up to the AppClarity administrator to accept or reject their request to retain the software.

Tip

Please refer to Deploying Software Reclaimer for more details about customizing, deploying and testing the Software Reclaimer.



10.4.15.2 Responding to an end-user request to retain reclaimable software

After you've created some opt-out reclaim policies you will need to keep track of the ones that are currently in operation and requires attention from reclaim administrator.

To administer software reclaim policies:

Navigate to the **AppClarity→Reclaim→Policies** page, you may need to refresh the page if you are already there.

Locate the required reclaim policy, you should see that the **Admin Actions** column shows **1**, indicating that there is one pending request to be processed.

Clicking on the number in the **Admin Actions** column displays the **Administration** page for that reclaim policy, please refer to Administration page for more details.

Here you can see the reclaims that have been completed for this policy and the reclaims still in progress. At the bottom of the page is the **Reclaim Override Management** table that lets you respond to requests for retaining software. To respond to a particular request you do the following:

Check the checkbox at the start of the request entry in the table

You then have the option of:

Clicking the **Accept** button to accept the end-user request to retain the software

Clicking the **Reject** button, in which case the optional software reclaim will be converted to a mandatory reclaim and the software will be removed without any further interaction with the end-user in very next cycle.

In our example we click the **Accept** button to allow the end-user to start using the software again, as they indicated in their reason.

A notification popup appears saying that the user's opt out request has been accepted and that the software will not be reclaimed at this time. Click on **OK** to close the notification.

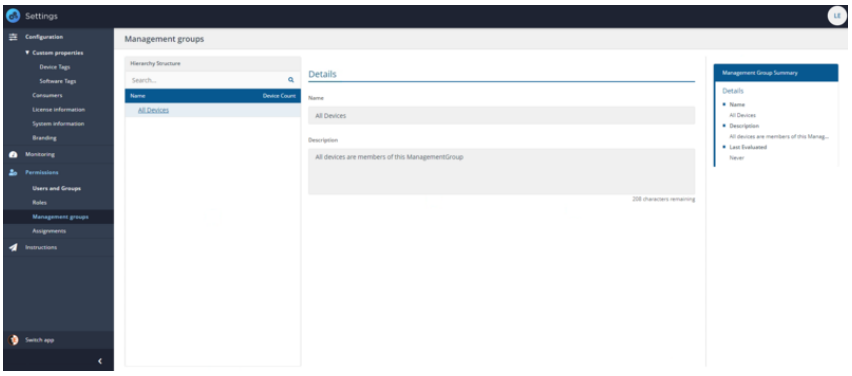
Clicking on the **AppClarity→Reclaim→Polices** page shows that there are now **0 Admin Actions** for this software reclaim policy.

10.4.15.3 Resolving overlapping reclaim policies

As a result of defining reclaim policies you may find that they overlap in terms of the devices and products they apply to. Only one policy can be applied for a given device and product and to resolve the conflict you can set the precedence to decide which of your policies are preferred. This becomes significant when management groups are involved.

> **Note**
>
> Click here to see how to create the management groups for this example...
>
> **Tip**
>
> Here we present an overview for the management groups used by this reclaim example. For detailed instructions on creating management groups please refer to Management Groups page.
>
> **Management Groups - tutorial**
>
> **In this tutorial**
>
> In this tutorial, we add a number of Management Groups for the ACME organization: one that uses the name of the devices and several that use the Organizational Unit (OU)

the devices belong to. The following picture shows what we have in our example Active Directory and how this will appear as Management Groups in Tachyon. Here you can see there are two servers in the AD Computers group, an additional Domain Controller server and five workstations in the OU.



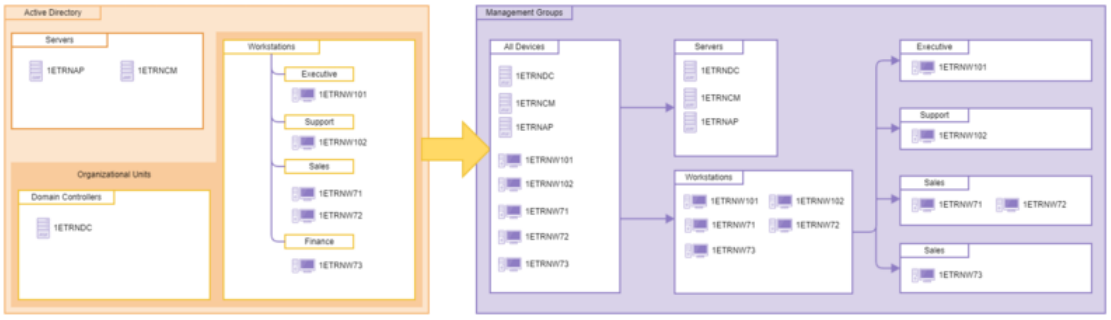
By the end of this example, you will have added six Management Groups in addition to the default All Devices Management Group:

All Devices - this Management Group brings all devices into a single Management Group

Servers, Workstations, Executive, Support, Sales and Finance - these Management Groups will use an OU rule to separate the devices according to the OU they belong to.

Note

If you want to take advantage of your Configuration Manager database, and pull in its inventory and usage data, so that you can mirror your Active Directory OU structure in your Management Groups, then you'll need to configure a System Center Configuration Manager connector in your Tachyon system.



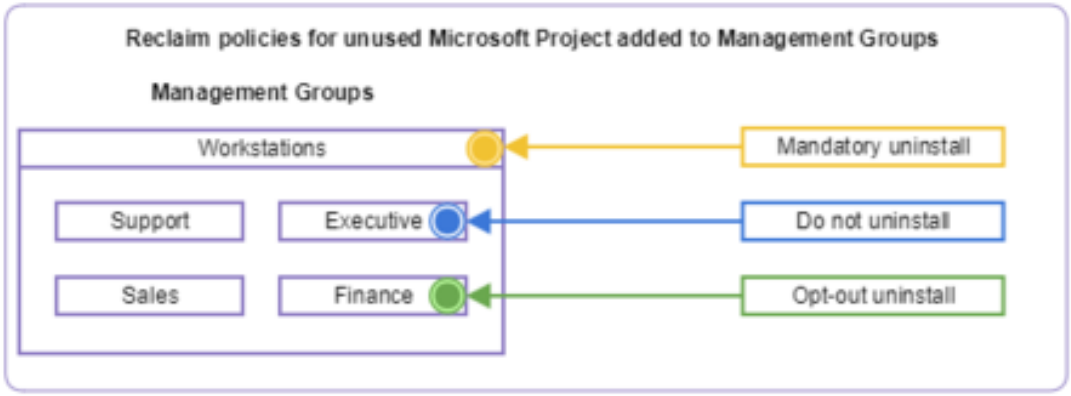
In this example

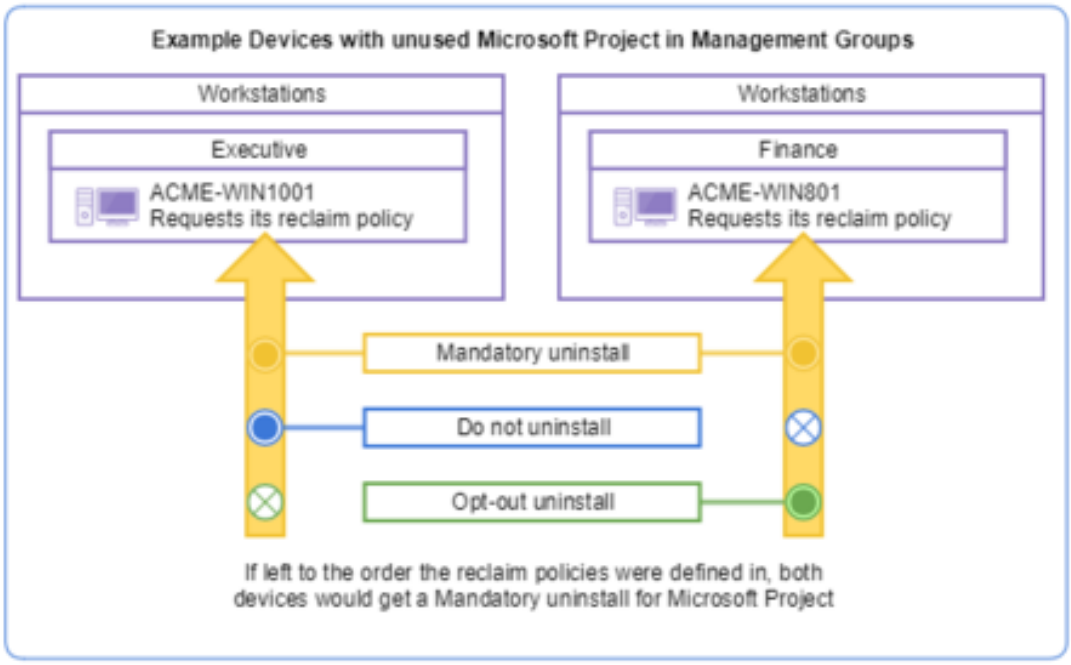
In this example we create three reclaim policies that target unused installations of Microsoft Project Professional. These overlapping policies will have different reclaim actions for unused software depending on the management groups, that come from the management group example above.

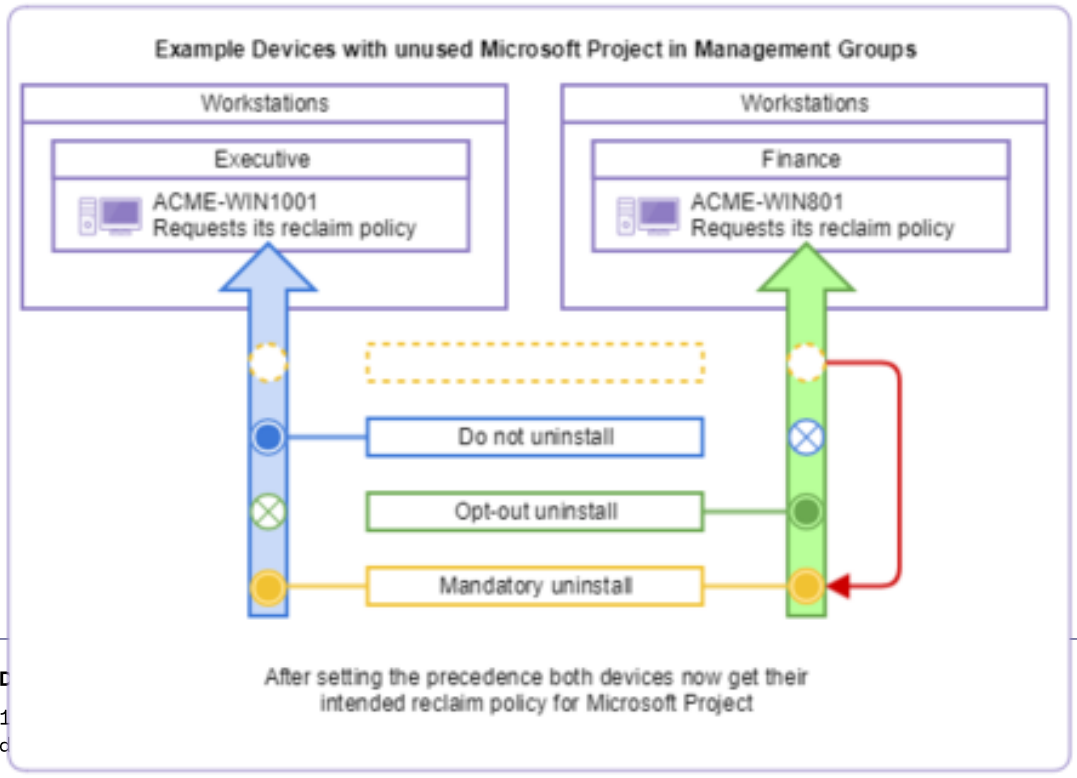
We will use three management groups which correspond to OU configured on our example ACME AD site. The first one, **Workstations** contains all the devices that are present in the other two, **Executive** and **Finance**, but those two sub OU are mutually exclusive. This means that devices in the **Executive** management group are also in the **Workstations** management and likewise devices in the **Finance** management group are also in the **Workstations** management group.

The purpose of this example is to create three reclaim policies for unused installations of Microsoft Project Professional for each of the **Workstations**, **Executive** and **Finance** management groups. Each reclaim policy will have a different reclaim action according to the management group they are associated with. However, in practice this means that the devices in the **Executive** and **Finance** management groups with their own reclaim policies will also be eligible for the reclaim policy associated with the **Workstations** management group.

For this reason a mechanism exists to set the precedence for the reclaim policies associated with a particular program so that you can ensure that the devices in each management group get the right reclaim policy.


Reclaim policies for unused Microsoft Project added to Management Groups
Management Groups
Workstations
Support
Executive
Sales
Finance
Mandatory uninstall
Do not uninstall
Opt-out uninstall


Example Devices with unused Microsoft Project in Management Groups
Workstations
Executive
ACME-WIN1001
Requests its reclaim policy
Workstations
Finance
ACME-WIN801
Requests its reclaim policy
Mandatory uninstall
Do not uninstall
Opt-out uninstall
If left to the order the reclaim policies were defined in, both devices would get a Mandatory uninstall for Microsoft Project


Example Devices with unused Microsoft Project in Management Groups
Workstations
Executive
ACME-WIN1001
Requests its reclaim policy
Workstations
Finance
ACME-WIN801
Requests its reclaim policy
Do not uninstall
Opt-out uninstall
Mandatory uninstall
After setting the precedence both devices now get their intended reclaim policy for Microsoft Project

By the end of this example you will have defined 3 new reclaim policies:

In the **Workstations** management group we will create a general policy that performs a mandatory uninstallation.

In the **Finance** management group we will create an opt-out uninstallation where the end-user can choose to keep the software.

For the **Executive** management group we will create a do not uninstall action for Microsoft Project Professional.

You will then have set the precedence for the policies so that they are selected in the correct order when a device runs its scheduled reclaimer policy retrieval.

In our example we have three Management Groups we are interested in: **Workstations**, **Executive** and **Finance**. You can set Management Groups up in **Settings->Permissions**->Management groups. The creation and population of Management groups is documented in the Management Groups page.

To set reclaim policies in each of these management groups:

Navigate to **AppClarity→Reclaim→Usage Summary**. In our example, we'll create our first reclaim policy directly from some known installations of the **Microsoft Project** product showing in the **Usage Summary** pages.

Initially we filter on the unused products, which will help to focus on the unused products we want to reclaim.

In our example we filter on **Visio Standard 2013** in the **Reclaim Usage** table, on **Title** containing **Visio** and by **Edition** containing **Standard**. If you have a large number of unused products in your environment you may need to set a specific filter to find the specific one you want to reclaim.

Selecting the product and at the end of the product's entry in the table click on the **Add Policy** button.

This displays the **Reclaim Policy** page prefilled with the product's details. In our example this shows:

Vendor is set to **Microsoft Corporation**

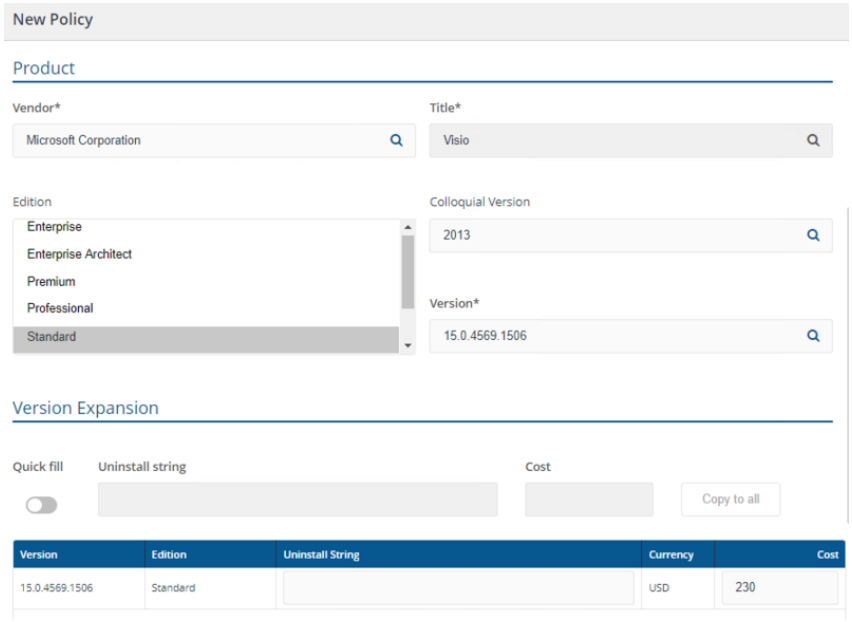
Title is set to **Visio**

Edition is selected as **Standard**

Colloquial Version is set to **2013**

Version is set to **15.0.4569.1506**

Version Expansion is already expanded to that same version.

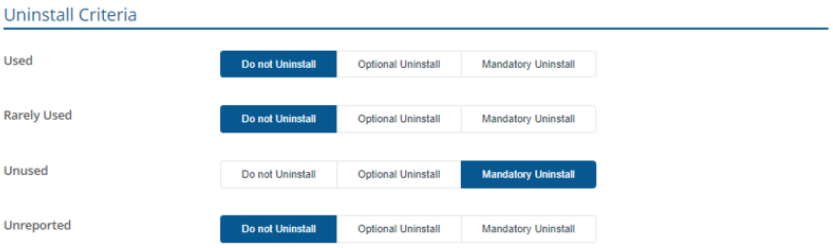


In our scenario we know that we want to create three reclaim policies for the same product which could lead to conflicts. So it makes sense to initially publish them so that they are not enabled, then resolve any conflicts and finally enable all the policies once the resolution is in place.

> In our scenario we can plan ahead, but you may encounter scenarios where you are not aware that there is another existing reclaim policy that overlaps with a new one that you want to publish. AppClarity deals with this by notifying you that there is an existing policy and automatically setting the new one so that it is not enabled, thereby giving you the opportunity to resolve the conflicts in the same way.

Having ensured that the policy is not enabled, you then select the management group the reclaim policy will be associated with. In our example this first reclaim policy for **Visio** will be associated with the **Workstations** management group.

Next, set the reclaim actions for **Used**, **Rarely Used**, **Unused**, and **Unreported**. In our example we are only concerned with the **Unused** category and leave the others at their default of **Do not Uninstall**. We then set the **Unused** action to **Mandatory Uninstall**.

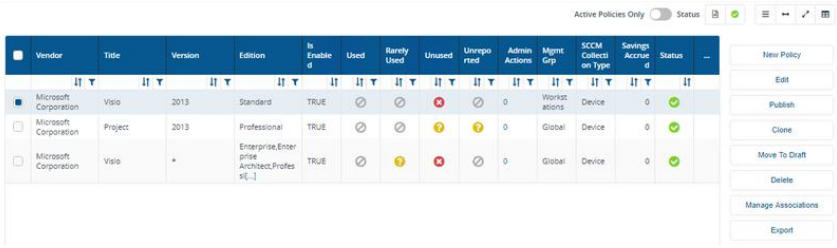


After the settings have been made click **Publish** to save the reclaim policy. This will display the **Published Reclaim Policies** page showing the saved policy.

10.4.15.3.1 Cloning a reclaim policy

In our example we want to create three reclaim policies for the same product, just in different Management Groups. We could go through the process outlined in the steps above for each of these, but a quicker method of doing this is to clone the reclaim policy we've just created:

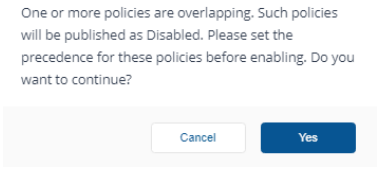
We select the policy entry for Visio Standard in the **Policies** table and then click **Clone** at the right-hand end of the reclaim policy's entry.



A new **Reclaim Policy** page will be displayed prefilled with the contents of the cloned reclaim policy.

The only things you need to change here would be the selected management group and the **Unused** category action. In our example we select the **Finance** management group and set the **Unused** category action to **Optional Uninstall**.

When you click **Publish** to save the new policy. You will then be prompted to set the precedence as you will now have overlapping policies which are published as Disabled by default.



10.4.15.3.2 Setting precedence reclaim policies

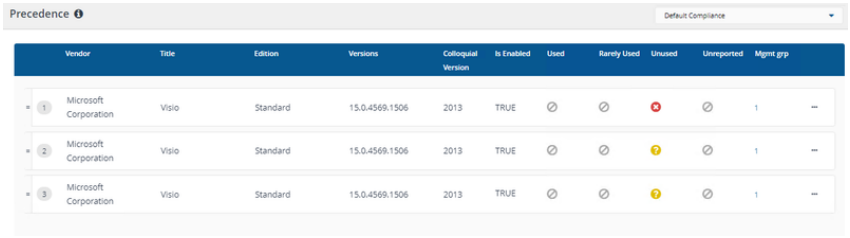
Conflicts between overlapping policies for a product are resolved from the **Reclaim Usage** page.

Navigate to **Usage Summary**.

Locate the product with overlapping policies in the **Across Mgmt Grp Policies** column. In our example we have filtered this column by **greater or equal** is set to **1**.

There is a **3** in the **Across Mgmt Grp Policies** column for **Visio Standard v15.0.4569.1506** indicating that there are 3 reclaim policies applied to this product across all management groups.

On the far side of the table we click **Set precedence**, doing this displays the **Precedence** page.



Reclaim policies are considered from top-to-bottom in this list. When the reclaimer runs on the target device, (usually according to a schedule set by the administrator who distributed the reclaimer on the network), it retrieves a single reclaim policy per targeted product from Inventory. The single reclaim policy provided to a device is dependent on the product, the management group and the order of the reclaim policy in the precedence list.

> Note the following about reclaim policies and the way they apply to devices in more than one management group:

A device can only get one policy per product

The policy for the product is dependent on the management groups the device belongs to

A device may be in more than one management group, so there may be more than one candidate policy

Reclaim may only provide one policy from the candidates, by default this is done in the order they were defined, which you can't easily control

You have to set the precedence for the policies to ensure the right one gets applied to the devices you are managing.

To set the precedence between overlapping policies you will usually need to check the Management Group that the policy belongs to. The Management Group **Names** column contains a number **Mgmt grp** link at the end of each row that displays the Management Group(s) that the policy applies to. In our example by clicking on each row we would see the reclaim policy in the:

Top row applies to the **Workstations** Management Group.

Second row applies to the **Finance** Management Group.

Third row applies to the **Executive** Management Group.

To change the precedence you can click, drag and drop (up or down) a row in the table to another position in the table. In our example we change the order of the reclaim policies in the following way:

Click and drag the reclaim policy with the **Unused Mandatory Uninstall** reclaim action, associated with the **Workstations** management group, to the bottom.

Click and drag the reclaim policy with the **Unused Optional Uninstall** reclaim action, associated with the **Finance** management group, to the second place.

The more general **Unused Mandatory Uninstall** reclaim policy associated with the **Workstations** management group is now at the bottom, this means that any device with an unused installation of **Visio Standard** in the:

Executive management group will get the **Do not Uninstall** reclaim action

Finance management group will get the **Optional Uninstall** reclaim action

Workstations management group will get the **Mandatory Uninstall** reclaim action.

At this point the reclaim consolidation report runs automatically, making the set precedence live.

We now need to enable each of the published policies to make them live:

Navigate to **Policies**.

Click on the **Edit** link at the end of one of the reclaim policy rows where the **Is Enabled** column shows **FALSE**.

Check the **Enabled** checkbox and then click **Publish**.

Repeat steps **b.** and **c.** for the other disabled policies until all the policies display **TRUE** in the **Is Enabled** column.

Our three reclaim policies for unused Visio Standard installations are now defined and associated with the **Workstations**, **Executive** and **Finance** Management Groups.

The reclaim policies have been made live and their precedence set and processed. This means that devices will subsequently receive appropriate reclaim policies for their unused Visio Standard installations depending on the management group they belong to.

10.4.15.4 Evaluating a reclaim policy without affecting your environment

If you're planning on setting up a reclaim policy want to be sure what the impact will be, (i.e. on impacted devices, where software is no longer installed and reclaimed), can evaluate your policy before setting it up. By using **Reclaim Evaluate** you can identify devices where software would be:

Marked for Mandatory Uninstall (i.e. will be removed in upcoming mandatory reclaim cycle)

Marked for Optional Uninstall.

If, after you evaluate the policy and you're comfortable with the impacted devices, you can setup the policy the same reclaim actions.

10.4.15.4.1Evaluating a Reclaim Policy

To evaluate a reclaim policy:

Navigate to **AppClarity**→**Reclaim**→**Policies** and click **New Policy**.

On **New Policy** screen, enter all the mandatory fields and all sections.

Click **Evaluate**.

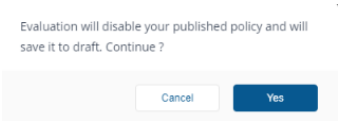
Refer to New Policy page for more details on how this page works.

The evaluate button generates a downloadable TSV file containing information about the devices and actions the policy contains.

Cost	DomainName	HostName	MatchedVendor	MatchedT	NextReclaimAction	User	UninstallAction	UsageCategory	ManagementGroup
10	1ETRN	1ETRNW71	Notepad++ Team	Notepad+	Marked for Optional uninstall	1ETRN\User	OptionalUninstall	Unreported	Global
10	1ETRN	1ETRNW72	Notepad++ Team	Notepad+	Marked for Optional uninstall	1ETRN\Tachyon_AdminPP	OptionalUninstall	Unreported	Global
10	1ETRN	1ETRNW73	Notepad++ Team	Notepad+	Marked for Optional uninstall	1ETRN\Tachyon_Admin1	OptionalUninstall	Unreported	Global
10	1ETRN	1ETRNW101	Notepad++ Team	Notepad+	Marked for Optional uninstall	1ETRN\Manager1	OptionalUninstall	Unreported	Global
10	1ETRN	1ETRNW102	Notepad++ Team	Notepad+	Marked for Optional uninstall	1ETRN\Tachyon_AdminG	OptionalUninstall	Unreported	Global

If you click evaluate on a **published policy**, you will get this warning message. Click on **Yes** and evaluate report is downloaded.

But, now this reclaim policy is converted into draft policy (i.e. not a reclaimable policy anymore). You will then have to go back click **Publish** again to move that policy back to published status and make it reclaimable. If you do not re-publish, none of the devices in your evaluate report will act on the policy.



10.4.15.5 Reclaiming a product using SCCM Uninstall

You can reclaim any software from your environment using either of these methods:

Traditional reclaim - the reclaimer included with earlier versions of AppClarity

SCCM custom Reclaim - which uses existing SCCM packages/applications added to any install collections

Using **1E SCCM Reclaim** creates an uninstall collection you can use to reclaim software using your SCCM installation.

> **Note**
>
> To use SCCM custom Reclaim, your administrator must have enabled the SCCM Uninstall Provider.

10.4.15.5.1 Setting up a reclaim policy

Once the SCCM Uninstall is switched on you can create a reclaim policy and associate it with the appropriate ConfigMgr package or application.

Switch app to **AppClarity→Reclaim→Policies**.

Click on **New Policy**.

Configure your policy as required, completing the **Basic Information**, **Product**, **Version Expansion** sections

Set the **Uninstall Criteria** as **Mandatory Uninstall** - SCCM Workflow is driven on reclaim policies for mandatory uninstall. Any optional reclaim policy will not work with SCCM Uninstall, until it becomes a candidate for mandatory uninstall.

Select a value in the **SCCM uninstall Collection Type** section. This selection is important, as it allows SCCM to create suitable uninstall collections and drive the reclaim workflow accordingly.

Click **Publish.**

10.4.15.5.2 Adding the Association

Switch app to **AppClarity→Reclaim→Policies**

Select the reclaim policy in the Policies listing page and click **Manage Associations**.

This opens the **Inventory→Manage Associations→Product to CM** page, and opens with your policy selected.

Select the product you want to associate to the SCCM Uninstall workflow with this reclaim policy then click **Add Association**.

On the **Add Associations** page, type in the name or part of the name of your SCCM Package or application.

Enter CM application/package name inside the **Search for a CM Application or Package** text box, the selected package/application details will show in grid below).

Select product and choose your desired action for:

Install Programs and **Uninstall Programs** for packages (for example **Per System Unattended** for Install Program OR **Per System Uninstall** for Uninstall program).

Applications do not require any selection for Install/Uninstall programs.

Click **Save**.

> **Note**
>
> You will see either an **A** or **P** icon next to the name, that will show either Package or Application Model. For a package, you will need to select the correct programs.

10.4.15.5.3 Verifying Reports

When the setup is completed the following reports are automatically triggered, and can be see in **Settings→Monitoring→Process logs**:

Reclaim Consolidation - to convert this reclaim policy from a traditional reclaim based setup to an SCCM reclaim based setup

SCCM uninstall report, to perform the following actions:

Verifies if the root folder (under Device Collection/User Collection) already exists to host device/useruninstall collections. If not, then **create root folder** with name as **1E**

Create an **Uninstall collection** under **1E** folder

Add those **device/user** into the **Uninstall collection**, from which software needs to be removed (i.e. based on the reclaim policy set)

Remove these **device/user** from **Install collection**

If the device, user or both are members of collections that have deployments for an install of the software that needs reclaiming, AppClarity removes them from the installation collection.

SCCM Uninstall actions also act as status poller, to fetch the statuses of uninstall or if any new device needs to be added into the Uninstall collection.

10.4.15.5.4 Verifying Reclaim History

To view the status history for these reclaims:

Run the **Reclaim Reporting** action for associated Compliance repository from **Settings**→**Monitoring**→**Process logs** and click **Execute**.

Select Compliance Repository, and action as **Reclaim Reporting** and click **Execute**.

Wait till the **Reclaim Reporting** action successfully completes, then:

Switch app to **AppClarity**→**Reclaim**→**Reclaim History**.

All devices which were added to Uninstall Collection in SCCM, and are still waiting to be uninstalled display a **CollectionUpdated** status.

After a successful uninstall, these devices will display a status of **Uninstalled**.

10.4.16 Stopping a reclaim policy

SAM users (AppClarity Administrator, Reclaim Administrator) who have defined reclaim policies may want to stop those policies from being applied. There are many reasons why this may be required, but here are some reasons:

A published policy needs to be temporarily stopped.

A published policy needs revision.

The policy is no longer needed or the policy was created accidentally or was used as part of a test.

There's an emergency, policies are not working as expected and need to be stopped to prevent any further consequences.

10.4.16.1 Disabling a published policy

Temporarily suspending a reclaim policy leaves the policy unchanged in a published state but disabled. You can subsequently re-enable it whenever necessary without requiring any other change to the policy.

To do this:

Navigate to **AppClarity**→**Reclaim**→**Policies**.

Locate the policy you want to disable. In our example, this is a policy for a mandatory uninstall of unused **Microsoft Project**.

Click on the **Edit** link at the right-hand end of the policy's row in the table to display the **Reclaim Policy** page.

Under '**Basic Information**' section, uncheck the **Enabled** checkbox.

Click **Publish** to save the change.

Notice how the **Is Enabled** column now displays **FALSE**.

The **Reclaim Consolidation** report is refreshed automatically when **Publish** is clicked, so the reclaimer changes come into effect immediately.

The published policy will still be published but will not be enabled any longer, and hence no reclaim will happen against this policy.

10.4.16.2 Save a published reclaim policy as a draft

Like disabling a published policy, this also has the effect of temporarily stopping the policy. The downside is that it gets converted into draft reclaim policy, and will need to be published again to make it reclaimable. But if the policy needs any revision, this may be a good option.

To do this:

Navigate to **AppClarity→Reclaim→Policies**.

Locate the policy you want to disable. In our example this is a policy for a mandatory uninstall of **Adobe Acrobat Reader MUI**.

Click on the **Edit** link at the right-hand end of the policy's row in the table to display the **Reclaim Policy** page (alternatively, from Policies screen only, a policy can be moved to draft, by selecting the policy and click on **Move to Draft** button at right hand side)

Scroll down to the bottom of the page.

Click **Save draft**.

This has the effect of changing the status of the policy from the **Published** to **Draft**.

The **Reclaim Consolidation** report is refreshed automatically when **Save draft** is clicked so the reclaimer changes come into effect immediately.

The published policy will no longer be published but will be in the draft state, so that it can be re-published at a later time.

10.4.16.3 Deleting a published reclaim policy

When you are sure that a published reclaim policy is no longer needed, and will not be needed again in the future, you can delete the policy.

To do this:

Navigate to **AppClarity→Reclaim→Policies**.

Locate the policy you want to disable. In our example this is a policy for a mandatory uninstall of all versions of **Microsoft Office 365**.

Check the checkbox at the left-hand end of the policy's row in the table.

Click **Delete**.

In the confirmation popup, click **OK** to delete the selected policy permanently. If you have instead changed your mind you can click **Cancel**.

This has the effect of removing the policy from the **Policies** listing page and from AppClarity altogether.

The **Reclaim Consolidation** report is refreshed automatically when **Delete** is clicked so the reclaimer changes come into effect immediately.

The published policy will no longer be available in AppClarity.

10.4.16.4 Perform an emergency stop of all reclaim policies

If you are in an emergency state, and not sure which reclaim policy to target you can disable all the policies in one step.

To do this:

Navigate to **Settings**→**Configuration**→**Provider Configuration**.

Select the check-box for **Reclaimer** uninstall configuration type, and click **Edit**

Click on the toggle button, to **toggle Off** (to disable) the **Reclaimer** control to stop all devices from downloading their reclaim policies, and then **Save**.

This will stop any subsequent attempts to download the reclaim policy. This will not prevent any reclaim policies that have already been downloaded from running.

When the emergency has been resolved, you can click on the toggle to turn reclaim policy downloads back on.

10.4.17 Viewing the software reclaim reports

SAM users interested in software reclaim would like to view summary/history information of software reclaim (i.e. successful, failed, in progress, opt out) in order to:

Verify a software reclaim policy is working as expected

Check the progress of a reclaim policy

Audit the software reclaims

Evaluate how effectively AppClarity saves money on licenses.

To do this the user checks the Software Reclaim Summary page.

10.4.17.1 Viewing software reclaim summary

When AppClarity is installed it creates a schedule to run **Reclaim reporting** each night at 00:00. This report updates the contents of the **AppClarity→Reclaim→ Reclaim History** and **Savings** pages. Both of these reports can be filtered by Management Group (if you have set these up) from the dropdown list at the top of the page. You can run the report manually also, if you need more up to date information, as will be seen in the following steps.

To view the**Software Reclaim Summary**report:

Navigate to **AppClarity**→**Reclaim**→**Reclaim History**.

Refresh **Reclaim reporting** using the **Refresh Reports** icon on the top right of the page.

The table should now display the summary status for software reclaims that have been performed up to the current time.

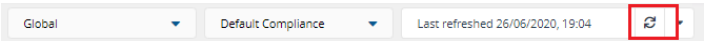
To filter on specific software, for example Microsoft Project, set a filter to get directly to the Microsoft Project installations.

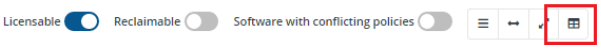
Click the

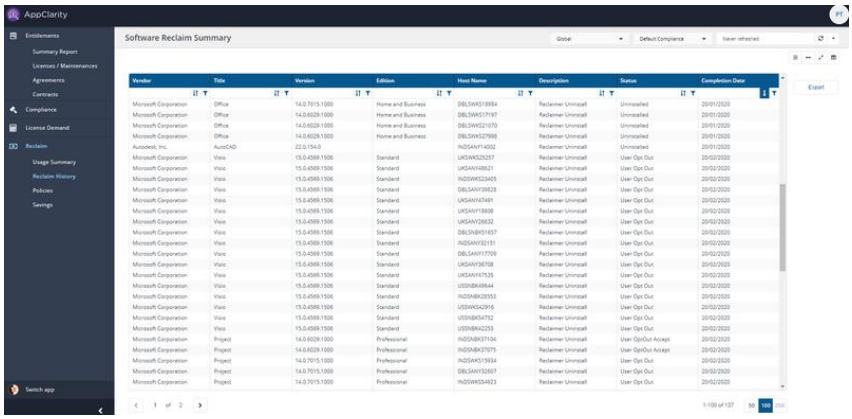
at the right-hand under the **Title** Column header.

Construct thefilter **Contains Project**.

Click **Apply** to set the filter.

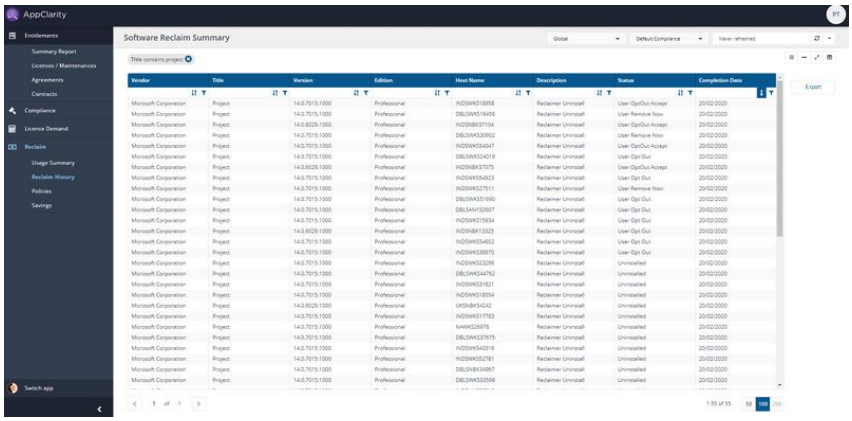
> **Note**
>
> You can refresh reports from individual AppClarity screens as well as using the **Settings** App. You can do this by using the refresh icon next to the**Last Refreshed**box, for example:
>
> 
>
>
> For a complete list of the specific reports you can run from particular pages refer to Running your first Compliance License Summary: Refresh Reports.

> **Note**
>
> You can choose which columns are displayed in Inventory and AppClarity detail tables to increase readability. On pages where you can pick the displayed columns you'll see a new control like the one highlighted below:
>
> 
>
>
> To find out more about this feature refer to Running your first Compliance License Summary: Choosing the columns to display in reports.



The rows in the filtered table indicate:

Status	Description
User OptOut Accept	A user requested to keep the software, they provided a suitable explanation and this was accepted by the AppClarity administrator for that policy so no software was reclaimed.
User Opt Out	A user requested to keep the software, they provided an explanation and this is pending acceptance by the AppClarity administrator for that policy.
User Remove Now	A user elected to remove the software now when prompted by the reclaimer running on their device.
Uninstalled	A user selected to remove the software, a mandatory uninstall policy was implemented and the software was successfully removed from their device.
FailedUninstallNoRetry	A user selected to remove the software, a mandatory uninstall policy was implemented and reclaimer attempts to uninstall software from device multiple times, and fails to uninstall. After a threshold of attempts, no further attempt to uninstall the software.
FailedUninstallRetry	A user selected to remove the software, a mandatory uninstall policy was implemented and reclaimer attempts to uninstall software from device. Reclaimer attempts will be made again to uninstall until a threshold is reached.
CollectionUpdated	When SCCM collection is updated (i.e. device is added to uninstall collection) through SCCM custom uninstall workflow.



10.4.17.2 Viewing the savings made by reclaiming software

To view the software reclaim savings report:

Navigate to **AppClarity**→**Reclaim**→**Savings** .

Having refreshed **Reclaim reporting** in the previous example, this page displays the reclaim savings that have been made by successful reclaims to date.

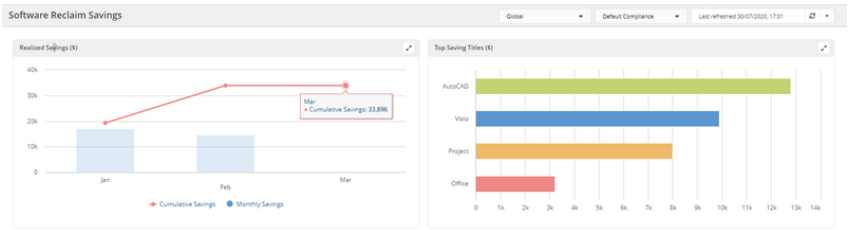
Here we can see in the **Realized Savings ($)** graph, it displays

Cumulative savings of successful reclaims so far, is **33,896**.

Monthly Savings due to successful reclaims each month (plots the data of last 12 months).

In the **Top Savings Titles ($)** you can click on each title and it's individual Cumulative Savings total will be displayed in **Realized Savings ($)**. **Top Savings Titles ($)** displays the top 5 saving titles.

> **Note**
>
> You can change the default displayed currency from USD to a currency of your choice, refer to Changing the default currency in AppClarity for details.



10.4.18 Scheduling AppClarity reports

When an entitlement repository or compliance repository is created, and e.g. reclaim consolidation is run for an compliance repository, then it creates a default reclaim consolidation schedule for this compliance repository, to run on daily basis. You can also create schedules for the repositories you create and schedule them to run at a frequency of your choice.

10.4.18.1 Scheduling a report refresh for a repository

Toautomaticallyrefresh a report for a repository you can set up a schedule:

Under the **Settings**→Configuration→Schedules and click **Add**.

In the Add schedule screen for:

Schedule name - enter a logical name for the new schedule.

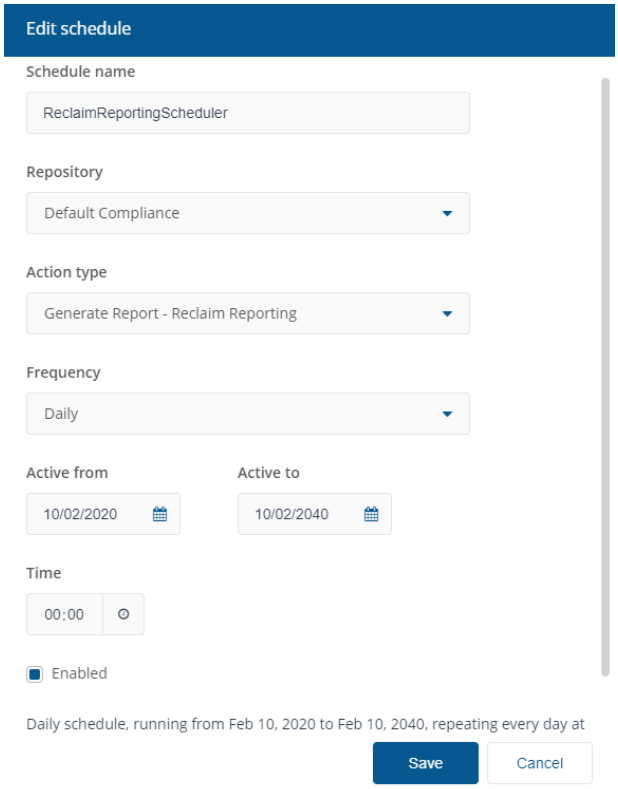
Repository - select your repository from the dropdown menu.

Action type - select the associated action type you want to schedule.

Frequency - select the frequency.

Note

For any entitlement repository, when a new entitlement is created (which triggers an entitlement consolidation) a **Schedule** called **EntitlementConsolidationScheduler** is created for this repository by default, it's set to run on a 24 hrs frequency (daily basis).



10.5 Troubleshooting

A general methodology for investigating issues with AppClarity, as well as identifying key issues and their resolutions.

For known issues relating to specific components, please refer to the respective troubleshooting pages:

Clients	Platform	Applications	Integration
1E Client	1E	Endpoint Automation	1E Core for ServiceNow
1E Client Deployment Assistant		Experience Analytics	1E ITSM Connect for ServiceNow
PXE Everywhere		Endpoint Troubleshooting	1E Service Catalog Connect for ServiceNow
		Writing 1E Instructions (1E SDK)	1E Virtual Assistant

10.5.1 1E Support contact details

10.5.1.1 Support Web portal

Maintenance support customers can log onto the 1E Support Web Portal at https://support.1e.com/ using the login details provided with their maintenance contract. This provides issue tracking, product hotfixes, and knowledge base articles related to each product.

10.5.1.2 Telephone support

Maintenance support customers can contact the technical support department at 1E through the following support numbers. Just phone the relevant number for your area, so your call can be routed quickly and efficiently to the correct support group:

US/Canada:	1-866-349-4032 (Toll-Free)
	1-917-339-2360 (Standard)
UK/Europe:	+44 (0)208 326 3499
India:	+91 120 402 4002
Australia:	+61 739 111 118

10.5.1.3 Email support

Maintenance customers can use the following email for additional support. Evaluation customers can also use this email with the temporary access code that is provided through customercare@1e.com as part of their evaluation.

support@1e.com

10.5.2 The technical support process

Read through the Troubleshooting pages to see if there are known issues, or quick resolutions to any problems you may have encountered.

Maintenance support customers can use the 1E Support Web Portal to review knowledge base articles and download hotfixes.

If still encountering problems, create a technical report (log files and details) and then contact the 1E technical support team.

10.5.2.1 Creating a technical report

If possible, please obtain the following details and log files before contacting 1E, to include in your technical report.

10.5.2.1.1 Version details

The OS, version number, and patch level for:

Tachyon Servers

1E Client

Configuration Manager - if used

Other 1E Server software, for example, Shopping, Nightwatchman, and WakeUp.

For Nomad and Shopping, please provide OS, version number, and patch level for:

Configuration Manager DPs

Nomad extensions used on Configuration Manager Consoles

ActiveEfficiency Server.

10.5.2.1.2 Environmental details

If there were any recent changes made to your configuration

The name of the machines, Configuration Manager Application and/or Package IDs for when the issue occurred

10.5.2.1.3 Problem details

When did the issue occur, ensure log files cover this period

The scope of the issue – did it affect a particular geographical location, group of users, or client machines

Details of any self-help troubleshooting steps you carried out

In the event of a service crash or if you are experiencing high CPU or memory usage, provide us with the dump file, event viewer logs, and traces. We will provide you with FTP details to upload these files.

10.5.2.2 Log files

Tachyon Server log files

For any issue, please provide a zip containing log files from the following locations:

%ALLUSERSPROFILE%\1E\Catalog*.log

%ALLUSERSPROFILE%\1E\ContentDistribution*.log

%ALLUSERSPROFILE%\1E\Platform Consumers*.log

%ALLUSERSPROFILE%\1E\SLA Platform*.log

%ALLUSERSPROFILE%\1E\Tachyon*.log

If you are having licensing issues, please include:

%ALLUSERSPROFILE%\1E\Licensing*

Please refer to the Tachyon Platform 8.1 - Log files page for more details.

1E Client logs on Windows

%ALLUSERSPROFILE%\1E\Client\1E.Client.log (used by 1E Client and Tachyon features, and Shopping client)

%ALLUSERSPROFILE%\1E\Client\NomadBranchUninstall-YYYY_MM_HHTMM_HH_SS_000Z.log

Nomad client log

%ALLUSERSPROFILE%\1E\NomadBranch\LogFiles\NomadBranch.log

WakeUp client log

%ALLUSERSPROFILE%\1E\Agent\WakeUpAgt.log

Shopping WSA client log

%ALLUSERSPROFILE%\1E\Client\WSA.log

10.5.2.2.1 Software Reclaimer log files

Every time the Reclaimer runs it will create a local log file of the process it is doing. The location and name of the log file depends on what task the reclaimer is doing.

Task	Logpath	Notes
Optout	**C:\Users\{USER}\AppData\Local\Temp\ AppClarity.SoftwareReclaimer.log**	Optout mode is normally run under user context so that the user can interact with the dialog. This

Task	Logpath	Notes
		means the log file will be in the users Temp folder within the user profile.
Mandatory	**C:\windows\Temp\AppClarity.SoftwareReclaimer.log**	Mandatory mode is normally set to run under system context, in order to process reclaim uninstall commands. Therefore, the log file will be under the system temp directory.
Reclaim	**C:\windows\Temp\AppClarity.SoftwareReclaimer.MSI.log**	For a mandatory reclaim, if a reclaim occurs using an MSI then an MSI log

Task	Logpath	Notes
		file is also created.

10.5.3 Known Issues

Lists of the current known issues with implementing, configuring, using, and extending Nomad.

If you cannot find an issue and its workaround on this page, please try searching the 1E Support Portal https://support.1e.com/ for issues that have hotfixes.

If you need further help, please refer to the Troubleshooting page for how to contact 1E Support and the technical support process.

Issue	Description	Workaround
Compliance Report fails, when there are many entitlements are available for the same vendor and title, with quantity as 1.	For any vendor, hundreds of entitlements are available in the system with qty=1 (For example, 500+ entitlements are available for Microsoft Corporation - Word with entitlement quantity =1) and also a large number of installations (For example, 50 K+ installations) exist for same vendor and title.	You can consolidate multiple entitlements into a single logical entitlement (For example, multiple entries for same vendor, title, version, metric type can be converted into a single entitlement).
While creating a new license/ maintenance based entitlement, a page has a tabbing problem if form data is entered using keyboard control only (and no mouse h/w is used).	The following are tab related problems, while adding a new form using manual input (mouse h/w is not used and only keyboard is being used). Tabs skipping drop-down fields such as Version Type, Metric, License Type etc Users can't select list and date using arrow keys & space bar When a user reaches on date control using tab, the date picker opens but does not get closed on moving to next control, so, It remains open on page	n\a

	Users cannot publish / save draft / cancel entitlements as the tab does not move on these buttons.	
When uploading entitlements using the entitlement.tsv connector, and the entitlement contains a wild card (that is, *) as Version, then it will not be automatically set as * in entitlement on UI.	While uploading an entitlement through .tsv files using the entitlement connector, if a user sets the version as * for any vendor and title, then it does not get assigned as * on the entitlement screen (that is, on license screen) after a successful upload.	n\a
Upgrading from AppClarity 6.1.100 to AppClarity 7.1 entitlements with caveats (in 6.1.100) do not display with a caveats warning icon and simply display as draft (with draft icon).	When AppClarity 6.1.100 is upgraded to AppClarity 7.1 and some entitlements in 6.1.100 had caveats. After the upgrade, these caveat entitlements do not display with a caveats warning icon, instead, they display as draft (with draft icon).	n\a
Reclaim Consolidation occasionally fails due to deadlock if any Vendor and Title has large number of policies (~ 18-20), and precedence is set.	Reclaim → Usage Summary → Precedence Any Vendor and Title which has a large number of overlapping policies (which need to be set for precedence) when a user opens the set precedence screen, on clicking the 'move up' arrow button for the last policy and this is done in quick succession for 3-4 times (for different policies), two errors are can be seen: System triggers the Reclaim Consolidation for each 'up' arrow click Out of those many reclaim consolidation actions, one fails with a deadlock error.	If multiple policies are available for precedence, and last policy is needed to be set for highest precedence, then use 'move to top' button, and it moves this policy on top.

For any uploaded License / Maintenance, which has several warnings, AppClarity only displays the remediation part to the user (instead of both warning and remediation) on the license / maintenance screen drawer.	Entitlements→License / Maintenance screen If any entitlement has warnings when uploaded using the entitlement connector, then only the remediation is displayed for that entitlement, instead of both warnings and remediation on entitlement drawers.	n\a
License Demand displaying as 1 for management group name 'License Exemption - Oracle Corporation'.	On the IBM Processor Value Unit (PVU) License Demand and Oracle Processor License Demand screens, License Demand displays as 1 for exempted management groups. This happens in the case of a Virtual Host Cluster Soft Partition, where optimized license demand is calculated based on physical devices, but the installations are on virtual machines. In other situations, it works correctly.	n\a
License exempted comment does not appear for Oracle Processor License Demand.	In Oracle license demand, exempted comments do not appear when the device is exempt.	n\a
Installations on non exempted devices are also marked for exemption under the Global Management group.	In case of IBM PVU and Oracle Processor License Demand, the installations on non exempted devices are also marked for exemption under the Global Management group.	n\a
Entitlement tsv uploaded using the entitlement .tsv connector fails if the tsv file only has a row with a newline/carriage return.	When uploading an entitlement.tsv file using the entitlement upload connector, if there are any blank lines inbetween the entitlements, then the entitlement connector fails.	Before you upload the .tsv file, make sure the data is sanitized.

Multiple issues when navigating to and from screens with favorite and non favorite repositories.	AppClarity [Compliance] : Adding a license from Compliance->License Summary opens license form in the default repository even though compliance is associated to non-default Entitlement repository. AppClarity [Manage Associations] : VTVE is selected (from Compliance-2, which is not favorite), and the Manage Association button is clicked, then AppClarity navigates the user to (INV-1, which is a favorite).	After switching between screens from different modules/consumers, make sure you have selected the intended repository.
On Compliance→License Summary installs by details screen, if a user keeps this screen open for long time, an error occurred while loading table data on details table.	On Compliance→License Summary installs by details screen, if a user keeps this screen open for a long time, an error occurred while loading table data on details table.	Refresh the page to view the data.
No reclaim policy displayed on Reclaim→Policies screen, as the policy is created for *. User navigated to policy using reclaim usage version 14.0.0.5548.	Reclaim→Usage Summary If a reclaim policy is created on wild card (for example, 1E - Tachyon - and version as *), then on the Reclaim→Usage Summary screen, for 1E Tachyon 1.0.0.0, Count of 'selected management group policies' displays as 1 (as hyperlink). On clicking this hyperlink, AppClarity navigates to Reclaim→Policies screen to display the total number of policies. Blank data is displayed on the Policies screen (due to incorrect version/edition filter).	n\a

	It works correctly, if a reclaim policy is created with the exact version.	
Error appears on creating a license for specific title (that is, Office 365 ProPlus) and few other version specific generic issues.	The following are issues when publishing a license for a specific title and edition (Office 365 ProPlus) and also with version values: Error comes up, when a user tries to create/publish a license for Office 365 (with edition as ProPlus) and (Version as Dot Version with value as 16.*) When creating a license for 'Office 365' with Edition as 'ProPlus' and Version as 'All versions', then after it's published, it's edition is changed to ***E3*** instead of ProPlus When a license is created as Version using 'Colloquial version', after publishing the license, the version is set as 'dot format' instead of 'Colloquial version'.	n\a
RBAC issues with different AppClarity user roles.	Multiple RBAC related issues for different AppClarity user roles: Reclaim Viewer user - can can also see the AppMigration consumer screen Reclaim v iewer role - when opening the report refresh dropdown, a user is able to see the Full report list link and when they click it, the page breaks with the message ‘Something went wrong’ Compliance viewer user role - on the compliance detailed installation screen or LDC detailed report screen, when a user clicks	n\a

	on device hyperlinks, the 'Something went wrong' message appears and the page breaks Entitlement administrator role - provider log displaying the reclaim PO's is visible to a user with the entitlement administrator role Entitlement administrator role - user is able to see inventory application and perform Configuration Manager manage associations activities.	
Intermittent issues on Reclaim Policies→Policy Administration screen.	Policy Administration (links like User Rejected, succeeded etc) when they have more than 500 or 1000 records, then pagination links do not appear until the user scrolls till the last record. If any reclaim policy has large number of pending admin action records (that is, 1197) available (on which reclaim admin need to take action), then when they drill down to the Policy Administration screen by clicking the counts hyperlink, a blank screen displays with no data showing in tabular structure.	The user needs to scroll till the last record (that is, up till bottom of page) to see the pagination buttons. Remove the sorting from 'Completed On' column, then data starts appearing.
Contracts which are exported, cannot be re-imported.	Contracts which are exported, cannot be reimported and AppClarity shows an error for "Start date" due to a space character.	n\a
Export not working for filtered data on aggregated columns such as 'Lic Qty', 'Mnt Qty' and' Total cost'	Entitlement→Summary Report If there are 4-5 entitlements (of the same vendor and title), and the user applies a filter on column 'License Qty' then when using the	n\a

columns of Entitlement Summary screen.	Export button, Filter and Export do not work on aggregated columns.	
Perpetual entitlements with future dates come with the 'Active only' filter.	If 'Active Only' filter is applied on entitlement listing page then Perpetual entitlements with future dates also come with this filter applied. It works for Subscription entitlements where future dates are filtered out.	n/a
Column picker choices goes back to default after refresh	When you refresh reports on a page where you have changed the displayed columns, the view will reset back to its view once the refresh completes and the page reloads.	n\a

10.6Reference

All the AppClarity-related tables of information, such as supported platforms, communications ports etc.

10.6.1 Supported Platforms

A list of all the platforms supported by AppClarity and the software required to allow AppClarity to be installed and work correctly.

> **Note**
>
> The list of Supported Platforms for AppClarity is identical to Tachyon Platform 8.1 because AppClarity is a Tachyon consumer application.

> **Note**
>
> 1E will provide you with a **Tachyon.lic** license file that defines the products and features your Tachyon System is able to use, for how long, and how many devices it supports, this may be an evaluation or subscription license.

The license must be activated. Once activated, it may be used only by the Tachyon System that activated it.

Licenses can be renewed or updated, but if allowed to expire, then the affected products or features will not be usable.

For a new installation, the Tachyon Setup program will let you select the license file from any folder on disk.

For an existing installation, the license file is copied into the folder: %PROGRAMDATA%\1E\Licensing on your Tachyon Server.

> For details of what the license file needs to contain, please refer to Design Considerations: License requirements for consumer applications.

The list of Supported Platforms for AppClarity is identical to Tachyon Platform because AppClarity is a Tachyon consumer application.

Please refer to Windows Server requirements for details.

10.6.1.1 1E Companion Products

Supported versions of 1E companion products that AppClarity 8.1 features depend on.

Products and features that AppClarity depends on	Supported versions of companion products	
1E Catalog	Required by all AppClarity features.	1E Catalog (included in Tachyon Platform 8.1)
Tachyon	Tachyon powered inventory using the optional Tachyon connector and full Tachyon infrastructure.	Tachyon Platform 8.1
AppClarity 5.2	Optional feature of AppClarity 8.1 to use its AppClarity 5.2 connector to migrate entitlements from AppClarity 5.2. Only requires the AppClarity 5.2 database, not the full AppClarity 5.2 infrastructure.	AppClarity 5.2.0

Supported versions of 1E companion products with features that depend on AppClarity 8.1.

Products and features that depend on AppClarity	Supported versions of companion products
None	

10.6.1.2 Connectors

The following table shows the supported versions of software used by the Tachyon out-of-box connectors.

The following table shows the supported versions of software used by the Tachyon out-of-box connectors.

Connector	Product	Notes
BigFix	BigFix	Please refer to the BigFix connector for prerequisites.
Intune	Intune	Please refer to the Intune connector page for prerequisites.
Microsoft Office 365	Azure	Please refer to the Microsoft Office 365 connector page for prerequisites.
OpenLM	OpenLM Server version 21.12	Please refer to the OpenLM connector page for prerequisites.
Oracle LMS	Oracle LMS	Please refer to the Oracle LMS connector page for prerequisites.
ServiceNow	ServiceNow Jakarta release	Please refer to the ServiceNow connector page for prerequisites.
System Center Configuration Manager (SCCM)	SCCM CB 2203 SCCM CB 2111 SCCM CB 2107 SCCM CB 2103 SCCM CB 2010	Please refer to the System Center Configuration Manager connector page for prerequisites.

Connector	Product	Notes
Tachyon	Tachyon 8.1	Please refer to the Tachyon connector page for prerequisites.
vCenter	VMware PowerCLI 11.1.0	VMware PowerCLI 11.1.0 (code.vmware.com/web/dp/tool/vmware-powercli/11.1.0) must be installed on the Tachyon Master server (where the SLA Integrate Services Agent service is hosted) before you can configure and use the vCenter connector. Earlier or later versions of PowerCLI are not supported and may cause errors. VMware PowerCLI is freeware and was previously known as vSphere PowerCLI. VMware PowerCLI supports multiple versions of VMware vCenter Server. For details, please refer to the VMware compatibility matrix using the following link: https://www.vmware.com/resources/compatibility/sim/interop_matrix.php#interop&2=&106= Please refer to the vCenter connector page for configuration details.
WSUS (Windows Server Update Services)	WSUS	Please refer to the Windows Server Update Services connector page for configuration details.

10.6.2 1E Companion Products

A list of the feature dependencies between AppClarity and other 1E companion products.

To view the general platform related dependencies for AppClarity please refer to Supported Platforms.

10.6.2.1 1E companion products that AppClarity 8.1 depends on

Supported versions of 1E companion products that AppClarity 8.1 features depend on.

Products and features that AppClarity depends on	Supported versions of companion products	
1E Catalog	Required by all AppClarity features.	1E Catalog (included in

Products and features that AppClarity depends on	Supported versions of companion products	
		Tachyon Platform 8.1)
Tachyon	Tachyon powered inventory using the optional Tachyon connector and full Tachyon infrastructure.	Tachyon Platform 8.1
AppClarity 5.2	Optional feature of AppClarity 8.1 to use its AppClarity 5.2 connector to migrate entitlements from AppClarity 5.2. Only requires the AppClarity 5.2 database, not the full AppClarity 5.2 infrastructure.	AppClarity 5.2.0

10.6.2.2 1E companion products that depend on AppClarity 8.1

Supported versions of 1E companion products with features that depend on AppClarity 8.1.

Products and features that depend on AppClarity	Supported versions of companion products
None	

10.6.3 Communication Ports

Diagrams and links to tables for all the external communication ports used by Tachyon and locally installed consumer applications. Useful, if needed, for configuring network and device firewalls.

Please refer to Tachyon Architecture for architecture diagrams.

10.6.3.1 Connections diagram

Please refer to Communications ports for the Tachyon Platform connections diagram.

10.6.3.2 Firewall requirements

Please refer to Firewall requirements for a Single-Server for details.

10.6.4 Installer properties

Please refer to AppClarity installer properties for details.

10.6.5 AppClarity page reference

A reference for the fields and tables on the pages in the AppClarity application.

10.6.5.1 Entitlements

A reference for the fields and tables on the pages under the **Entitlements** node in the **AppClarity** application.

10.6.5.1.1 Summary Report page

A description of the fields on the **Summary Report** page.

Here you can view the entitlements for a selected entitlements repository. You get to this page by clicking the **AppClarity→Entitlements→Summary Report** node in the navigation panel.

The fields on the **Summary Report** page are:

Entitlements repository selector

Entitlements Records

Costs Breakdown

Active Entitlements only toggle

Action Buttons

Export

Entitlements table

Vendor

Title

Edition

Metric

Lic Qty

Mnt Qty

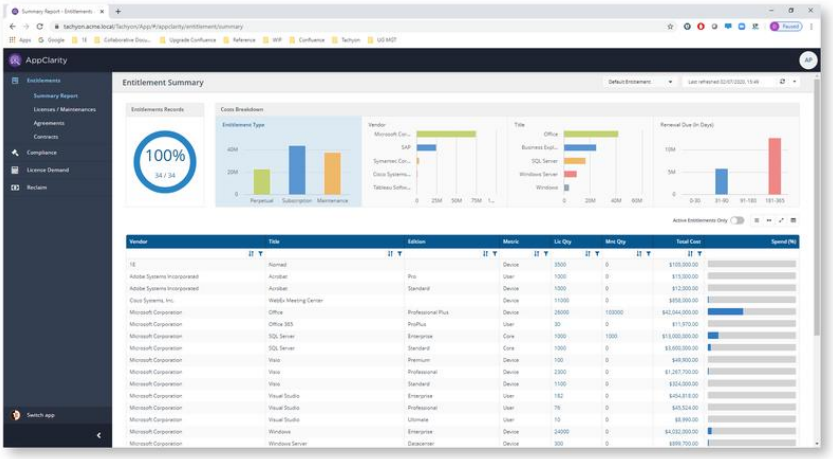
Total Cost

Spend (%)

Column actions

Column sort

Column filter



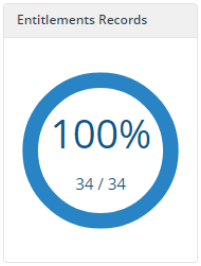
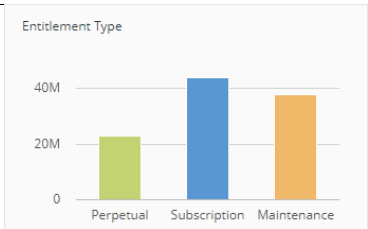
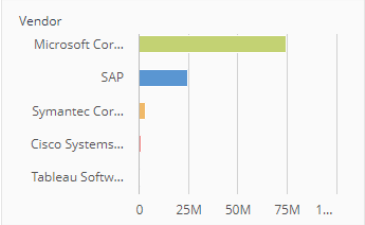
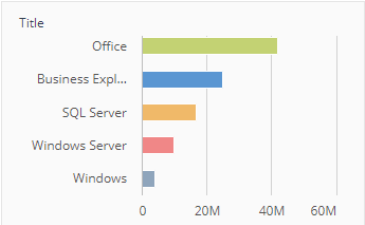
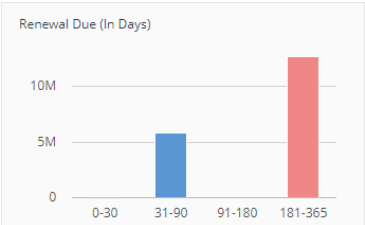
Field	Description
Entitlements repository selector	This field lets you select the repository where the entitlements data displayed on the page comes from. By default this is set to **Default Entitlements**. If you have created your own entitlements repositories, click on the name to select any of these from the drop-down list.
Entitlements Records	This chart shows the percentage of the total number of Entitlements Records in the selected Entitlements repository that are currently being displayed on this page as a result of the applied filters. The figures below the chart show the number of Entitlements Records being displayed over the total number of Entitlements Records in the selected Entitlements repository. 
Costs Breakdown	These charts show the costs breakdown for various aspects of the Entitlements in the currently selected Entitlements repository.

Chart	Description
Entitlement Type	This chart shows the breakdown and numbers for the Entitlements Records in the selected Entitlements repository according to their Entitlement type: Perpetual, Subscription or Maintenance.

Field	Description
	
Vendor	This chart shows the breakdown and numbers for the top 5 Vendors according to their total Entitlements costs in the selected Entitlements repository. 
Title	This chart shows the breakdown and numbers for the top 5 software Titles according to their total Entitlements costs in the selected Entitlements repository. 
Renewal Due (In Days)	This chart shows the number of entitlement renewals that are due within certain numbers of days in the selected Entitlements repository. 
Active Entitlements only toggle	The **Active Entitlements only** toggle adds a filter when it's turned on that filters the table to only display the entitlements that have been published and not the ones that are in draft.

Field	Description
Action Buttons	The following table describes the action buttons displayed on the**Summary Report**page.

Button	Description
Export	Exports all the entitlements currently displayed in the **Entitlements** table as a TSV file. This button takes the filters currently applied to the table into account, but not the sorting or the current selection.

Entitlements table

The following table describes the columns displayed in the **Entitlements** table:

Column	Description
Vendor	The vendor portion of the vendor, title, version and edition attributes that are used to identify which software products the entitlement or agreement is for. For example, **Microsoft Corporation** or **1E**. You can sort and filter on this column.
Title	The title portion of the vendor, title, version and edition attributes that are used to identify which software products the entitlement is for. For example, **Visio** or **Nomad**. You cansortandfilteron this column.
Edition	The edition portion of the vendor, title, version and edition attributes that are used to identify which software products the entitlement is for. For example, **Standard** or **-** (where no edition is specified or exists). You cansortandfilteron this column.
Metric	The metric type for a license or maintenance entitlement. This may be one of:

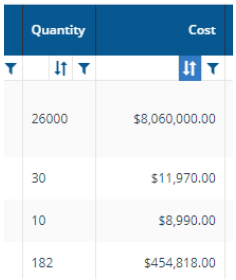
Type	Description
Core	The metric for the license is related to the number of cores present on a device. For example, licenses for **Microsoft SQL database** are related to the

Field	Description		
			number of cores on the server where **Microsoft SQL** is installed.
		Device	The metric for the license is for devices. For example licenses for **Microsoft Visio** are on a per device basis. This is the default type.
		Other	This can be used to reference your own license metric type.
		Processor	The metric for the license is related to the number of processors for a device. For example, licenses for certain **Oracle** products are related to the number of processors on the server where the **Oracle** product is installed.
		PVU	The metric for the license is related to the Processor Value Unit present on a device. For example. licenses for **IBM** products are related to the **Processor Value Unit (PVU)** for the device where the IBM product is installed.
		User	The metric for the license is related to the users for the product. For example, **Microsoft Office 365** licenses are related to users and not the devices the software is running on.
		You cansortandfilteron this column.	
	Lic Qty	The **Lic Qty** column shows the number of licenses related to each Entitlement in the table. You can sort and filter on this column.	
	Mnt Qty	The **Mnt Qty** column shows the number of maintenance licenses related to each Entitlement int the table. You can sort and filter on this column.	

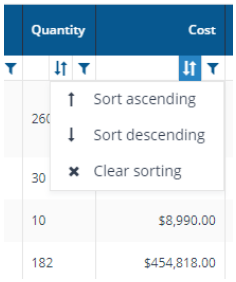
Field	Description
Total Cost	The **Total Cost** column displays the total cost for the number of licenses and maintenances covered by each entitlement in the table. You can sort and filter on this column.
Spend (%)	The **Spend (%)** column shows the percentage of the overall spend for each Entitlement in the selected Entitlement repository. The complete bar represents the overall spend, the blue bar indicates the % spend for this Entitlement and the grey bar shows the % remainder.

Column actions

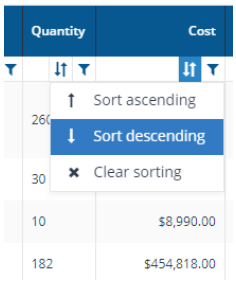
The following column actions are available on some columns in the table.

Column action	Description
Column sort	**Using column sorts** The picture opposite shows an example taken from AppClarity. In our example we want to sort the table on the **Cost** column from the highest cost at the top to the lowest at the bottom.To sort the table on the **Cost** column: Click on the sort icon ⇅ just beneath the header row in the **Cost** column.  The sort popup is displayed.

Field	Description

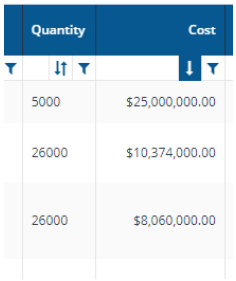


Now select the sort direction. In our example this will be **Sort descending**.



After selecting this the data in the table is now sorted on the **Cost** column from highest to lowest and the sort icon has changed to a sort descending icon

.



Clearing the sort

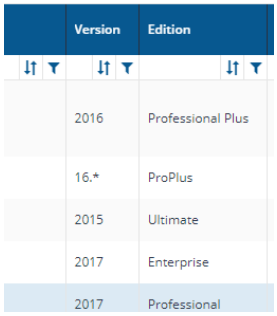
You can clear the sort by clicking on the sort icon again and selecting the **Clear sorting** menu item from the sorting popup.

Column filter

Using column filters

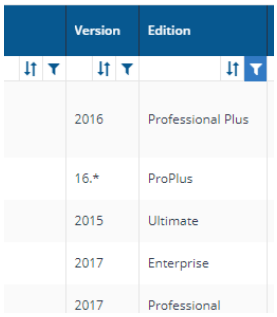
The picture shows an example taken from AppClarity. In our example we want to filter the table to show only those items where the **Edition** contains the text **Prof**.

Field	Description

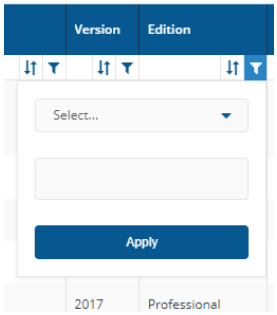


To filter the table on the **Edition** column:

Click on the filter icon just beneath the header row in the **Edition** column.

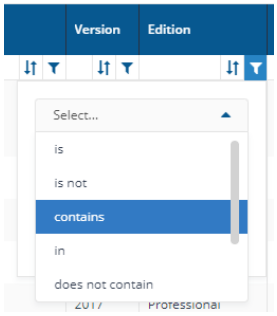


The filter popup is displayed.

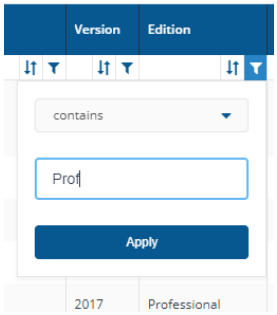


Now select the operator. In our example this will be **contains**.

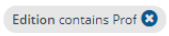
Field	Description



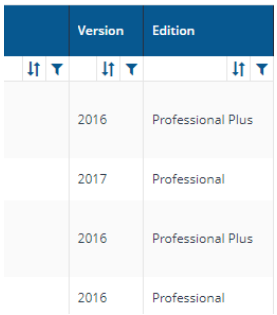
Then type the text **Prof** into the text field.



Click **Apply** and a new filter will be added to the table.



The table will be filtered to just those items whose **Edition** contains the text **Prof**.



Adding another filter

You can add another filter by clicking on the filter icon for any of the columns. The picture opposite shows another filter added selecting table rows where the **Type** also contains the text **License**. The table will also be filtered accordingly.

Field	Description
	Removing filters You can remove filters by clicking on the filter close icon at the end of the filter.

10.6.5.1.2 Licenses / Maintenances page

A description of the fields on the **Licenses / Maintenances** page.

Here you can view, edit, copy, create, publish and delete License and Maintenance entitlements. You can also view any components related to a License or Maintenance and export all the entitlements in the selected repository to a TSV file. You get to this page by clicking the **AppClarity→Entitlements→Licenses / Maintenances** node in the navigation panel.

The fields on the **Licenses / Maintenances** page are:

Entitlement Repository selector

Report Refresh

Active Entitlements only toggle

Status filters

Action Buttons

New License

New Maintenance

Edit

Publish

Clone

Move to Draft

Delete

Components

Export

Column Picker

Licenses / Maintenances table

Vendor

Title

Version

Edition

Type

Metric

Product SKU

Quantity

Cost

End Date

Management Group

Identifier

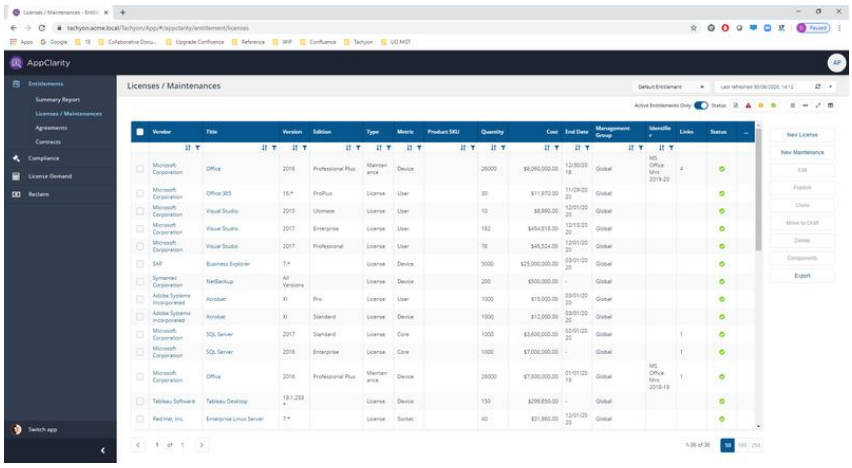
Links

Status

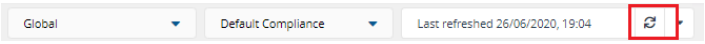
...

Column sort

Column filter



Field	Description
Entitlement Repository selector	This field lets you select the repository where the entitlements data displayed on the page comes from. By default this is set to **Default Entitlements**. If you have created your own entitlements repositories, click on the name to select any of these from the drop-down list.

Field	Description
Report Refresh	You can refresh reports from individual AppClarity screens as well as using the Settings App. Where this is available you can do this by using the refresh icon next to the **Last Refreshed** box: 
Active Entitlements only toggle	The **Active Entitlements only** toggle adds a filter when it's turned on that filters the table to only display the entitlements that have been published and not the ones that are in draft.
Status filters	The Status filters are displayed in the top-right of the page and let you filter the table according to the status of the items in the table. Clicking on an icon filters the table to display only items with that status, as described in the following table.

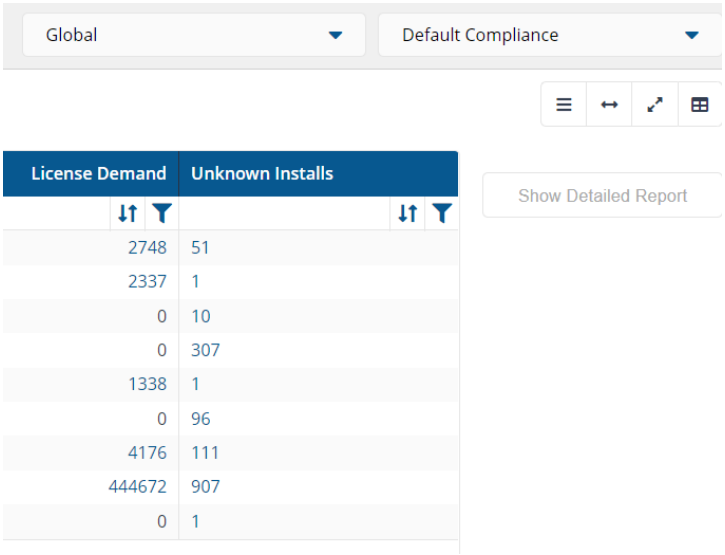
Icon	Description
	Filters to show only items in Draft.
	Filters to show only items in Draft with errors.
	Filters to show only items in Draft with warnings.
	Filters to show only items that are Published.

Action Buttons	The following table describes the action buttons displayed on the **Licenses / Maintenances** page.

Button	Description
New License	Creates a New License. Please refer to New License page for more details.
New Maintenance	Creates a New Maintenance. Please refer to New Maintenance page for more details.
Edit	This button is only enabled when there is a single selection in the **Licenses / Maintenances** table.

Field	Description
	Edits the selected entitlement and opens the Edit License or Edit Maintenance page, depending on the type of the selected entitlement. Please refer to New License or New Maintenance pages for more details.
Publish	This button is enabled when there is at least one selection in the **Licenses / Maintenances** table. Publishes the selected entitlements.
Clone	This button is only enabled when there is a single selection in the **Licenses / Maintenances** table. Clones the selected entitlement and opens the Edit License or Edit Maintenance page, depending on the type of the selected entitlement, with a clone of the details from the entitlement. Please refer to New License or New Maintenance pages for more details.
Move to Draft	This button is enabled when there is at least one selection in the **Licenses / Maintenances** table. Moves the selected entitlements to Draft.
Delete	This button is enabled when there is at least one selection in the **Licenses / Maintenances** table. Deletes the selected entitlements.
Components	This button is only enabled when there is a single selection in the **Licenses / Maintenances** table. Displays the components for the selected entitlement. If the entitlement has no components the message displayed is **Data not available**. Components refer to the bundled software related to a license. For example you may have a bundle for **Microsoft BackOffice Small Business Server**, which would contain components for **Exchange Server**, **FrontPage**, **Internet Explorer** and **Outlook**.

Field	Description
	Export Exports all the entitlements currently displayed in the **Licenses / Maintenances** table as a TSV file. This button takes the filters currently applied to the table into account, but not the sorting or the current selection.
Column Picker	Where the column picker control is shown you can choose which columns are displayed. In the following example on the **Microsoft Core License Demand** page we hide the **Unknown Installs** column and move the **License Demand** column to the left of the page.

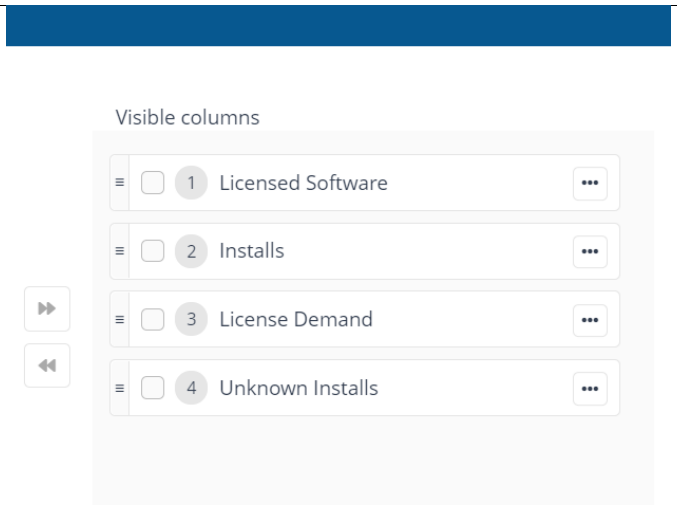


License Demand	Unknown Installs
2748	51
2337	1
0	10
0	307
1338	1
0	96
4176	111
444672	907
0	1

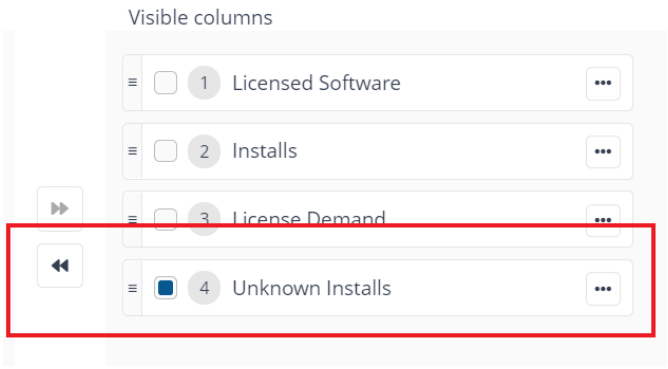
To pick the displayed columns:

Click on the Choose columns icon to the right of the header row to view the visible columns.

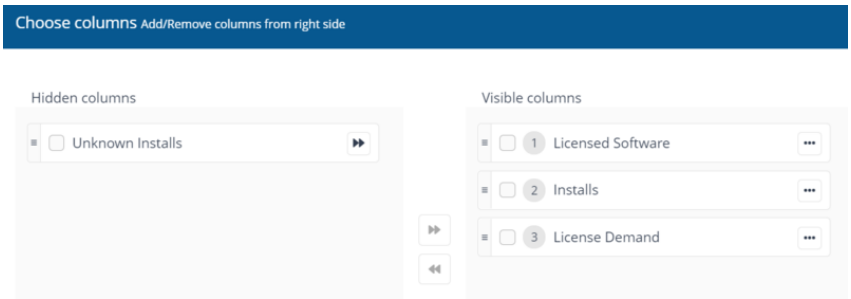
Field	Description



To exclude **Unknown Installs**, select the Unknown Installs row and click **Exclude columns** button.

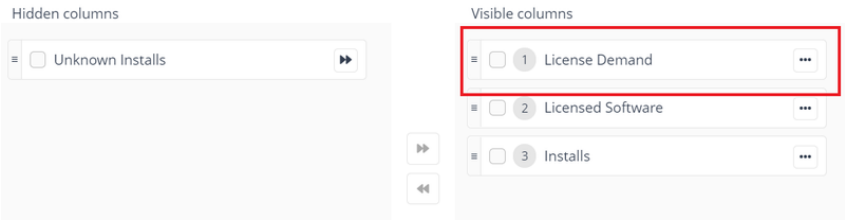


The **Unknown Installs** column is now hidden.



To move the **License Demand** column to the top of the list, hover your mouse over **License Demand** and using the direction control drag it to the top of the list.

Field	Description



The Microsoft Core License Demand page has now been automatically updated with our changes.

License Demand	Licensed Software	Installs
2748	Windows Server DataCenter	647
2337	SQL Server Enterprise	649
0	SQL Server Analysis Services	0
0	SQL Server Integration Services	0
1338	SQL Server Standard	300
0	SQL Server Reporting Services	0
4176	Windows Server Enterprise	265
444672	Windows Server Standard	4019
0	SQL Server Data Quality Services	0

Licenses / Maintenances table

The following table describes the columns displayed in the **Licenses / Maintenances** table:

Column	Description
Vendor	The vendor portion of the vendor, title, version and edition attributes that are used to identify which software products the entitlement or agreement is for. For example, **Microsoft Corporation** or **1E**. You can sort and filter on this column.
Title	The title portion of the vendor, title, version and edition attributes that are used to identify which software products the entitlement is for. For example, **Visio** or **Nomad**. You can sort and filter on this column.
Version	The version portion of the vendor, title, version and edition attributes that are used to identify software products. For example, **11.0.3216.5614** or **6.3.100.0**. You can sort and filter on this column.

Field	Description
Edition	The edition portion of the vendor, title, version and edition attributes that are used to identify which software products the entitlement is for. For example, **Standard** or **-** (where no edition is specified or exists). You can sort and filter on this column.
Type	The **Type** column displays the type of the entitlement in the table. This can be either **License** or **Maintenance**. You can sort and filter on this column.
Metric	The metric type for a license or maintenance entitlement. This may be one of:

Type	Description
Core	The metric for the license is related to the number of cores present on a device. For example, licenses for **Microsoft SQL database** are related to the number of cores on the server where **Microsoft SQL** is installed.
Device	The metric for the license is for devices. For example licenses for **Microsoft Visio** are on a per device basis. This is the default type.
Other	This can be used to reference your own license metric type.
Processor	The metric for the license is related to the number of processors for a device. For example, licenses for certain **Oracle** products are related to the number of processors on the server where the **Oracle** product is installed.
PVU	The metric for the license is related to the Processor Value Unit present on a device. For example. licenses for **IBM** products are

Field	Description	
		related to the **Processor Value Unit (PVU)** for the device where the IBM product is installed.
	User	The metric for the license is related to the users for the product. For example, **Microsoft Office 365** licenses are related to users and not the devices the software is running on.
		You can sort and filter on this column.
Product SKU		A SKU (pronounced 'skue') is an identification, usually alphanumeric, of a particular product that allows it to be tracked for inventory purposes. In AppClarity, via the 1E Catalog, a SKU is associated with the license metrics and use rights associated with a particular software product purchase. You can sort and filter on this column.
Quantity		The **Quantity** column displays the number of licenses covered by the entitlement. You can sort and filter on this column.
Cost		The **Cost** column displays the cost for each entitlement in the table. You can sort and filter on this column.
End Date		The **End Date** column shows the date the entitlement will end. You can sort and filter on this column.
Management Group		Displays all of the management groups the software reclaim policy is associated with. You can sort and filter on this column.
Identifier		Displays the **Identifier** information configured for the entitlement or agreement.

Field	Description
	You can sort and filter on this column.
Links	Displays the **Identifier** information configured for the entitlement or agreement.
Status	The icon indicates the status of the entitlement or agreement:

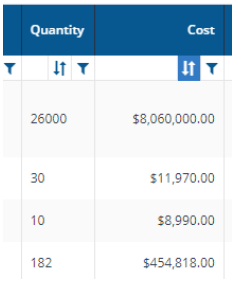
Icon	Description
	Draft.
	Draft with errors.
	Draft with warnings.
	Published.

...

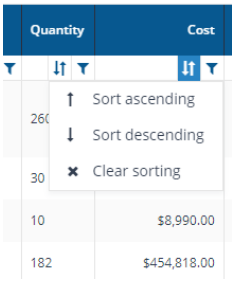
The following column actions are available on some table columns.

Column actions	Description
Column sort	**Using column sorts** The picture opposite shows an example taken from AppClarity. In our example we want to sort the table on the **Cost** column from the highest cost at the top to the lowest at the bottom.To sort the table on the **Cost** column: Click on the sort icon ⇅ just beneath the header row in the **Cost** column.

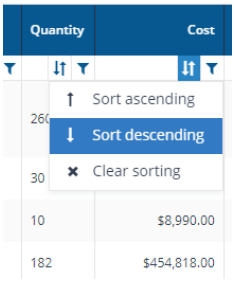
Field	Description



The sort popup is displayed.

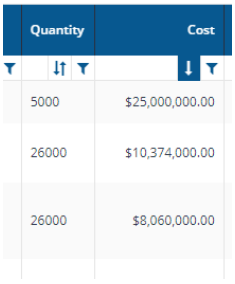


Now select the sort direction. In our example this will be **Sort descending**.



After selecting this the data in the table is now sorted on the **Cost** column from highest to lowest and the sort icon has changed to a sort descending icon

.



Field	Description

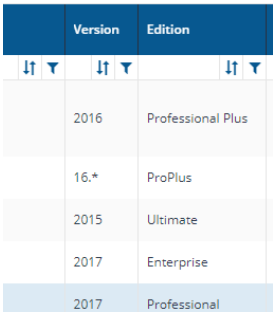
Clearing the sort

You can clear the sort by clicking on the sort icon again and selecting the **Clear sorting** menu item from the sorting popup.

Column filter

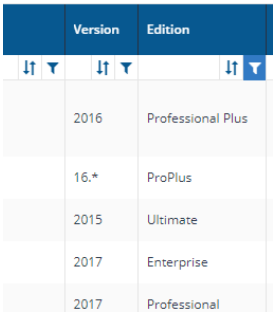
Using column filters

The picture opposite shows an example taken from AppClarity. In our example we want to filter the table to show only those items where the **Edition** contains the text **Prof**.

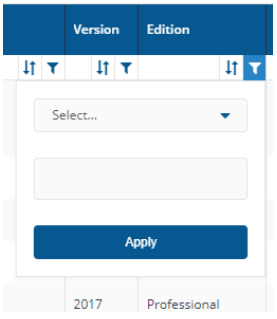


To filter the table on the **Edition** column:

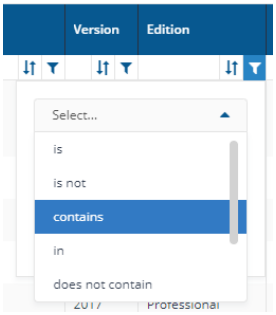
Click on the filter icon just beneath the header row in the **Edition** column.



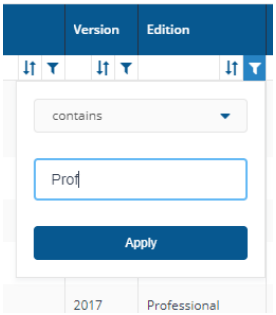
The filter popup is displayed.



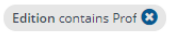
Now select the operator. In our example this will be **contains**.



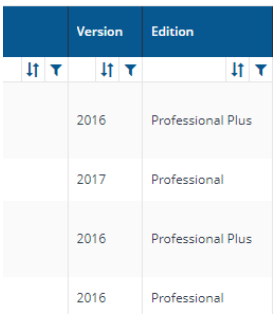
Then type the text **Prof** into the text field.



Click **Apply** and a new filter will be added to the table.

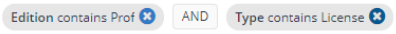


The table will be filtered to just those items whose **Edition** contains the text **Prof**.



Adding another filter

You can add another filter by clicking on the filter icon for any of the columns. The picture opposite shows another filter added selecting table rows where the **Type** also contains the text **License**. The table will also be filtered accordingly.

Field	Description
	 **Removing filters** You can remove filters by clicking on the filter close icon at the end of the filter.

10.6.5.1.2.1 New License page

A description of the fields in each section of the **New License** page. This also covers the **Edit License** page.

A license entitlement type in AppClarity specifies the rights and limitations of software and/or services that may be installed and/or used on an organizations computing devices. For example you could specify a license for Microsoft Visio 2016 and enable version downgrade rights to ensure that the license covers all versions up to 2016.

The sections on the **New License** or **Edit License** page are:

The Summary panel

Basic Information

Product

Coverage

Entitlement Term

Rights

Costs

Entitlement Links

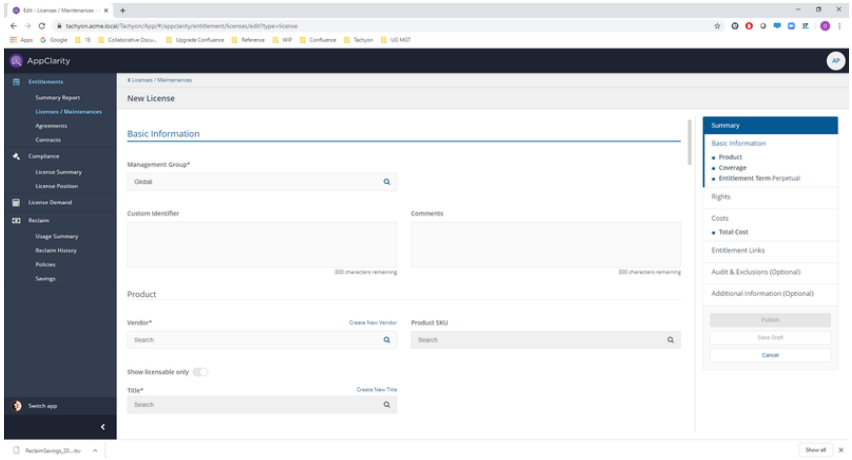
Parent

Associations

Children

Audit & Exclusions (Optional)

Additional information (Optional)

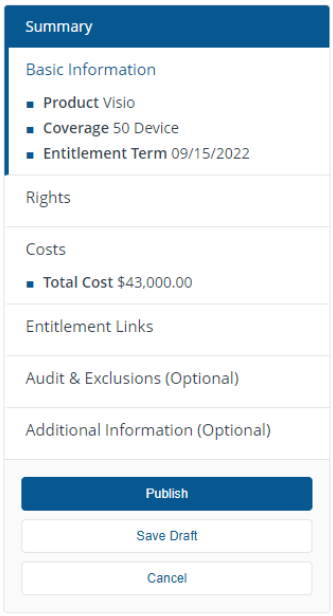


10.6.5.1.2.1.1 The Summary panel

The Summary panel on the right-hand side of the entitlement displays a summary of the settings that have been made in the entitlement so far. It's always visible on screen and can be used to navigate between the various sections of the entitlement.

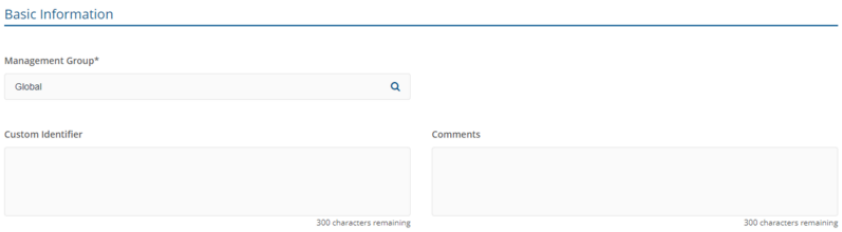
The panel also contains the following buttons:

Button	Description
Publish	Publishes the entitlement so it becomes active.
Save Draft	Saves the current settings in the entitlement to a draft. This can be used to save edits if you are part way through creating or making changes to the entitlement. It can also be used to inactivate an entitlement by removing its published status.
Cancel	Cancels the current edits and closes the page.



10.6.5.1.2.1.2 Basic Information

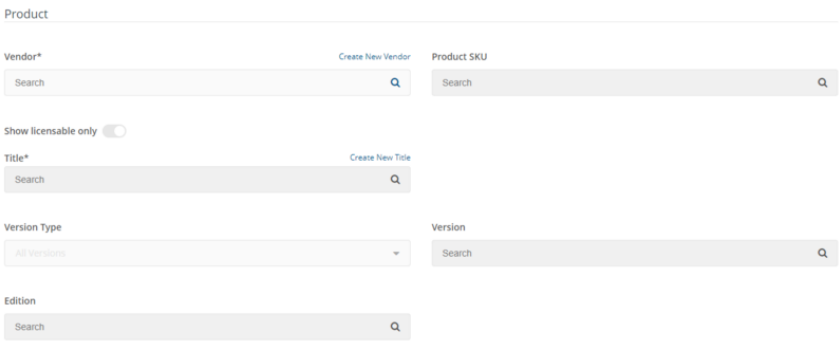
This section deals with the basic information for the entitlement, such as details of the product, the coverage and term of the entitlement.



Field	Details
Management Group*	Here you can associate the entitlement with Management Group of your choice.
Custom Identifier	An optional field. You can specify any alpha-numeric value to help identify the entitlement in the**Draft**and**Published**pages and when linking to other entitlements.
Comments	Enter text here to store any comments you have related to the entitlement.

10.6.5.1.2.1.2.1 Product

This sub-section defines the product covered by the entitlement.

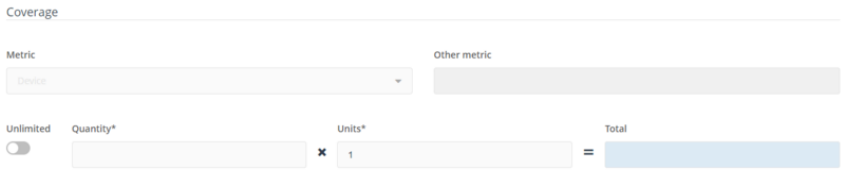


Field	Details
Vendor*	Defines the vendor of the product the license will apply to. The vendor part of the vendor, title, version and edition for a product. This must be filled out before any other fields. Suggested suitable vendors that match your text are displayed as you type into the field, which you can select to auto-complete the entry.
Product SKU	Suggested matching SKU are displayed as you type into the field, which you can select to auto-complete the entry. When you select a SKU other fields in the license will be automatically prefilled. For example, selecting the SKU for a particular edition of Microsoft Office 365 may set the **License Type** to **Subscription**, the **Product title** to **Office 365** and the **Edition** to **ProPlus**. These fields will then be fixed as they are derived from the SKU and not entered by hand.
Show licensable only	This toggle, which is on by default, sets whether the matches from 1E Catalog are filtered to show only products that are marked as licensable - and therefore appropriate for entitlements. You can flip this to off, if the product you are looking for is not visible and you're not sure if it's licensable or not, to see the unfiltered list of product related information from 1E Catalog.
Title*	Defines the title of the product the license will apply to. This is a mandatory field. The title part of the vendor, title, version and edition for a product. Suggested suitable titles from the selected vendor that match your text are displayed as you type into the field, which you can select to auto-complete the entry.
Version Type	**All Versions**, **Dot Format**,or **Colloquial**. By default this is set to**All Versions**.
Version	Defines the version of the product the license will apply to.

Field	Details
	The version part of the vendor, title, version and edition for a product. The Version format is dependent on the chosen **Version Type**. This field is disabled for a **Version Type** of **All Versions.**
Edition	Defines the edition of the product the license will apply to. The edition part of the vendor, title, version and edition for a product. Suggested suitable editions for the selected vendor and title that match your text are displayed as you type into the field, which you can select to auto-complete the entry.

10.6.5.1.2.1.2.2 Coverage

This sub-section defines the coverage details for the entitlement, such as: the metric that will be used for the entitlement and the number of installations the entitlement covers, i.e. whether the entitlement is unlimited or defined by a specific quantity of units.



Field	Details
Metric	The metric type for a license or maintenance entitlement. This may be one of:

Type	Description
Core	The metric for the license is related to the number of cores present on a device. For example, licenses for **Microsoft SQL database** are related to the number of cores on the server where **Microsoft SQL** is installed.
Device	The metric for the license is for devices. For example licenses for **Microsoft Visio** are on a per device basis. This is the default type.
Other	This can be used to reference your own license metric type.
Processor	The metric for the license is related to the number of processors for a device. For example, licenses for certain **Oracle** products are related

Field	Details	
		to the number of processors on the server where the **Oracle** product is installed.
	PVU	The metric for the license is related to the Processor Value Unit present on a device. For example. licenses for **IBM** products are related to the **Processor Value Unit (PVU)** for the device where the IBM product is installed.
	User	The metric for the license is related to the users for the product. For example, **Microsoft Office 365** licenses are related to users and not the devices the software is running on.
	The **Metric** works with the **Quantity** field to determine how licenses are applied.	
Other metric	This field is enabled if the Metric field is set to Other and allows you to specify an entitlement metric that is not covered by default in AppClarity. This field is only enabled if **Other** is selected in the **Metric Type** for entitlements and allows you to enter a metric that is not covered by the basic **Metric Type** options.	
Unlimited	If you set the**Unlimited**toggle to on, this entitlement will cover all installations and the**Quantity**and **Units** fields will be disabled.	
Quantity	Sets the number of licenses bought for this entitlement. Only enabled if the **Unlimited** toggle is set to off, in which case this field is also mandatory.	
Units	Sets the number of units per licenses purchased. Only enabled if the**Unlimited**toggle is set to off, in which case this field is also mandatory.	
Total	The total number of licenses, which is the Quantity value times the Units value. AppClarity will count each unit in the **Total** field against a single unit of the given **Metric** type. So if the **Metric** type is **Device** and the **Total** calculates to **50** this will count against **50** devices. For an SQL Server Enterprise example the **Metric** type would be **Core** so this will count against **50** cores.	

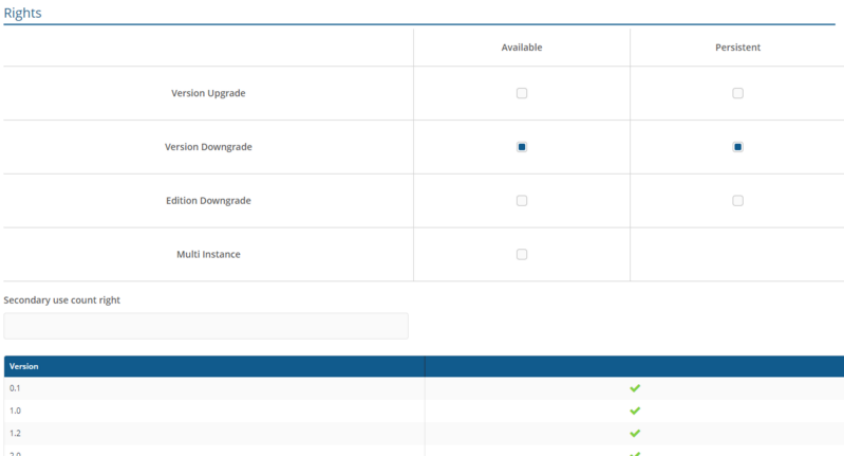
10.6.5.1.2.1.2.3 Entitlement Term

This sub-section defines the type and length details for the entitlement, such as: the type (perpetual or subscription), the start date and, if the type is subscription, the duration and end date.

Field	Details
Entitlement Type	For License entitlements this can be set to **Perpetual** or **Subscription**. By default this is set to **Perpetual**. For Maintenance entitlements this can only be set to **Subscription**.
Start Date*	When the entitlement starts applying. This defaults to the date the entitlement was created.
Duration*	The **Duration** and **End Date** fields are only enabled for **Subscription** entitlements. If you set the **Duration** the **End Date** is calculated. If you set the **End Date** the **Duration** is calculated. These fields determine how long the entitlement is applicable for after start date. The **Duration** is set in terms of months and determines the number of months the entitlement will be valid for.
End Date*	The **Duration** and **End Date** fields are only enabled for **Subscription** entitlements. If you set the **Duration** the **End Date** is calculated. If you set the **End Date** the **Duration** is calculated. These fields determine how long the entitlement is applicable for after start date. The **End Date** indicates the last date the entitlement will be valid until and is set using a date picker.

10.6.5.1.2.1.3 Rights

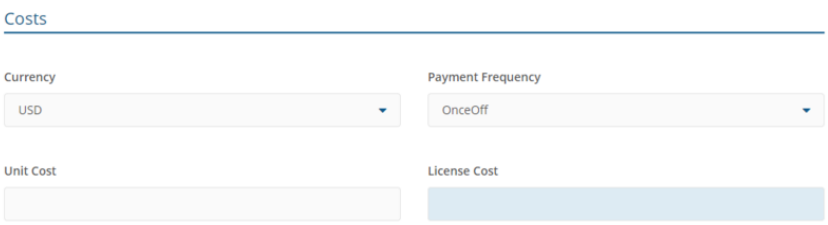
This section lets you control how the entitlement applies to existing versions of the product it's related to.

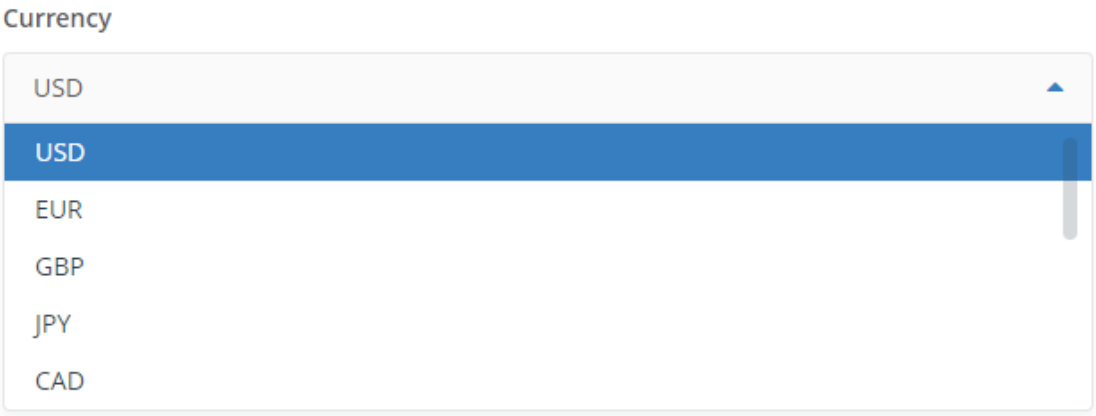


Field	Details
Version Upgrade	Rights to check if the entitlement is also applicable on higher versions of selected version
Version Downgrade	Rights to check if the entitlement is also applicable on lower versions of selected version. By default it is true
Edition Downgrade	Rights to check if the entitlement is also applicable on lower editions of selected edition
Multi Instance	Rights to check if the same license is also applicable on multiple installations on same device
Secondary use count right	The available count of secondary uses
Versions covered	The table below the fields shows the overall versions and editions covered by the entitlement based on the selected rights.

10.6.5.1.2.1.4 Costs

This section lets you control how the entitlement is costed and how it can be considered within the overall spend.

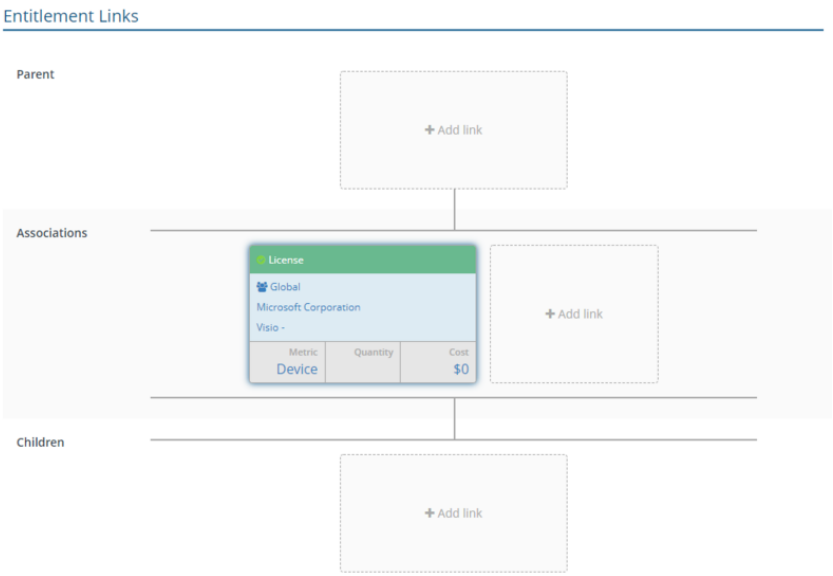


Field	Details
Currency	The currency applied to the entitlement. Clicking on the Currency field displays a list of currencies to choose from. 
Payment Frequency	**OnceOff, Monthly, Quarterly, Yearly**. The default is **OnceOff**.
Unit Cost	The cost of the licence per unit, combined with the **Quantity** and **Unit Cost Type** values to calculate the license cost.
License Cost	This is calculated based on value filed in the **Quantity**, **Unit Cost** and **Payment Frequency**. This value only displays the cost and cannot be edited directly.

10.6.5.1.2.1.5 Entitlement Links

This section lets you create links between your entitlements. If you are creating a new entitlement this section will initially look like this:

After you have saved the entitlement this section provides an interface for linking it to other entitlements:

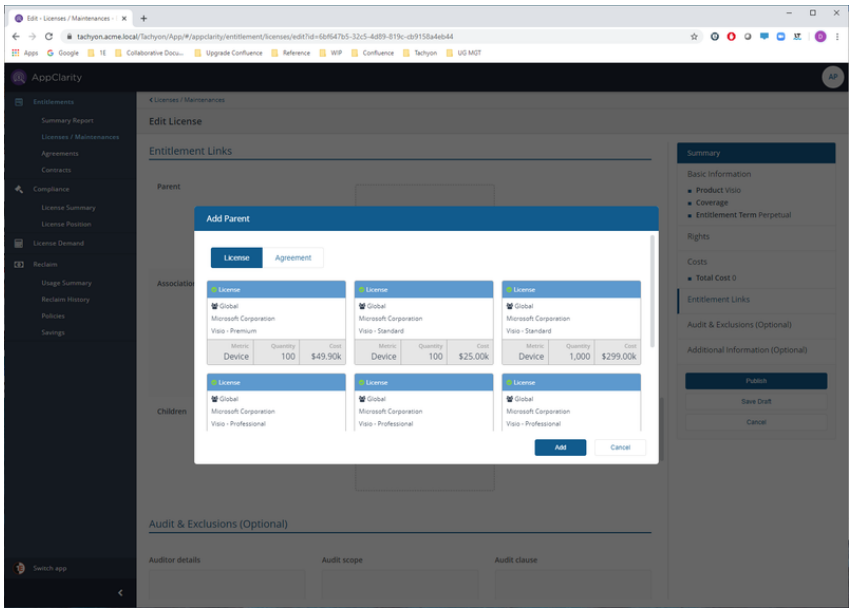


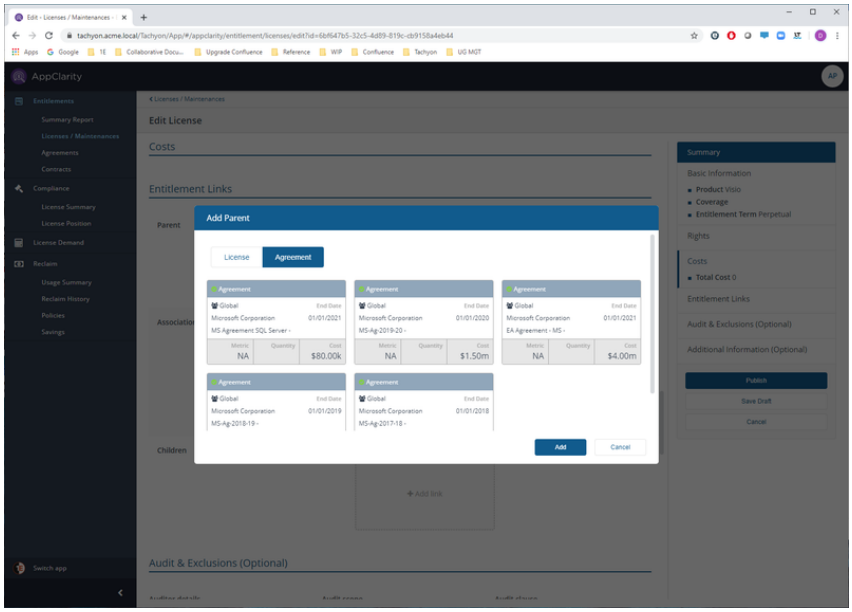
There are three sub-sections:

10.6.5.1.2.1.5.1 Parent

Here you can link parent licenses or agreements. Clicking on the **+Add link** area displays the **Add Parent** popup.

Select **License** or **Agreement** to add that type of link, a list of entitlements of the selected type will be displayed. Click on any of these and a green check mark will appear to indicate the selected parent, you can only select one. Once you've made your choice click the **Add** button to link the checked parent.

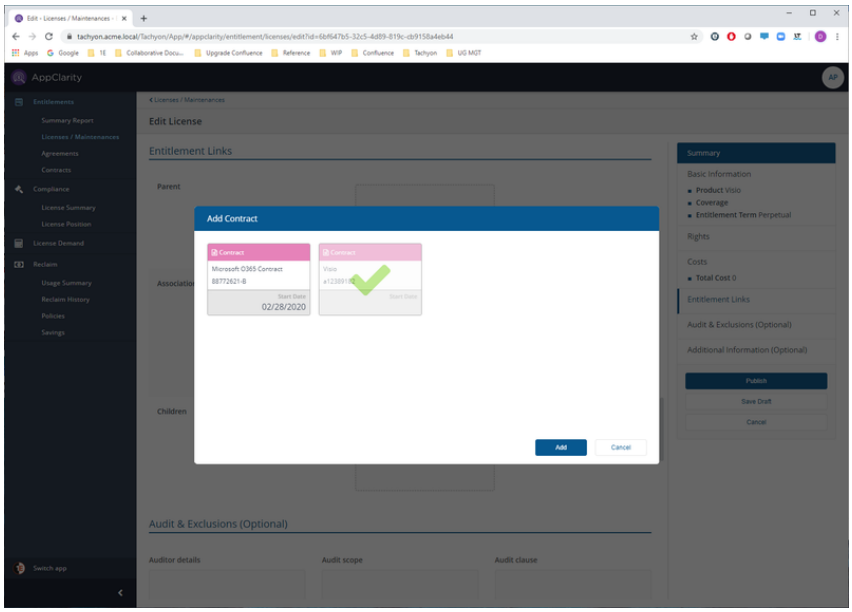




10.6.5.1.2.1.5.2 Associations

Here you can link contracts. Clicking on the **+Add link** area displays the **Add Contract** popup.

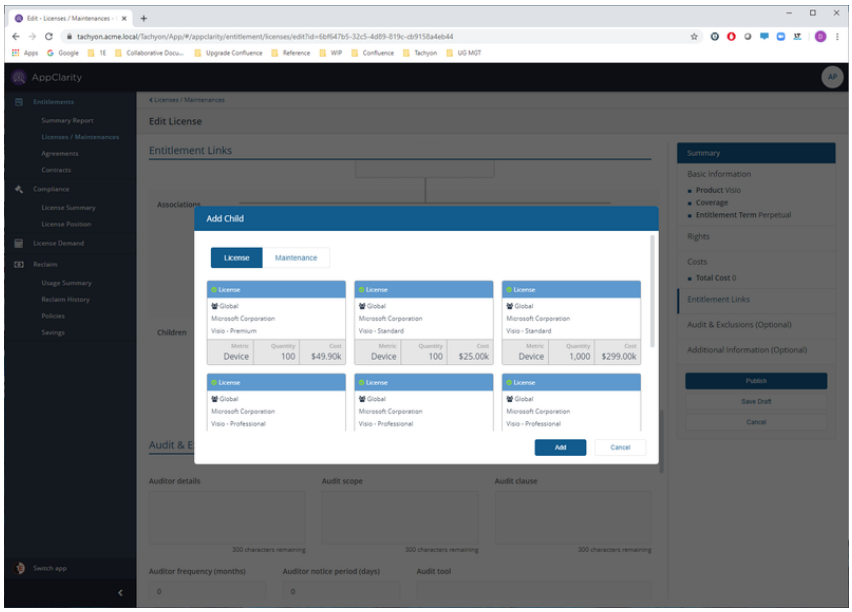
A list of contracts will be displayed. Click on any of these and a green check mark will appear to indicate the selected contract, you can select more than one contract to link. Once you've made your choice click the **Add** button to link the checked contract(s).



10.6.5.1.2.1.5.3 Children

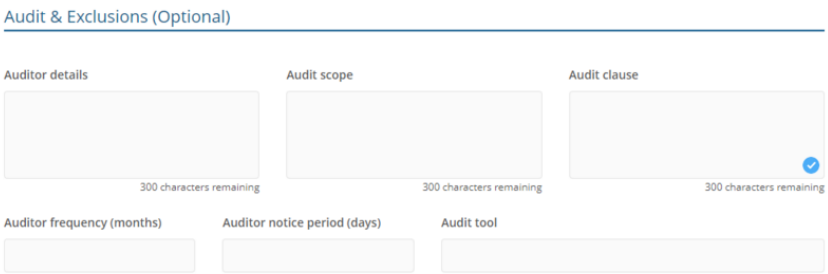
Here you can link child licenses or maintenances. Clicking on the **+Add link** area displays the **Add Child** popup.

Select **License** or **Agreement** to add that type of link, a list of entitlements of the selected type will be displayed. Click on any of these and a green check mark will appear to indicate the selected child - you can select more than one. Once you've made your choice click the **Add** button to link the checked children.



10.6.5.1.2.1.6 Audit & Exclusions (Optional)

This section lets you control how the entitlement is audited.



Field	Details
Auditor Details	Organizations that are allowed to perform the audit including (if appropriate), the licensor organization and any third-party organizations, according to what was agreed in the contract.
Audit Scope	Defines what part of the software customer organization is allowed to be audited.
Audit Clause	Provides additional information on what could trigger the audit.

Field	Details
Auditor Frequency	Definition of the highest agreed frequency of the audit expressed in months.
Auditor Notice period	Notice period in days.
Audit Tool	Name of the tool(s) which are approved for use in the audit.

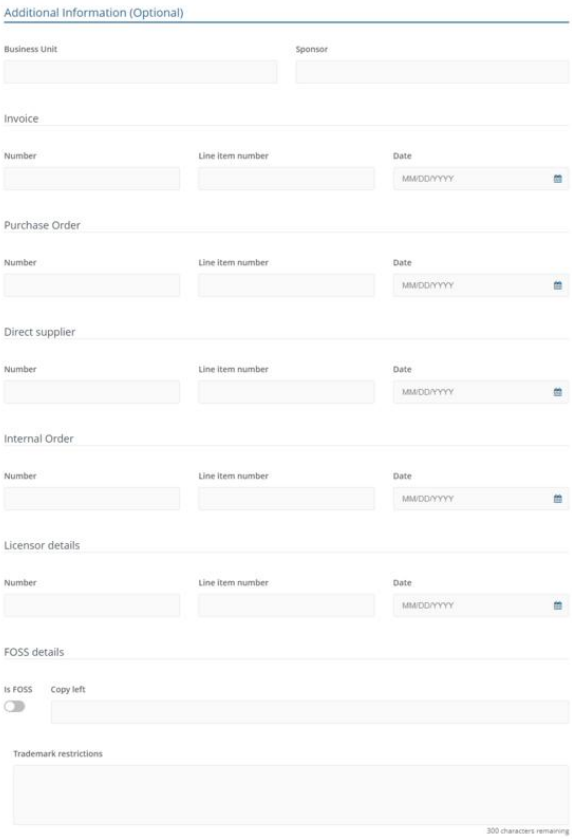
10.6.5.1.2.1.7 Additional information (Optional)

This section lets you enter additional information related to the entitlement that may come from a Vendor agreement or contract.

Sub-Section	Field	Field Details
	Business Unit	Specifies the Business Unit the agreement will be applied to. This may correspond to your management groups, depending on how you have those configured.
Sponsor	Name of the person who manages the budget associated with an agreement (this field is likely to be used only on agreements, but could be extended to other entitlements)	
Invoice	Number	The invoice number, usually specified in the customer contract.
Line Item Number	This optionally identifies the line number (if provided) on the customer contract that pertains to the invoice.	
Date	The date for the invoice.	
Purchase Order	Number	The purchase order number, usually specified in the customer contract.

Sub-Section	Field	Field Details
Line Item Number	This optionally identifies the line number (if provided) on the customer contract that pertains to the purchase order.	
Date	The date for the purchase order.	
Direct Supplier	Number	The number that identifies the direct supplier. For example, in some organizations this may be the same as the contract number.
Line Item Number	This optionally identifies the line number (if provided) on the contract that pertains to the direct supplier.	
Date	The date for the contract.	
Internal Order	Number	The ITARS or similar internal identifier for the order as specified in the customer contract.
Line Item Number	This optionally identifies the line number(if provided)on the contract that pertains to the internal order.	
Date	The date for the contract.	
Licensor Details	Number	The number (or name) of the licensor, could be the vendor or a VAR.
Line Item Number	This is intended as a reference to a licensor source other than an invoice, e.g. to an on-line portal of license purchases.	
Date	The date for the contract.	
FOSS Details	IsFoss	This value is true only if the granted rights fulfill the

Sub-Section	Field	Field Details
		requirements of both definition of the Free software maintained by the Free Software Foundation.
Copy Left	This value provides information on whether derivative works (which are always allowed for open source software) are themselves required to be open source software. There are three allowed values: “strong” means that all kinds of derivative works are required to be open source software themselves, “no” means that for all kinds of derivative works, it is allowed to distribute the derivative work as proprietary software. The intermediate value of “weak” means that there are some restrictions and the details are to be checked in the license.	
Trademark restrictions	FOSS trademark restrictions.	



10.6.5.1.2.2 New Maintenance page

A description of the fields in each section of the **Create Maintenance** page. This also covers the **Edit Maintenance** page.

A Maintenance entitlement type in AppClarity specifies the rights and limitations for an organization to install and/or use updated versions of software defined in a license. For example you could specify a maintenance entitlement for Microsoft Visio 2016 to cover all new versions from the current date for the next 3 years.

The sections on the **New Maintenance** or **Edit Maintenance** page are:

The Summary panel

Basic Information

Product

Coverage

Entitlement Term

Rights

Costs

Entitlement Links

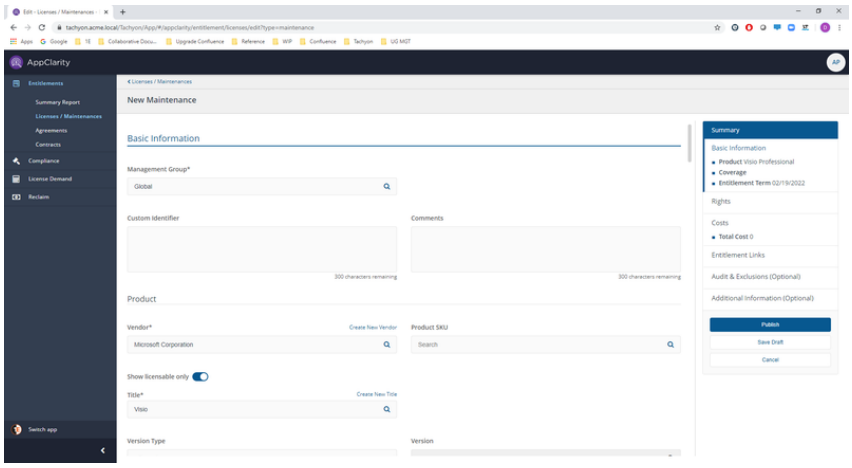
Parent

Associations

Children

Audit & Exclusions (Optional)

Additional information (Optional)



10.6.5.1.2.2.1 The Summary panel

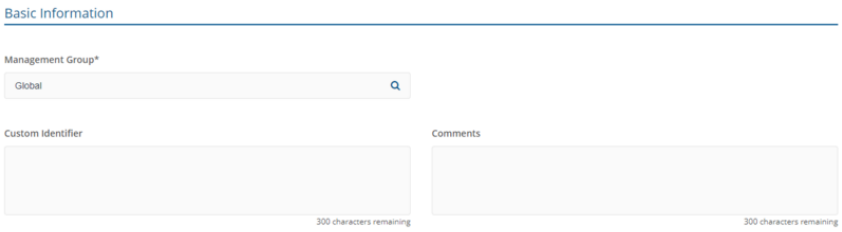
The Summary panel on the right-hand side of the entitlement displays a summary of the settings that have been made in the entitlement so far. It's always visible on screen and can be used to navigate between the various sections of the entitlement.

The panel also contains the following buttons:

Button	Description
Publish	Publishes the entitlement so it becomes active.
Save Draft	Saves the current settings in the entitlement to a draft. This can be used to save edits if you are part way through creating or making changes to the entitlement. It can also be used to inactivate an entitlement by removing its published status.
Cancel	Cancels the current edits and closes the page.

10.6.5.1.2.2.2 Basic Information

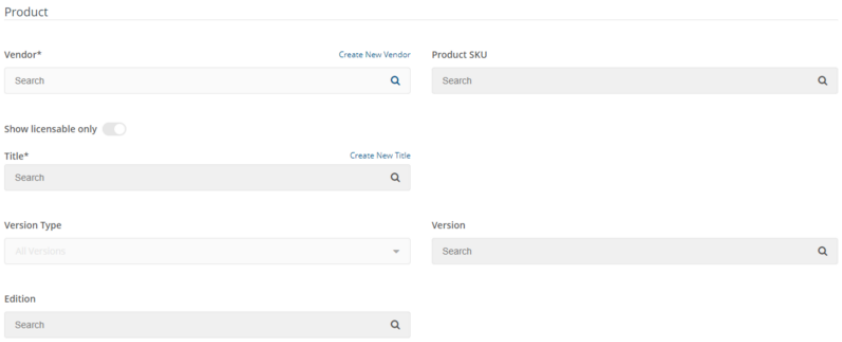
This section deals with the basic information for the entitlement, such as details of the product, the coverage and term of the entitlement.



Field	Details
Management Group*	Here you can associate the entitlement with Management Group of your choice.
Custom Identifier	An optional field. You can specify any alpha-numeric value to help identify the entitlement in the**Draft**and**Published**pages and when linking to other entitlements.
Comments	Enter text here to store any comments you have related to the entitlement.

10.6.5.1.2.2.2.1 Product

This sub-section defines the product covered by the entitlement.

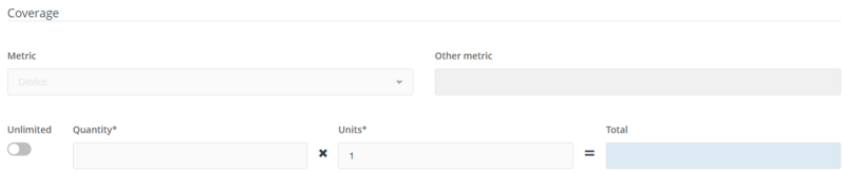


Field	Details
Vendor*	Defines the vendor of the product the license will apply to.The vendor part of the vendor, title, version and edition for a product. This must be filled out before any other fields. Suggested suitable vendors that match your text are displayed as you type into the field, which you can select to auto-complete the entry.
Product SKU	Suggested matching SKU are displayed as you type into the field, which you can select to auto-complete the entry. When you select a SKU other fields in the license will be automatically prefilled. For example, selecting the SKU for a particular edition of Microsoft Office 365 may set the **License Type** to **Subscription**, the **Product title** to **Office 365** and the

Field	Details
	Edition to **ProPlus**. These fields will then be fixed as they are derived from the SKU and not entered by hand.
Show licensable only	This toggle, which is on by default, sets whether the matches from 1E Catalog are filtered to show only products that are marked as licensable - and therefore appropriate for entitlements. You can flip this to off, if the product you are looking for is not visible and you're not sure if it's licensable or not, to see the unfiltered list of product related information from 1E Catalog.
Title*	Defines the title of the product the license will apply to. This is a mandatory field.The title part of the vendor, title, version and edition for a product. Suggested suitable titles from the selected vendor that match your text are displayed as you type into the field, which you can select to auto-complete the entry.
Version Type	**All Versions**, **Dot Format**,or **Colloquial**. By default this is set to**All Versions**.
Version	Defines the version of the product the license will apply to.The version part of the vendor, title, version and edition for a product. The Version format is dependent on the chosen **Version Type**. This field is disabled for a **Version Type** of **All Versions.**
Edition	Defines the edition of the product the license will apply to.The edition part of the vendor, title, version and edition for a product. Suggested suitable editions for the selected vendor and title that match your text are displayed as you type into the field, which you can select to auto-complete the entry.

10.6.5.1.2.2.2.2 Coverage

This sub-section defines the coverage details for the entitlement, such as: the metric that will be used for the entitlement and the number of installations the entitlement covers, i.e. whether the entitlement is unlimited or defined by a specific quantity of units.



Field	Details
Metric	The metric type for a license or maintenance entitlement. This may be one of:

Type	Description
Core	The metric for the license is related to the number of cores present on a device. For example, licenses for **Microsoft SQL database** are related to the number of cores on the server where **Microsoft SQL** is installed.
Device	The metric for the license is for devices. For example licenses for **Microsoft Visio** are on a per device basis. This is the default type.
Other	This can be used to reference your own license metric type.
Processor	The metric for the license is related to the number of processors for a device. For example, licenses for certain **Oracle** products are related to the number of processors on the server where the **Oracle** product is installed.
PVU	The metric for the license is related to the Processor Value Unit present on a device. For example. licenses for **IBM** products are related to the **Processor Value Unit (PVU)** for the device where the IBM product is installed.
User	The metric for the license is related to the users for the product. For example, **Microsoft Office 365** licenses are related to users and not the devices the software is running on.

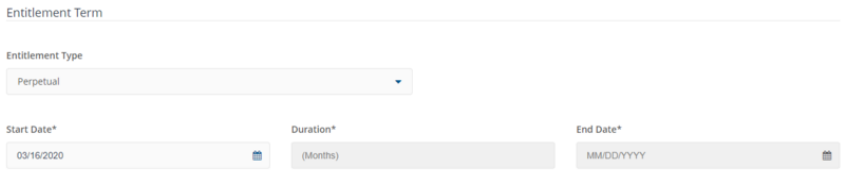
The **Metric** works with the **Quantity** field to determine how licenses are applied.

Other metric	This field is enabled if the Metric field is set to Other and allows you to specify an entitlement metric that is not covered by default in AppClarity. This field is only enabled if **Other** is selected in the **Metric Type** for entitlements and allows you to enter a metric that is not covered by the basic **Metric Type** options.
Unlimited	If you set the**Unlimited**toggle to on, this entitlement will cover all installations and the**Quantity**and **Units** fields will be disabled.

Field	Details
Quantity	Sets the number of licenses bought for this entitlement. Only enabled if the **Unlimited** toggle is set to off, in which case this field is also mandatory.
Units	Sets the number of units per licenses purchased. Only enabled if the**Unlimited**toggle is set to off, in which case this field is also mandatory.
Total	The total number of licenses, which is the Quantity value times the Units value. AppClarity will count each unit in the **Total** field against a single unit of the given **Metric** type. So if the **Metric** type is **Device** and the **Total** calculates to **50** this will count against **50** devices. For an SQL Server Enterprise example the **Metric** type would be **Core** so this will count against **50** cores.

10.6.5.1.2.2.3 Entitlement Term

This sub-section defines the type and length details for the entitlement, such as: the start date and the duration and end date.

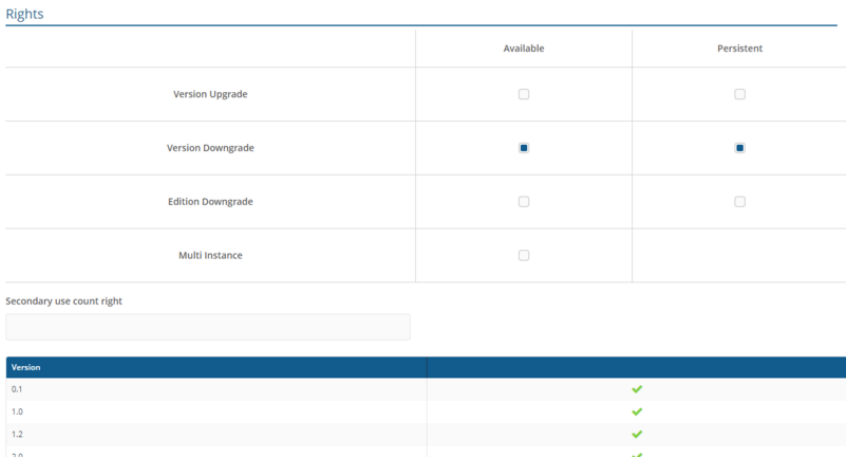


Field	Details
Entitlement Type	For License entitlements this can be set to **Perpetual** or **Subscription**. By default this is set to **Perpetual**. For Maintenance entitlements this can only be set to **Subscription**.
Start Date*	When the entitlement starts applying. This defaults to the date the entitlement was created.
Duration*	The **Duration** and **End Date** fields are only enabled for **Subscription** entitlements. If you set the **Duration** the **End Date** is calculated. If you set the **End Date** the **Duration** is calculated. These fields determine how long the entitlement is applicable for after start date.

Field	Details
	The **Duration** is set in terms of months and determines the number of months the entitlement will be valid for.
End Date*	The **Duration** and **End Date** fields are only enabled for **Subscription** entitlements. If you set the **Duration** the **End Date** is calculated. If you set the **End Date** the **Duration** is calculated. These fields determine how long the entitlement is applicable for after start date. The **End Date** indicates the last date the entitlement will be valid until and is set using a date picker.

10.6.5.1.2.2.3 Rights

This section lets you control how the entitlement applies to existing versions of the product it's related to.

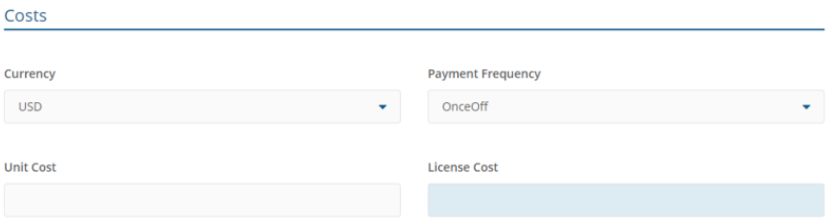


Field	Details
Version Upgrade	Rights to check if the entitlement is also applicable on higher versions of selected version
Version Downgrade	Rights to check if the entitlement is also applicable on lower versions of selected version. By default it is true
Edition Downgrade	Rights to check if the entitlement is also applicable on lower editions of selected edition

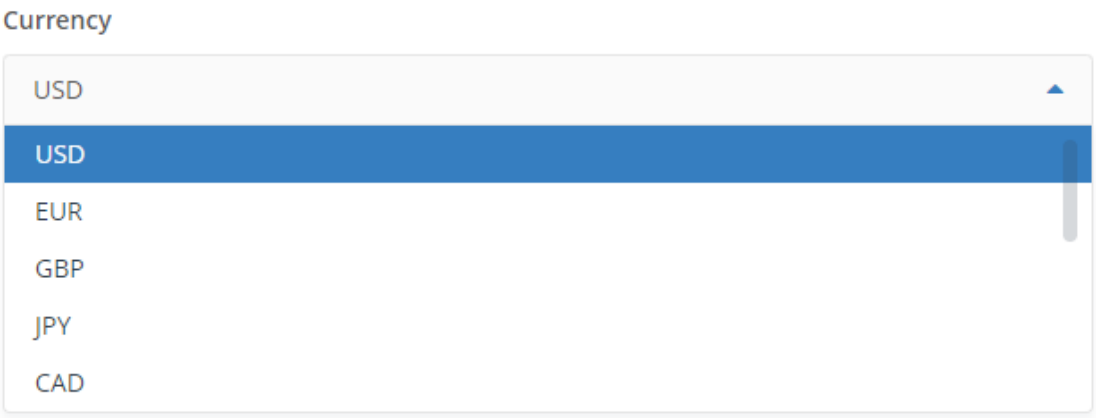
Field	Details
Multi Instance	Rights to check if the same license is also applicable on multiple installations on same device
Secondary use count right	The available count of secondary uses
Versions covered	The table below the fields shows the overall versions and editions covered by the entitlement based on the selected rights.

10.6.5.1.2.2.4 Costs

This section lets you control how the entitlement is costed and how it can be considered within the overall spend.



Field	Details
Currency	The currency applied to the entitlement. Clicking on the Currency field displays a list of currencies to choose from.
Payment Frequency	**OnceOff, Monthly, Quarterly, Yearly**. The default is **OnceOff**.

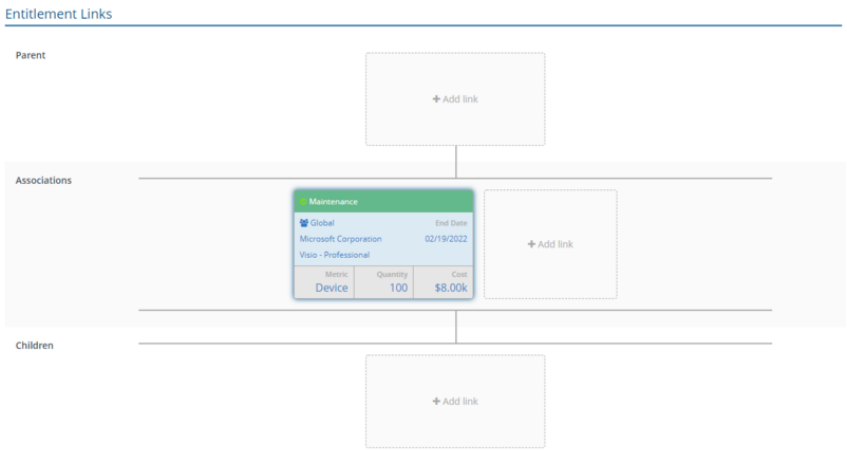


Field	Details
Unit Cost	The cost of the licence per unit, combined with the **Quantity** and **Unit Cost Type** values to calculate the license cost.
License Cost	This is calculated based on value filed in the **Quantity**, **Unit Cost** and **Payment Frequency**. This value only displays the cost and cannot be edited directly.

10.6.5.1.2.2.5 Entitlement Links

This section lets you create links between your entitlements. If you are creating a new entitlement this section will initially look like this:

After you have saved the entitlement this section provides an interface for linking it to other entitlements:

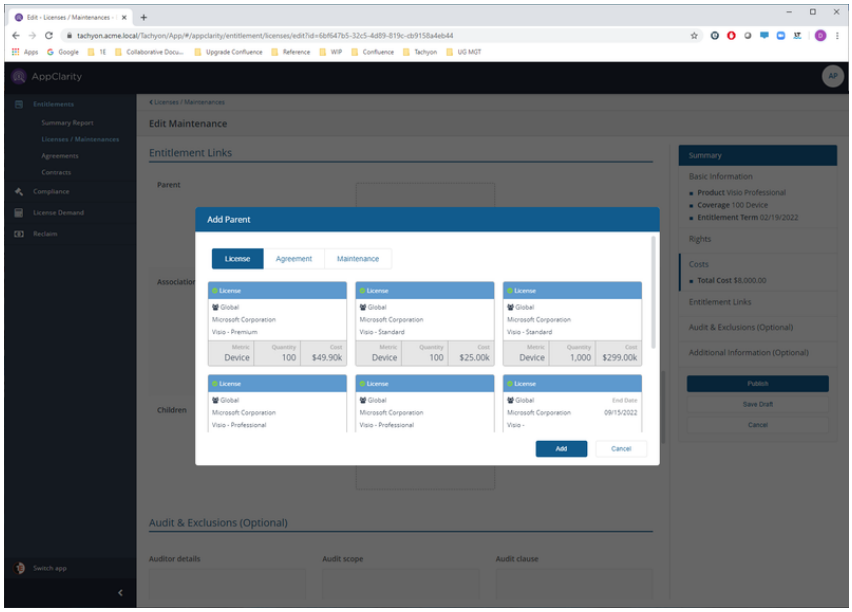


There are three sub-sections:

10.6.5.1.2.2.5.1 Parent

Here you can link a parent license, agreement or maintenance. Clicking on the **+Add link** area displays the **Add Parent** popup.

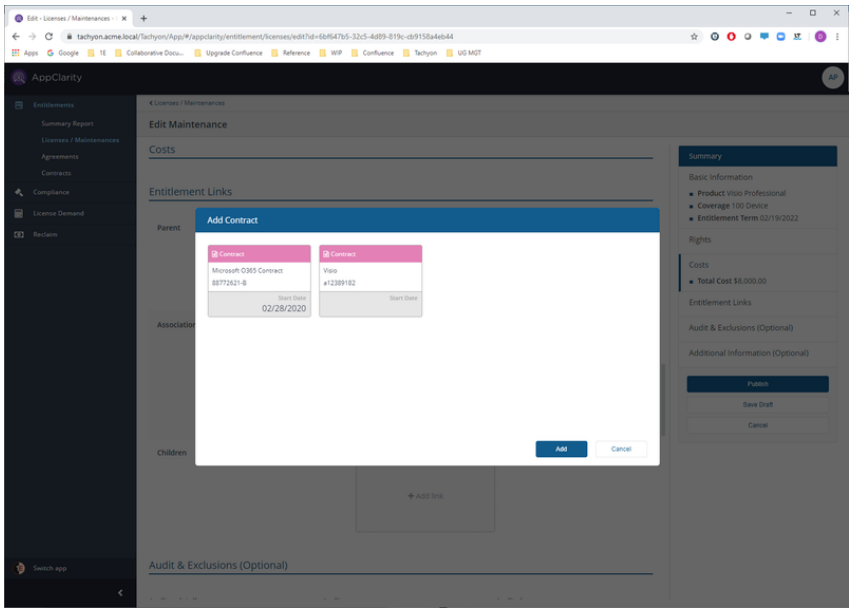
Select **License**, **Agreement** or **Maintenance** to add that type of link - a list of entitlements of the selected type will be displayed. Click on any of these and a green check mark will appear to indicate the selected parent, you can only select one. Once you've made your choice click the **Add** button to link the checked parent.



10.6.5.1.2.2.5.2 Associations

Here you can link contracts. Clicking on the **+Add link** area displays the **Add Contract** popup.

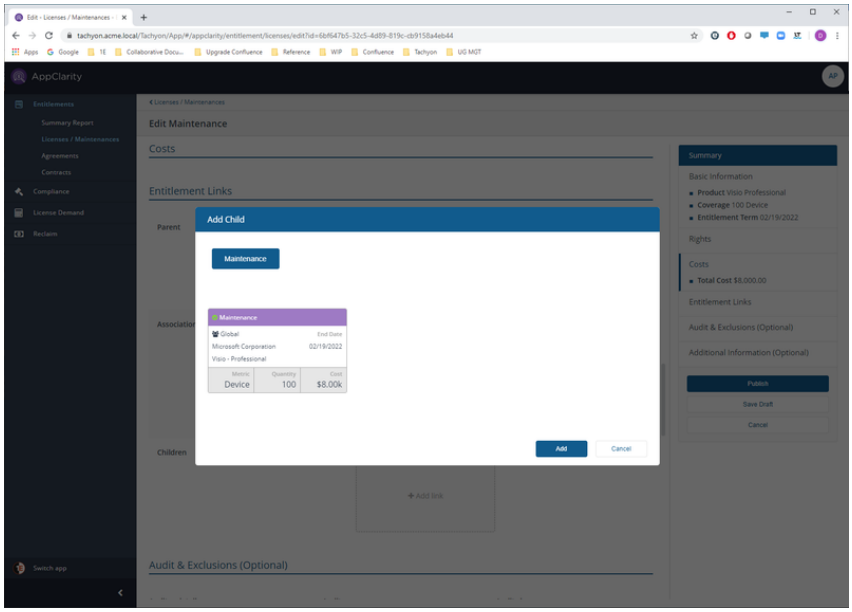
A list of contracts will be displayed. Click on any of these and a green check mark will appear to indicate the selected contract, you can select more than one contract to link. Once you've made your choice click the **Add** button to link the checked contract(s).



10.6.5.1.2.2.5.3 Children

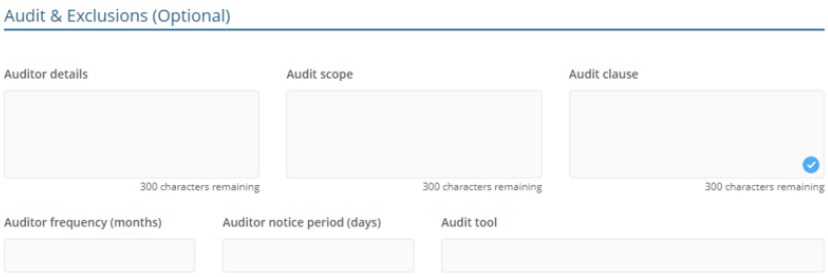
Here you can link child maintenances. Clicking on the **+Add link** area displays the **Add Child** popup.

A list of maintenance entitlements is displayed. Click on any of these and a green check mark will appear to indicate the selected child - you can select more than one child. Once you've made your choice click the **Add** button to link the checked children.



10.6.5.1.2.2.6 Audit & Exclusions (Optional)

This section lets you control how the entitlement is audited.



Field	Details
Auditor Details	Organizations that are allowed to perform the audit including (if appropriate), the licensor organization and any third-party organizations, according to what was agreed in the contract.
Audit Scope	Defines what part of the software customer organization is allowed to be audited.
Audit Clause	Provides additional information on what could trigger the audit.
Auditor Frequency	Definition of the highest agreed frequency of the audit expressed in months.

Field	Details
Auditor Notice period	Notice period in days.
Audit Tool	Name of the tool(s) which are approved for use in the audit.

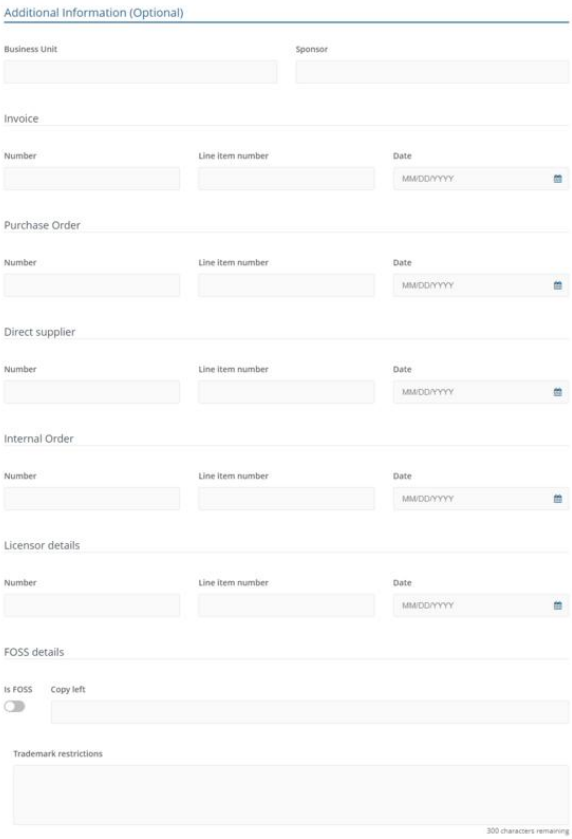
10.6.5.1.2.2.7 Additional information (Optional)

This section lets you enter additional information related to the entitlement that may come from a Vendor agreement or contract.

Sub-Section	Field	Field Details
	Business Unit	Specifies the Business Unit the agreement will be applied to. This may correspond to your management groups, depending on how you have those configured.
Sponsor	Name of the person who manages the budget associated with an agreement (this field is likely to be used only on agreements, but could be extended to other entitlements)	
Invoice	Number	The invoice number, usually specified in the customer contract.
Line Item Number	This optionally identifies the line number (if provided) on the customer contract that pertains to the invoice.	
Date	The date for the invoice.	
Purchase Order	Number	The purchase order number, usually specified in the customer contract.

Sub-Section	Field	Field Details
Line Item Number	This optionally identifies the line number (if provided) on the customer contract that pertains to the purchase order.	
Date	The date for the purchase order.	
Direct Supplier	Number	The number that identifies the direct supplier. For example, in some organizations this may be the same as the contract number.
Line Item Number	This optionally identifies the line number (if provided) on the contract that pertains to the direct supplier.	
Date	The date for the contract.	
Internal Order	Number	The ITARS or similar internal identifier for the order as specified in the customer contract.
Line Item Number	This optionally identifies the line number(if provided)on the contract that pertains to the internal order.	
Date	The date for the contract.	
Licensor Details	Number	The number (or name) of the licensor, could be the vendor or a VAR.
Line Item Number	This is intended as a reference to a licensor source other than an invoice, e.g. to an on-line portal of license purchases.	
Date	The date for the contract.	
FOSS Details	IsFoss	This value is true only if the granted rights fulfill the

Sub-Section	Field	Field Details
		requirements of both definition of the Free software maintained by the Free Software Foundation.
Copy Left	This value provides information on whether derivative works (which are always allowed for open source software) are themselves required to be open source software. There are three allowed values: “strong” means that all kinds of derivative works are required to be open source software themselves, “no” means that for all kinds of derivative works, it is allowed to distribute the derivative work as proprietary software. The intermediate value of “weak” means that there are some restrictions and the details are to be checked in the license.	
Trademark restrictions	FOSS trademark restrictions.	



10.6.5.1.3 Agreements page

A description of the fields on the **Agreements** page.

Here you can view, edit, copy, create, publish and delete agreements. You can also export all the agreements in the selected repository to a TSV file. You get to this page by clicking the **AppClarity→Entitlements→Agreements** node in the navigation panel.

The fields on the **Agreements** page are:

Report RefreshReport Refresh

Active Agreements only toggle

Status filters

Column Picker

Agreements table

Vendor

Name

Number

Start Date

End Date

Cost

Management Group

Identifier

Links

Status

...

Column actions

Column sort

Column filter

Action Buttons

New Agreement

Edit

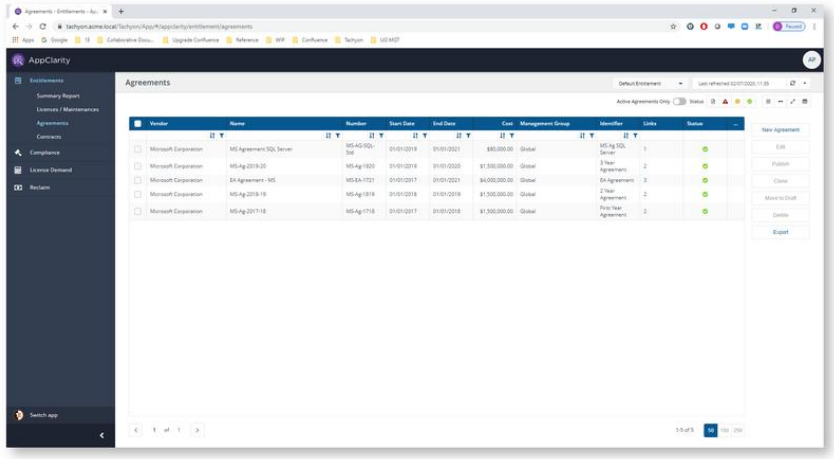
Publish

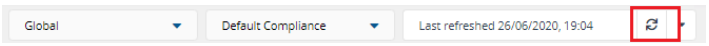
Clone

Move to Draft

Delete

Export



Field	Description
Report Refresh	You can refresh reports from individual AppClarity screens as well as using the Settings App. Where this is available you can do this by using the refresh icon next to the **Last Refreshed** box: 
Active Agreements only toggle	The **Active Agreements only** toggle adds a filter when it's turned on that filters the table to only display the agreements that have been published and not the ones that are in draft.
Status filters	The Status filters are displayed in the top-right of the page and let you filter the table according to the status of the items in the table. Clicking on an icon filters the table to display only items with that status, as described in the following table.
Column Picker	Where the column picker control is shown you can choose which columns are displayed. In the following example on the Microsoft Core License Demand page we hide the Unknown Installs column and move the License Demand column to the left of the page.To pick the displayed columns:Click on the Choose columns icon to the right of the header row to view the visable columns.To exclude Unknown Installs, select the Unknown Installs row and click Exclude columns button.The Unknown Installs column is now hidden.To move the License Demand column to the top of the list, hover your mouse over License Demand and using the direction control drag it to the top of the list.The Microsoft Core License Demand page has now been automatically updated with our changes.

Icon	Description
	Filters to show only items in Draft.
	Filters to show only items in Draft with errors.
	Filters to show only items in Draft with warnings.
	Filters to show only items that are Published.

Field	Description
Agreements table	The following table describes the columns displayed in the **Agreements** table:

Column	Description
Vendor	The vendor portion of the vendor, title, version and edition attributes that are used to identify which software products the entitlement or agreement is for. For example, **Microsoft Corporation** or **1E**. You can sort and filter on this column.
Name	The name used for the agreement. For example, you might want to define an agreement that covers all your Microsoft Office and related products, so you could name the agreement**Microsoft Office Agreement - 2018**. You can sort and filter on this column.
Number	Corresponds to the contract number, usually supplied on the customer contract. You can sort and filter on this column.
Start Date	When the agreement starts to be applicable. You can sort and filter on this column.
End Date	This is the last date the agreement is applicable until. You can sort and filter on this column.
Cost	The cost of the agreement as arranged with the Vendor. You can sort and filter on this column.
Management Group	Displays all of the management groups the software reclaim policy is associated with. You can sort and filter on this column.
Identifier	Displays the **Identifier** information configured for the entitlement or agreement.

Field	Description
	You can sort and filter on this column.
Links	Displays the **Parent**, **Associations** and **Children Links** to other entitlements, agreements or contracts configured for the entitlement or agreement.
Status	The icon indicates the status of the entitlement or agreement:

Icon	Description
	Draft.
	Draft with errors.
	Draft with warnings.
	Published.

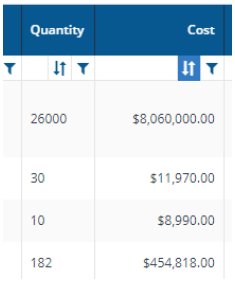
...

Column actions

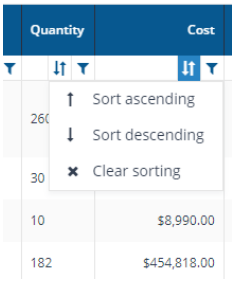
The following column actions are available on some columns in the table.

Column action	Description
Column sort	**Using column sorts** The picture opposite shows an example taken from AppClarity. In our example we want to sort the table on the **Cost** column from the highest cost at the top to the lowest at the bottom. To sort the table on the **Cost** column: Click on the sort icon just beneath the header row in the **Cost** column.

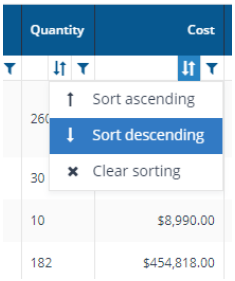
Field	Description



The sort popup is displayed.



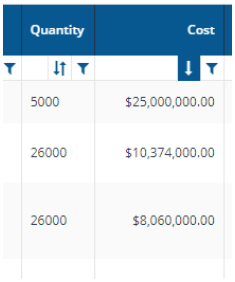
Now select the sort direction. In our example this will be **Sort descending**.



After selecting this the data in the table is now sorted on the **Cost** column from highest to lowest and the sort icon has changed to a sort descending icon

.

Field	Description



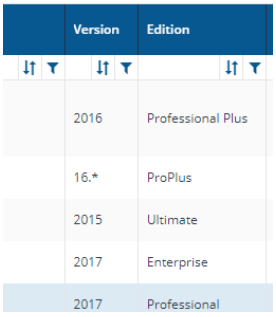
Clearing the sort

You can clear the sort by clicking on the sort icon again and selecting the **Clear sorting** menu item from the sorting popup.

Column filter

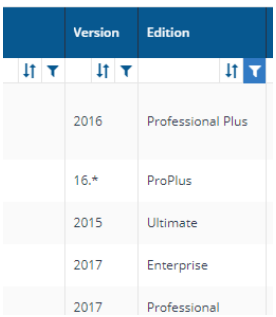
Using column filters

The picture opposite below an example taken from AppClarity. In our example we want to filter the table to show only those items where the **Edition** contains the text **Prof**.



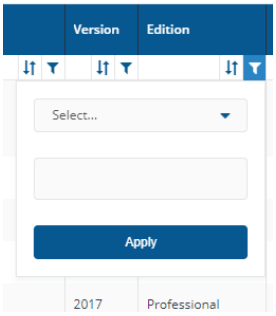
To filter the table on the **Edition** column:

Click on the filter icon just beneath the header row in the **Edition** column.

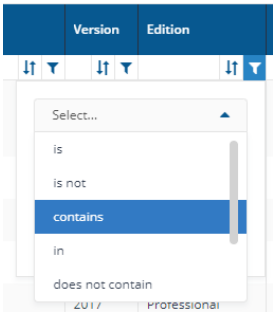


The filter popup is displayed.

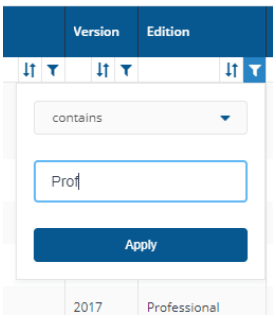
Field	Description



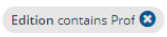
Now select the operator. In our example this will be **contains**.



Then type the text **Prof** into the text field.

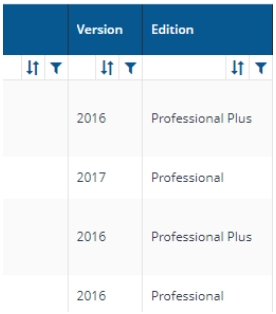


Click **Apply** and a new filter will be added to the table.



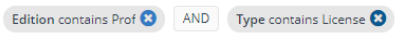
The table will be filtered to just those items whose **Edition** contains the text **Prof**.

Field	Description



Adding another filter

You can add another filter by clicking on the filter icon for any of the columns. The picture opposite shows another filter added selecting table rows where the **Type** also contains the text **License**. The table will also be filtered accordingly.



Removing filters

You can remove filters by clicking on the filter close icon at the end of the filter.

Action Buttons

The following table describes the action buttons displayed on the **Agreements** page.

Button	Description
New Agreement	Creates a new agreement. See New Agreement page for more details.
Edit	This button is only enabled when there is a single selection in the **Agreements** table. Edits the selected agreement and opens the **Edit Agreement** page. SeeNew Agreement pagefor more details.
Publish	This button is enabled when there is at least one selection in the **Agreements** table. Publishes the selected agreements.

Field	Description
Clone	This button is only enabled when there is a single selection in the **Agreements** table. Clones the selected agreement and opens the Edit License or Edit Maintenance page, depending on the type of the selected agreement, with a clone of the details from the agreement. SeeNew Agreement pagefor more details.
Move to Draft	This button is enabled when there is at least one selection in the **Agreements** table. Moves the selected agreements to Draft.
Delete	This button is enabled when there is at least one selection in the **Agreements** table. Deletes the selected agreements.
Export	Exports all the agreements currently displayed in the **Agreements** table as a TSV file. This button takes the filters currently applied to the table into account, but not the sorting or the current selection.

10.6.5.1.3.1 New Agreement page

A description of the fields in each section of the **New Agreement** page. This also covers the **Edit Agreement** page.

An agreement entitlement type in AppClarity provides a structure to license and maintenance entitlements. Agreements can be used to model the contractual structure an organization uses for their purchasing process, or their internal software disbursement process.

The sections on the **New Agreement** or **Edit Agreement** page are:

The Summary panel

Basic Information

Particulars

Entitlement Term

Costs

Entitlement Links

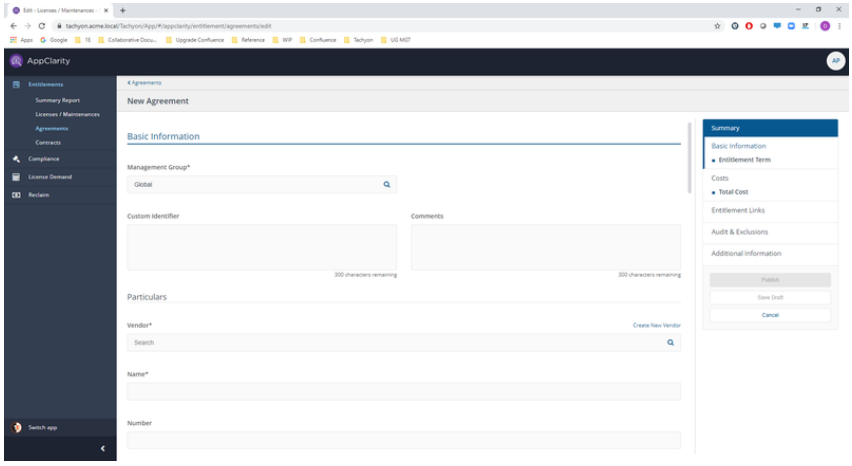
Parent

[Associations]

[Children]

[Audit & Exclusions]

[Additional information (Optional)]

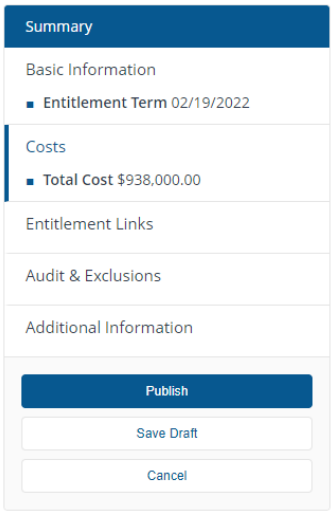


10.6.5.1.3.1.1 The Summary panel

The Summary panel on the right-hand side of the entitlement displays a summary of the settings that have been made in the entitlement so far. It's always visible on screen and can be used to navigate between the various sections of the entitlement.

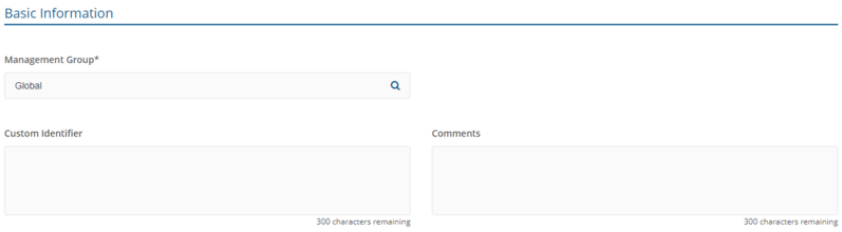
The panel also contains the following buttons:

Button	Description
Publish	Publishes the entitlement so it becomes active.
Save Draft	Saves the current settings in the entitlement to a draft. This can be used to save edits if you are part way through creating or making changes to the entitlement. It can also be used to inactivate an entitlement by removing its published status.
Cancel	Cancels the current edits and closes the page.



10.6.5.1.3.1.2 Basic Information

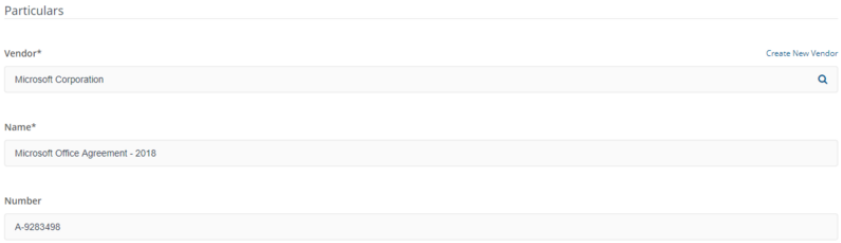
This section deals with the basic information for the entitlement, such as details of the product, the coverage and term of the entitlement.



Field	Details
Management Group*	Here you can associate the entitlement with Management Group of your choice.
Custom Identifier	An optional field. You can specify any alpha-numeric value to help identify the entitlement in the**Draft**and**Published**pages and when linking to other entitlements.
Comments	Enter text here to store any comments you have related to the entitlement.

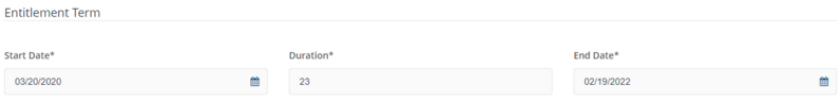
10.6.5.1.3.1.2.1 Particulars

This sub-section defines the basis of the agreement.



Field	Details
Vendor	The vendor portion of the vendor, title, version and edition attributes that are used to identify which software products the entitlement or agreement is for. For example, **Microsoft Corporation** or **1E**.In the **New Agreement** page this must be filled out before any other fields. Suggested suitable vendors that match your text are displayed as you type into the field, which you can select to auto-complete the entry.
Name	The name used for the agreement. For example, you might want to define an agreement that covers all your Microsoft Office and related products, so you could name the agreement**Microsoft Office Agreement - 2018**.
Number	Corresponds to the contract number, usually supplied on the customer contract.

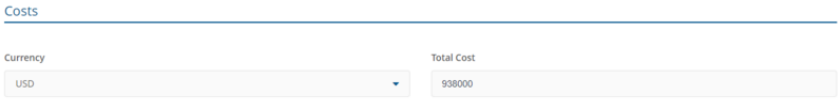
10.6.5.1.3.1.2.2 Entitlement Term



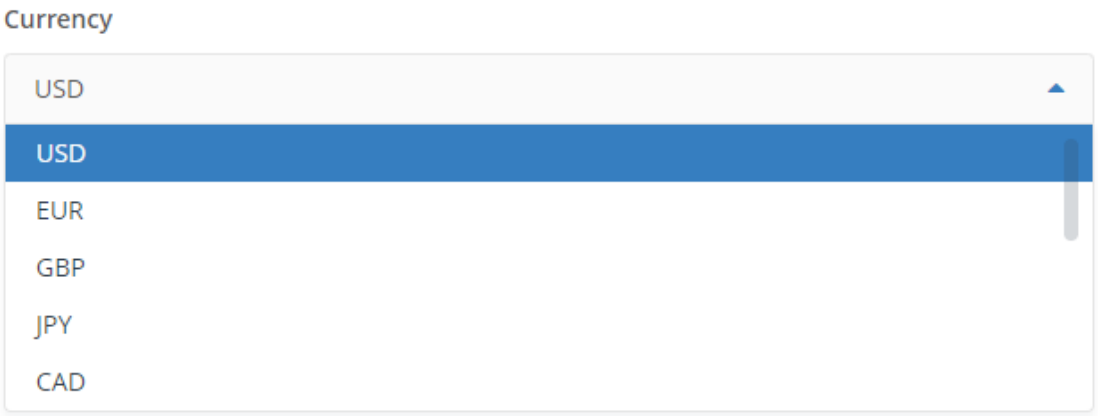
Field	Details
Start Date	When the agreement starts to be applicable.
Duration	How long in months the agreement is applicable for after the start date.Setting the **Duration** sets the **End Date**. Setting the **End Date** sets the **Duration**.
End Date	This is the last date the agreement is applicable until.Setting the **Duration** sets the **End Date**. Setting the **End Date** sets the **Duration**.

10.6.5.1.3.1.2.3 Costs

This section lets you control how the entitlement is costed and how it can be considered within the overall spend.



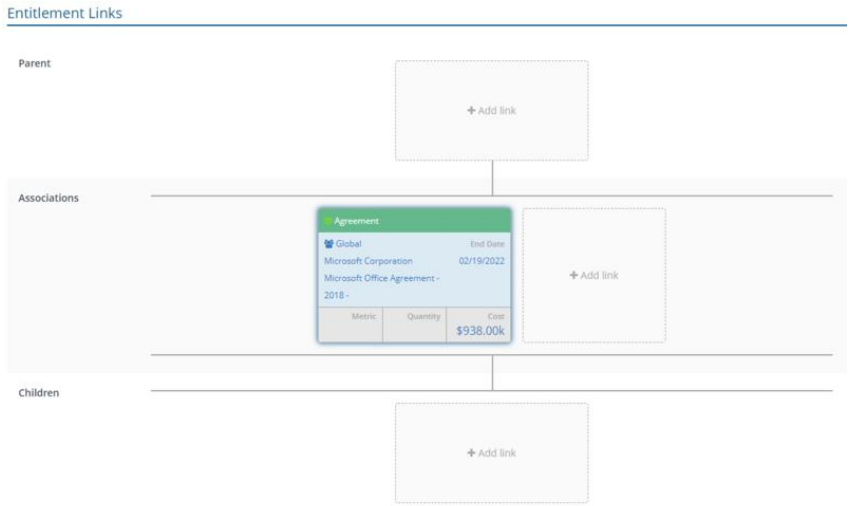
Field	Details
Currency	The currency applied to the entitlement. Clicking on the Currency field displays a list of currencies to choose from.
Total Cost	The cost of the agreement as arranged with the Vendor.Here you enter the total cost of the agreement corresponding with the currency field.



10.6.5.1.3.1.3 Entitlement Links

This section lets you create links between your entitlements. If you are creating a new entitlement this section will initially look like this:

After you have saved the entitlement this section provides an interface for linking it to other entitlements:

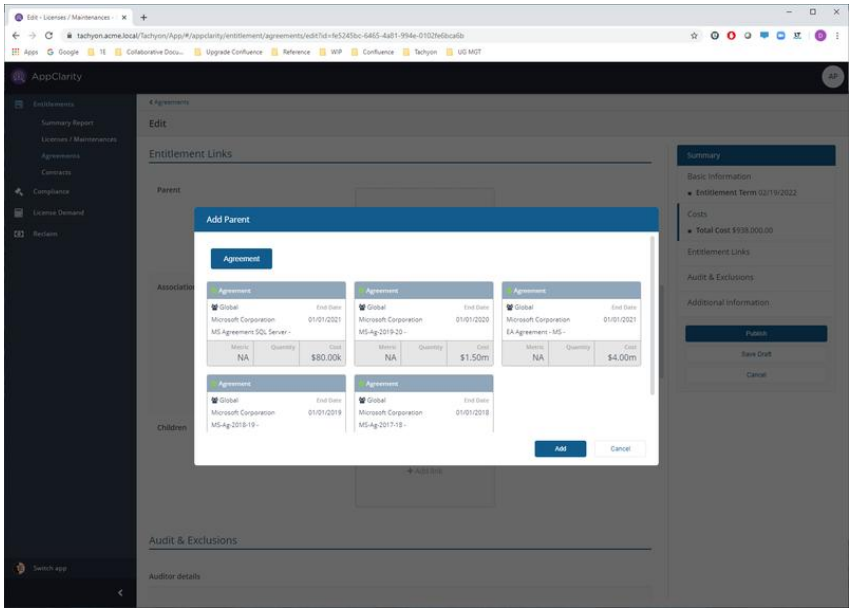


There are three sub-sections:

10.6.5.1.3.1.3.1 Parent

Here you can link parent agreements. Clicking on the **+Add link** area displays the **Add Parent** popup.

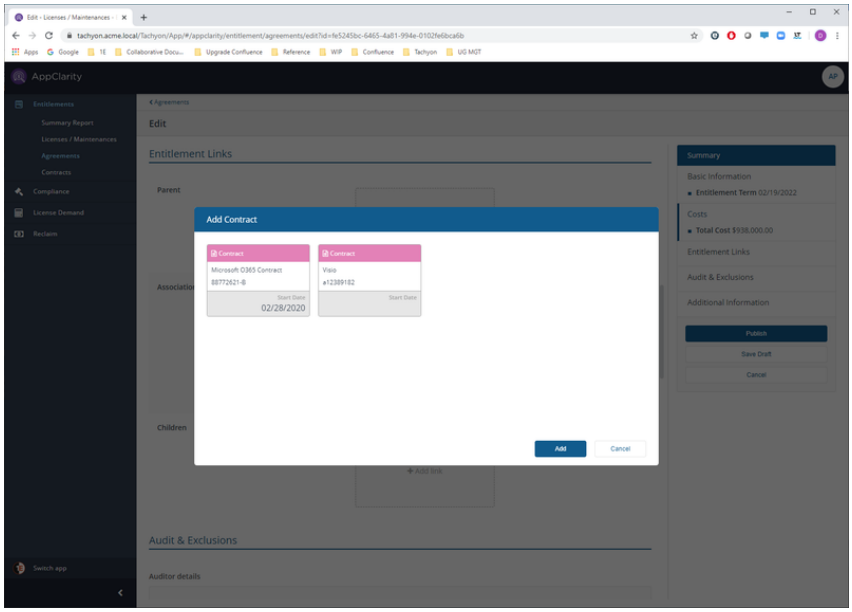
A list of agreement entitlements is displayed. Click on any of these and a green check mark will appear to indicate the selected parent, you can only select one. Once you've made your choice click the **Add** button to link the checked parent.



10.6.5.1.3.1.3.2 Associations

Here you can link contracts. Clicking on the **+Add link** area displays the **Add Contract** popup.

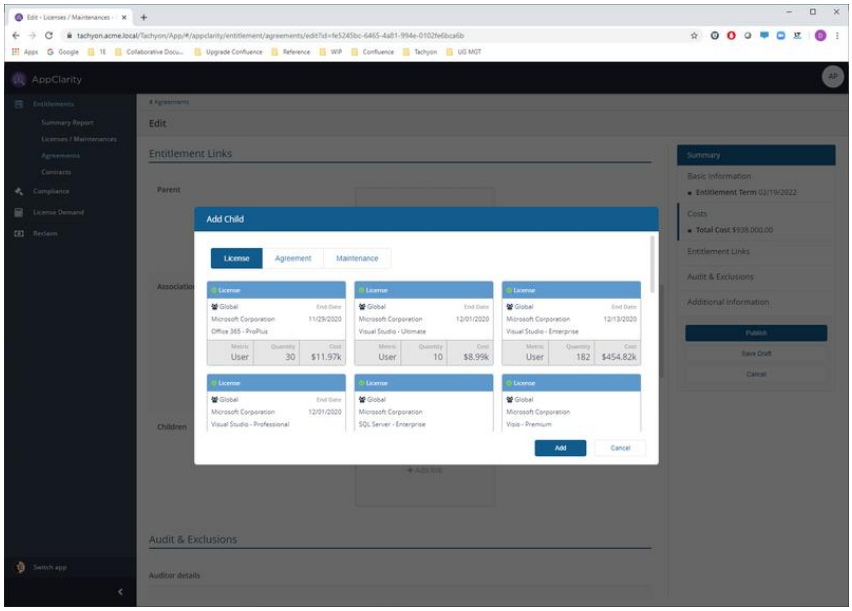
A list of contracts will be displayed. Click on any of these and a green check mark will appear to indicate the selected contract, you can select more than one contract to link. Once you've made your choice click the **Add** button to link the checked contract(s).



10.6.5.1.3.1.3.3 Children

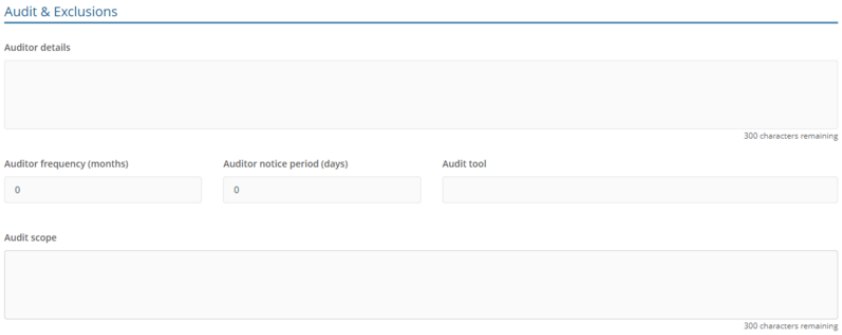
Here you can link child licenses, agreements or maintenances. Clicking on the **+Add link** area displays the **Add Child** popup.

Select **License**, **Agreement** or **Maintenance** to add that type of link, a list of entitlements of the selected type will be displayed. Click on any of these and a green check mark will appear to indicate the selected child - you can select more than one. Once you've made your choice click the **Add** button to link the checked children.



10.6.5.1.3.1.4 Audit & Exclusions

This section lets you control how the entitlement is audited.



Field	Details
Auditor Details	Organizations that are allowed to perform the audit including (if appropriate), the licensor organization and any third-party organizations, according to what was agreed in the contract.
Audit Clause	Provides additional information on what could trigger the audit.
Auditor Frequency	Definition of the highest agreed frequency of the audit expressed in months.
Auditor Notice period	Notice period in days.
Audit Tool	Name of the tool(s) which are approved for use in the audit.
Audit Scope	Defines what part of the software customer organization is allowed to be audited.

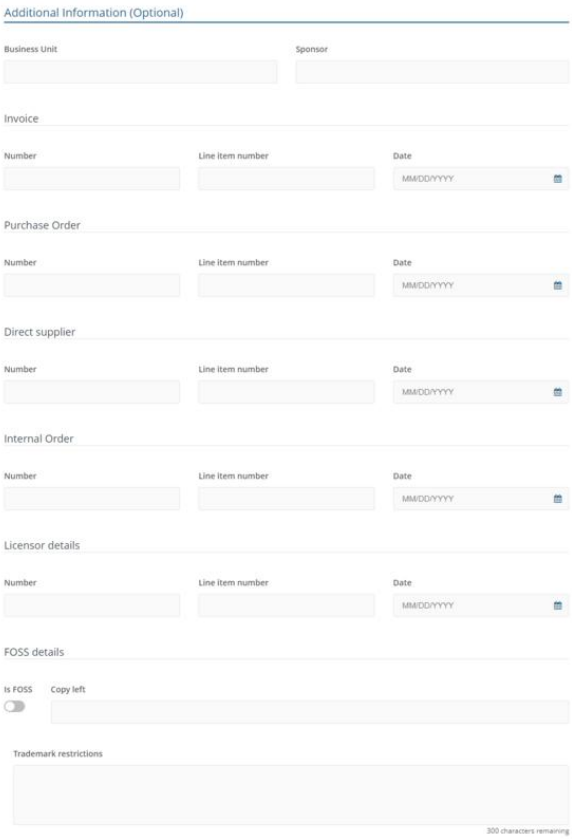
10.6.5.1.3.1.4.1 Additional information (Optional)

This section lets you enter additional information related to the entitlement that may come from a Vendor agreement or contract.

Sub-Section	Field	Field Details
	Business Unit	Specifies the Business Unit the agreement will be applied to. This may correspond to your management groups, depending on how you have those configured.

Sub-Section	Field	Field Details
Sponsor	Name of the person who manages the budget associated with an agreement (this field is likely to be used only on agreements, but could be extended to other entitlements)	
Invoice	Number	The invoice number, usually specified in the customer contract.
Line Item Number	This optionally identifies the line number (if provided) on the customer contract that pertains to the invoice.	
Date	The date for the invoice.	
Purchase Order	Number	The purchase order number, usually specified in the customer contract.
Line Item Number	This optionally identifies the line number (if provided) on the customer contract that pertains to the purchase order.	
Date	The date for the purchase order.	
Direct Supplier	Number	The number that identifies the direct supplier. For example, in some organizations this may be the same as the contract number.
Line Item Number	This optionally identifies the line number (if provided) on the contract that pertains to the direct supplier.	
Date	The date for the contract.	
Internal Order	Number	The ITARS or similar internal identifier for the order as

Sub-Section	Field	Field Details
		specified in the customer contract.
Line Item Number	This optionally identifies the line number(if provided)on the contract that pertains to the internal order.	
Date	The date for the contract.	
Licensor Details	Number	The number (or name) of the licensor, could be the vendor or a VAR.
Line Item Number	This is intended as a reference to a licensor source other than an invoice, e.g. to an on-line portal of license purchases.	
Date	The date for the contract.	
FOSS Details	IsFoss	This value is true only if the granted rights fulfill the requirements of both definition of the Free software maintained by the Free Software Foundation.
Copy Left	This value provides information on whether derivative works (which are always allowed for open source software) are themselves required to be open source software. There are three allowed values: “strong” means that all kinds of derivative works are required to be open source software themselves, “no” means that for all kinds of derivative works, it is allowed to distribute the derivative work as proprietary software. The intermediate value of “weak” means that there are some restrictions and the details are to be checked in the license.	
Trademark restrictions	FOSS trademark restrictions.	



10.6.5.1.4 Contracts page

A description of the fields on the **Contracts** page.

Here you can view, edit, and delete contracts. You can also export all the contracts in the selected repository to a TSV file. You get to this page by clicking the **AppClarity**→**Entitlements**→**Contracts** node in the navigation panel.

The fields on the **Contracts** page are:

Report Refresh

Contracts table

Name

Number

Start Date

Technical Resource

Resource

Links

...

Column actions

Column sort

Column filter

Column Picker

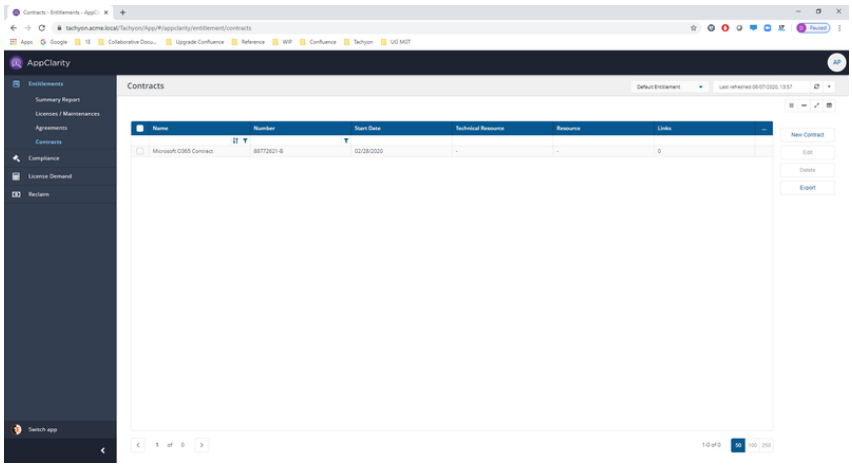
Action Buttons

New Contract

Edit

Delete

Export



Field	Description
Report Refresh	You can refresh reports from individual AppClarity screens as well as using the Settings App. Where this is available you can do this by using the refresh icon next to the **Last Refreshed** box:
Contracts table	The following table describes the columns displayed in the **Contracts** table:

Column	Description
Name	The vendor portion of the vendor, title, version and edition attributes that are used to identify which software products the entitlement or agreement is for. For example, **Microsoft Corporation** or **1E**. You can sort and filter on this column.

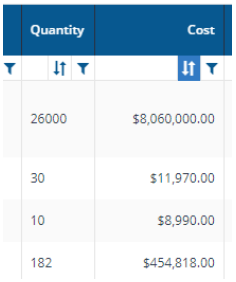
Field	Description
Number	An alpha-numeric string that identifies the contract. For example: **8877621-B** could be used to identify a particular contract, perhaps taken from a paper or emailed copy of the contract. You can filter on this column.
Start Date	The date when the contracts starts.
Technical Resource	The name of the person who knows the technical details behind licensing, or product information for an agreement (optional) This would likely be used only on agreements, but could be extended to individual entitlements.
Resource	Name of the person who manages the agreement This would likely be used only on agreements, but could be extended to individual entitlements.
Links	Identifies the number of times the contract has been linked to from other entitlements or agreements.
...	

Column actions

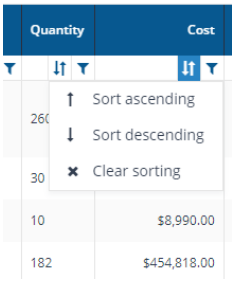
The following column actions are available on some columns in the table.

Column action	Description
Column sort	**Using column sorts** The picture opposite shows an example taken from AppClarity. In our example we want to sort the table on the **Cost** column from the highest cost at the top to the lowest at the bottom. To sort the table on the **Cost** column: Click on the sort icon ⇅ just beneath the header row in the **Cost** column.

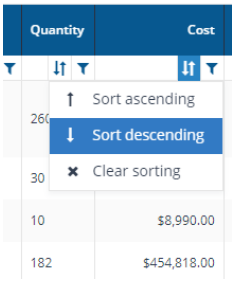
Field	Description



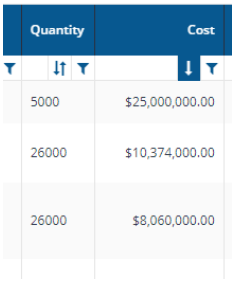
The sort popup is displayed.



Now select the sort direction. In our example this will be **Sort descending**.

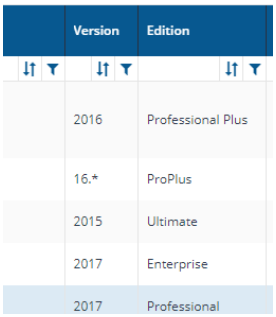


After selecting this the data in the table is now sorted on the **Cost** column from highest to lowest and the sort icon has changed to a sort descending icon



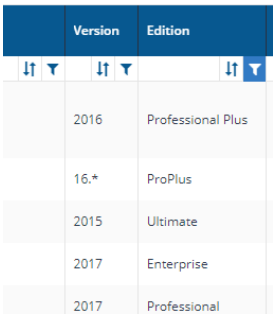
Clearing the sort

Field	Description
	You can clear the sort by clicking on the sort icon again and selecting the **Clear sorting** menu item from the sorting popup.
Column filter	**Using column filters** The picture opposite shows an example taken from AppClarity. In our example we want to filter the table to show only those items where the **Edition** contains the text **Prof**.

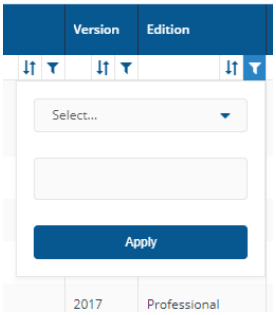


To filter the table on the **Edition** column:

Click on the filter icon just beneath the header row in the **Edition** column.

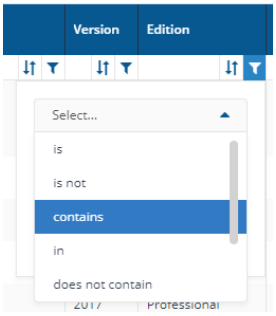


The filter popup is displayed.

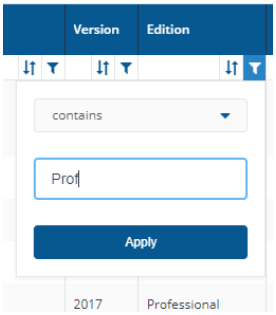


Now select the operator. In our example this will be **contains**.

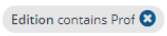
Field	Description



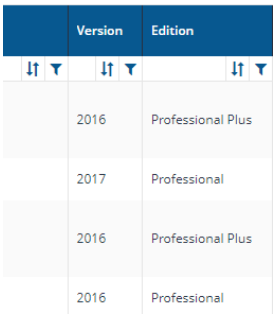
Then type the text **Prof** into the text field.



Click **Apply** and a new filter will be added to the table.

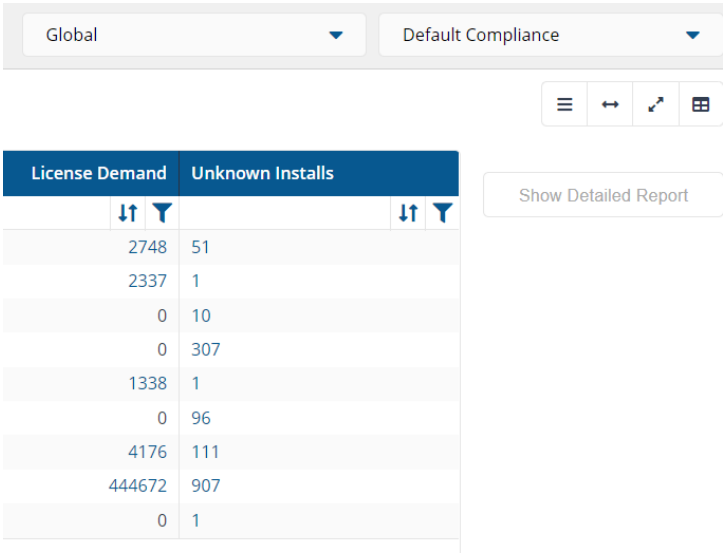


The table will be filtered to just those items whose **Edition** contains the text **Prof**.

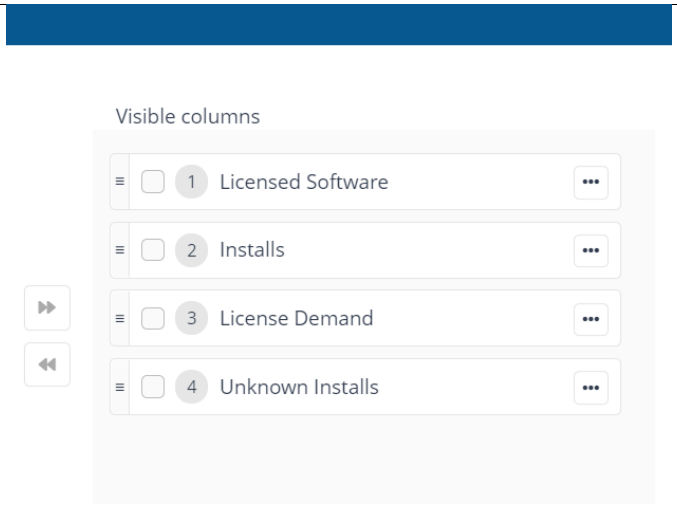


Adding another filter

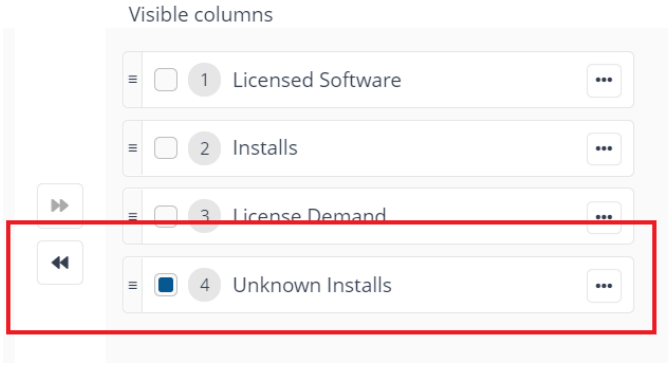
You can add another filter by clicking on the filter icon for any of the columns. The picture opposite shows another filter added selecting table rows where the **Type** also contains the text **License**. The table will also be filtered accordingly.

Field	Description
	Removing filters You can remove filters by clicking on the filter close icon at the end of the filter.
Column Picker	Where the column picker control is shown you can choose which columns are displayed. In the following example on the **Microsoft Core License Demand** page we hide the **Unknown Installs** column and move the **License Demand** column to the left of the page.  To pick the displayed columns: Click on the Choose columns icon o the right of the header row to view the visable columns.

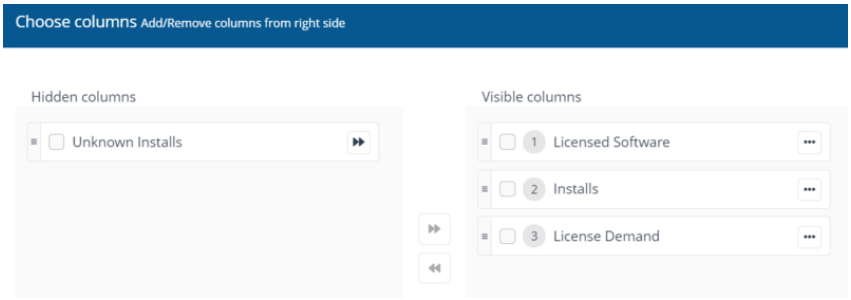
Field	Description



To exclude **Unknown Installs**, select the Unknown Installs row and click **Exclude columns** button.

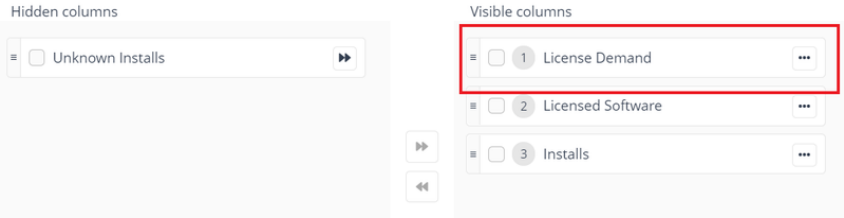


The **Unknown Installs** column is now hidden.



To move the **License Demand** column to the top of the list, hover your mouse over **License Demand** and using the direction control drag it to the top of the list.

Field	Description



The Microsoft Core License Demand page has now been automatically updated with our changes.

License Demand	Licensed Software	Installs
2748	Windows Server DataCenter	647
2337	SQL Server Enterprise	649
0	SQL Server Analysis Services	0
0	SQL Server Integration Services	0
1338	SQL Server Standard	300
0	SQL Server Reporting Services	0
4176	Windows Server Enterprise	265
444672	Windows Server Standard	4019
0	SQL Server Data Quality Services	0

Action Buttons

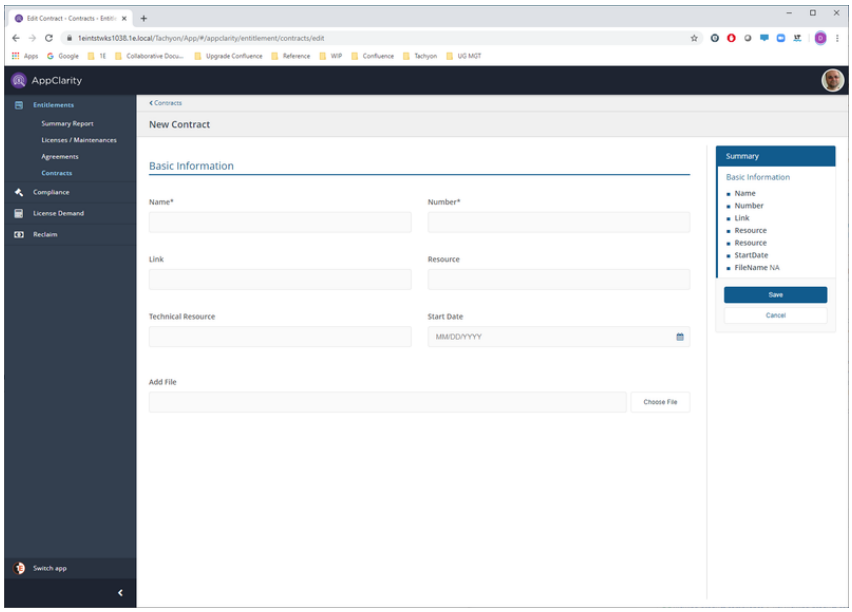
The following table describes the action buttons displayed on the **Contracts** page.

Button	Description
New Contract	Creates a new contract. Please refer to New Contract page for more details.
Edit	This button is only enabled when there is a single selection in the **Contracts** table. Edits the selected contract and opens the **Edit Contract** page. Please refer to New Contract page for more details.
Delete	This button is enabled when there is at least one selection in the **Contracts** table. Deletes the selected contracts.
Export	Exports all the contracts currently displayed in the **Contracts** table as a TSV file. This button takes the filters currently applied to the table into account, but not the sorting or the current selection.

10.6.5.1.4.1 New Contract page

A description of the fields on the**Create Contract**page. This also covers the **Edit Contract** page.

A contract entitlement type in AppClarity represents the evidence or proof that the license exists and is genuine. It is an artifact that can be virtually anything - it may be a scan of the signed contract for an enterprise agreement, for example, or it could be a PDF of the use rights for the software. Essentially the contract is where you will link file details that describe the specifics of an agreement.



10.6.5.1.4.1.1 The Summary panel

The Summary panel on the right-hand side displays a summary of the settings that have been made in the contract so far.

The panel also contains the following buttons:

Button	Description
Save	Saves the contract so it becomes available for linking to entitlements.
Cancel	Cancels the current edits and closes the page.

10.6.5.1.4.1.2 Basic Information

The following fields are available on the **New Contract** page.

Field	Details
Name	Name of the contract. For example: **Microsoft O365 Contract**.
Number	An alpha-numeric string that identifies the contract. For example: **8877621-B** could be used to identify a particular contract, perhaps taken from a paper or

Field	Details
	emailed copy of the contract.You should ensure that the combination of the **Name** and **Number** is unique.
Link	A link to an online contract.
Resource	Name of the person who manages the agreement This would likely be used only on agreements, but could be extended to individual entitlements.
Technical Resource	The name of the person who knows the technical details behind licensing, or product information for an agreement (optional) This would likely be used only on agreements, but could be extended to individual entitlements.
Start Date	The date when the contracts starts.You can select the date using the date picker.
Add File	The file attachment. This field displays the attachment after it has been selected using the **Choose File** button.
Choose File	Clicking this button displays a file **Open** dialog where you can browse to find any attachment that you want to add to the contract.

10.6.5.2 Compliance

A reference for the fields and tables on the pages under the **Compliance** node in the **AppClarity** section of the SLA Platform.

10.6.5.2.1 License Summary page

A description of the fields on the **License Summary** page.

Here you can view your License Summary. You get to this page by clicking the **AppClarity→Compliance→License Summary** node in the navigation panel.

The fields on the **License Summary** page are:

Management group selector

Compliance repository selector

Report Refresh

Column Picker

Action Buttons

Add License

Add Reclaim Policy

[Export](#)

[License Summary table](#)

[Vendor](#)

[Title](#)

[Total Installs](#)

[Total Devices](#)

[Total Users](#)

[Compliance Category](#)

[Unknown Installs](#)

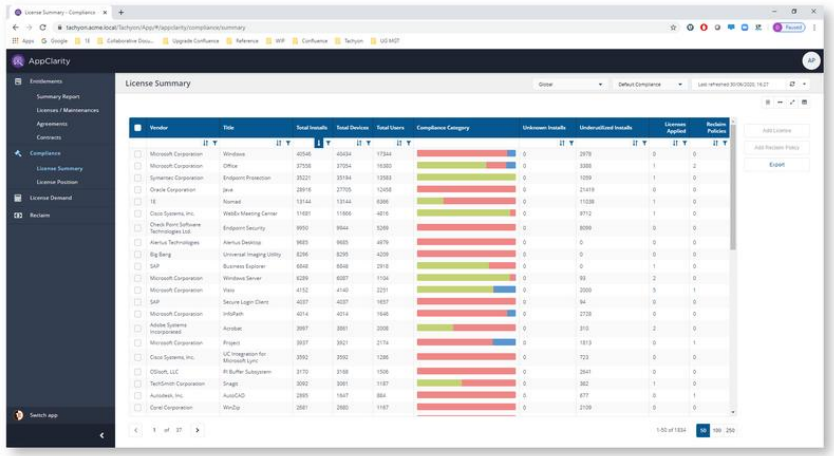
[Underutilized Installs](#)

[Licenses Applied](#)

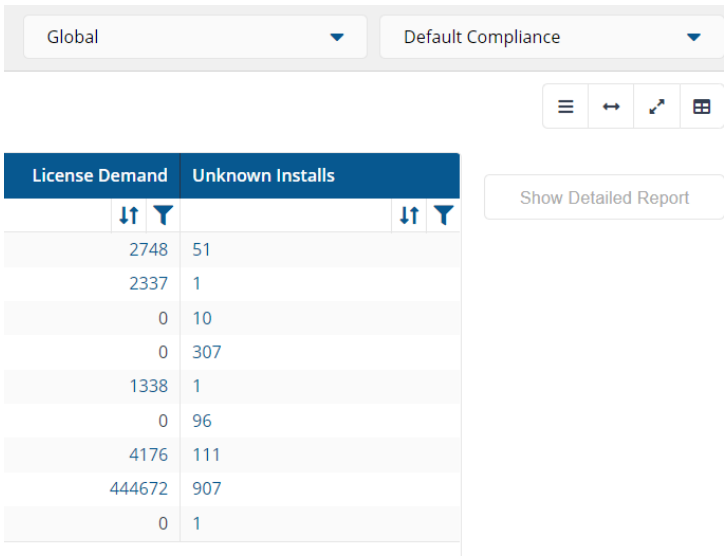
[Reclaim Policies](#)

[Column sort](#)

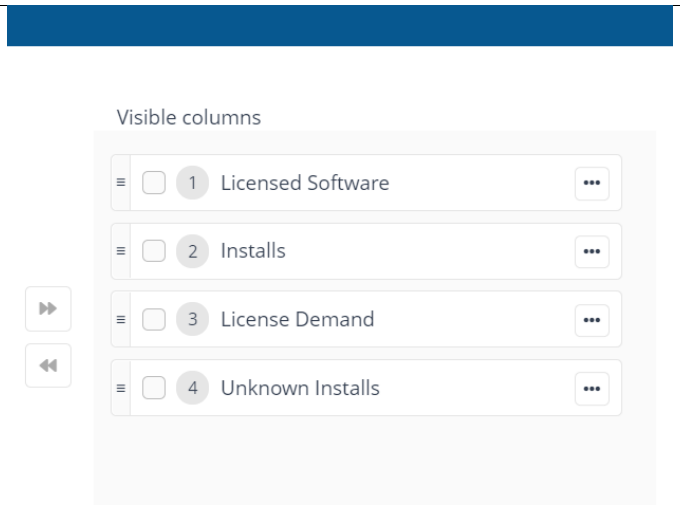
[Column filter](#)



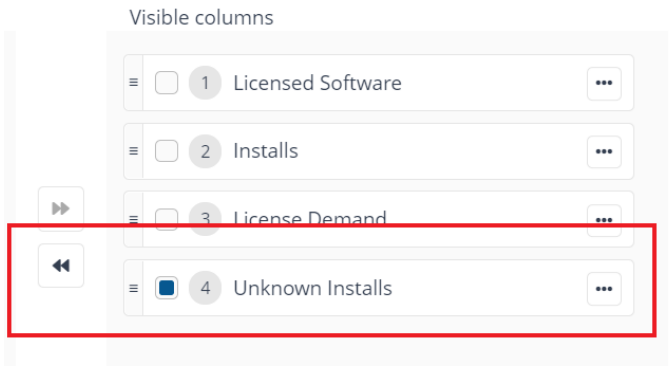
Field	Description
Management group selector	Certain pages in AppClarity have a management groups selector. This drop-down lets you select the management group you are interested in. By default this is set to **Global**.
Compliance repository selector	This field lets you select the repository where the compliance data displayed on the page comes from. By default this is set to **Default Compliance**.

Field	Description
	If you have created your own compliance repositories, click on the name to select these from the drop-down list.
Report Refresh	You can refresh reports from individual AppClarity screens as well as using the Settings App. Where this is available you can do this by using the refresh icon next to the **Last Refreshed** box:
Column Picker	Where the column picker control is shown you can choose which columns are displayed. In the following example on the **Microsoft Core License Demand** page we hide the **Unknown Installs** column and move the **License Demand** column to the left of the page.  To pick the displayed columns: Click on the Choose columns icon to the right of the header row to view the visible columns.

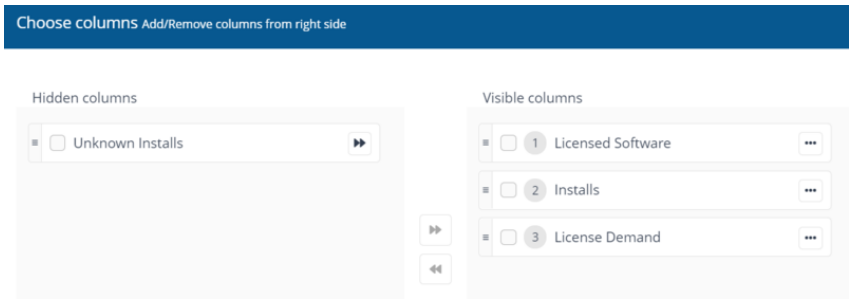
Field	Description



To exclude **Unknown Installs**, select the Unknown Installs row and click **Exclude columns** button.

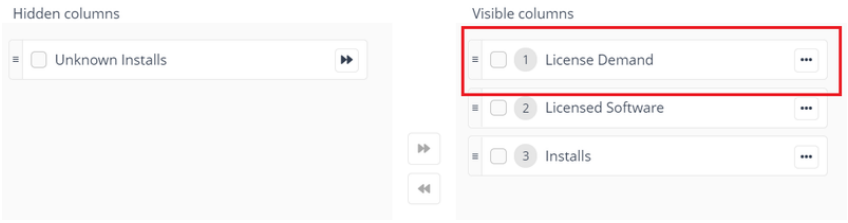


The **Unknown Installs** column is now hidden.



To move the **License Demand** column to the top of the list, hover your mouse over **License Demand** and using the direction control drag it to the top of the list.

Field	Description



The Microsoft Core License Demand page has now been automatically updated with our changes.

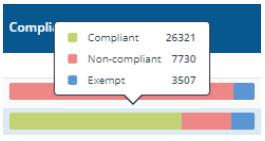
License Demand	Licensed Software	Installs
2748	Windows Server DataCenter	647
2337	SQL Server Enterprise	649
0	SQL Server Analysis Services	0
0	SQL Server Integration Services	0
1338	SQL Server Standard	300
0	SQL Server Reporting Services	0
4176	Windows Server Enterprise	265
444672	Windows Server Standard	4019
0	SQL Server Data Quality Services	0

Action Buttons

The following table describes the action buttons displayed on the **License Summary** page:

Button	Description
Add License	This button is only enabled when there is a single selection in the **License Summary** table. Creates a new license for the selected product and opens the New License page with the details of the product pre-filled. Please refer to New License page for more details.
Add Reclaim Policy	This button is only enabled when there is a single selection in the **License Summary** table. Creates a new reclaim policy for the selected product and opens the New Policy page with the details of the product pre-filled. Please refer to <New Policy page placeholder> for more details.
Export	Exports all the entitlements currently displayed in the **License Summary** table as a TSV file. This button takes the filters currently applied to the table into account, but not the sorting or the current selection.

Field	Description
License Summary table	The following table describes the columns displayed in the **License Summary** table:

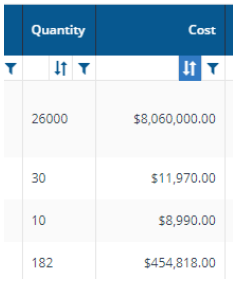
Column	Description
Vendor	The vendor portion of the vendor, title, version and edition attributes that are used to identify software products. For example, **Microsoft Corporation** or **1E**.
Title	The title portion of the vendor, title, version and edition attributes that are used to identify software products. For example, **Visio** or **Nomad**.
Total Installs	This column provides a total count of the installations for the product. This may be different from the **Total Devices** column as some software, such as Microsoft SQL Server, may be installed more than once on a device.
Total Devices	This column provides a total count of the devices where the product is installed. This may be different from the **Total Installs** column as some software may be installed more than once on a device.
Total Users	This column provides the total users accessing the software across all these devices.
Compliance Category	This column displays a compliance status bar for each product.  This bar displays a summary of the compliance status for the product installations in the selected compliance repository, taking into account any entitlements you have added. Hovering over the bar displays a summary of the compliance breakdown for the product. This is divided into **Compliant**, **Non-compliant** and **Exempt** installations.

Field	Description
	Clicking on the bar displays the Summary by Installs page for the selected product.
Unknown Installs	This column provides a count of the installations for the product where there are details that are unknown, thereby implying a risk for compliance calculation.
Underutilized Installs	This column provides a count of the installations for the product where the product is rarely used or unused.
Licenses Applied	This column provides a count of the licenses that have been applied to the product. If this number is greater than zero it becomes a link to the Licenses / Maintenances page filtered to show the applied licenses.
Reclaim Policies	This column provides a count of the reclaim policies that have been associated with the product. If this number is greater than zero it becomes a link to the filtered to show the associated reclaim policies.

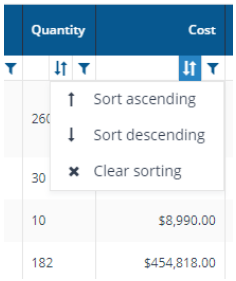
The following column actions are available on some table columns.

Column actions	Description
Column sort	**Using column sorts** The picture opposite shows an example taken from AppClarity. In our example we want to sort the table on the **Cost** column from the highest cost at the top to the lowest at the bottom. To sort the table on the **Cost** column: Click on the sort icon ⇅ just beneath the header row in the **Cost** column.

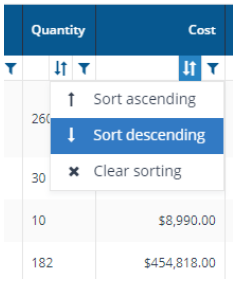
Field	Description



The sort popup is displayed.



Now select the sort direction. In our example this will be **Sort descending**.



After selecting this the data in the table is now sorted on the **Cost** column from highest to lowest and the sort icon has changed to a sort descending icon

.

Field	Description

Quantity	Cost
5000	$25,000,000.00
26000	$10,374,000.00
26000	$8,060,000.00

Clearing the sort

You can clear the sort by clicking on the sort icon again and selecting the **Clear sorting** menu item from the sorting popup.

Column filter

Using column filters

The picture opposite shows an example taken from AppClarity. In our example we want to filter the table to show only those items where the **Edition** contains the text **Prof**.

Version	Edition
2016	Professional Plus
16.*	ProPlus
2015	Ultimate
2017	Enterprise
2017	Professional

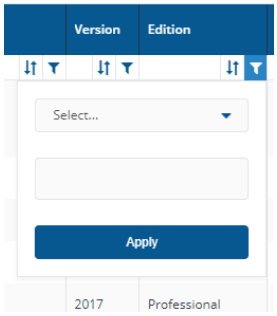
To filter the table on the **Edition** column:

Click on the filter icon just beneath the header row in the **Edition** column.

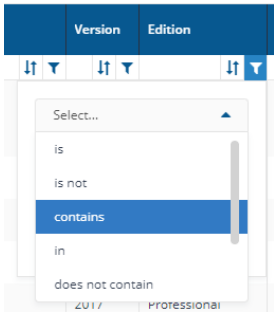
Version	Edition
2016	Professional Plus
16.*	ProPlus
2015	Ultimate
2017	Enterprise
2017	Professional

The filter popup is displayed.

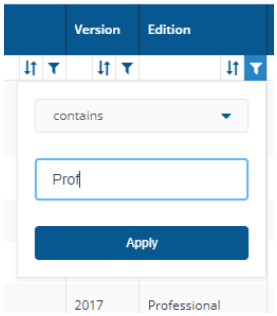
Field	Description



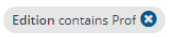
Now select the operator. In our example this will be **contains**.



Then type the text **Prof** into the text field.

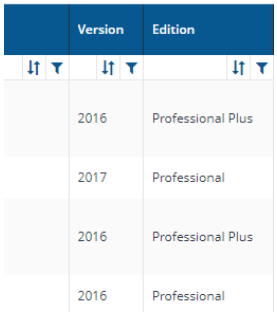


Click **Apply** and a new filter will be added to the table.



The table will be filtered to just those items whose **Edition** contains the text **Prof**.

Field	Description



Adding another filter

You can add another filter by clicking on the filter icon for any of the columns. The picture opposite shows another filter added selecting table rows where the **Type** also contains the text **License**. The table will also be filtered accordingly.

Removing filters

You can remove filters by clicking on the filter close icon at the end of the filter.

10.6.5.2.1.1 Summary by Installs page

A description of the fields on the **Summary by Installs** page.

Here you can view summary and detailed information for the installations of a selected product. You get to this page by clicking the Compliance Category bar for a product on the License Summary page.

The fields on the **Summary by Installs** page are:

Management Group Selector

Repository Selector

Report Refresh

Edition Table

Edition

Compliant

Non-Compliant

Exempted

Unknown

Device Summary Table

Licensed Software

Licensed Version

Total License Available

Total Consumed

Effective License Position

Device Detailed Table

Machine Name

Management Group

Primary User

Canonical Version

Edition

Licensed Software

License Demand

License Consumed

Status

Comments

Export

Entitlement Summary Table

License Vendor

License Title

License Edition

License Metric

Management Group

Total License Units

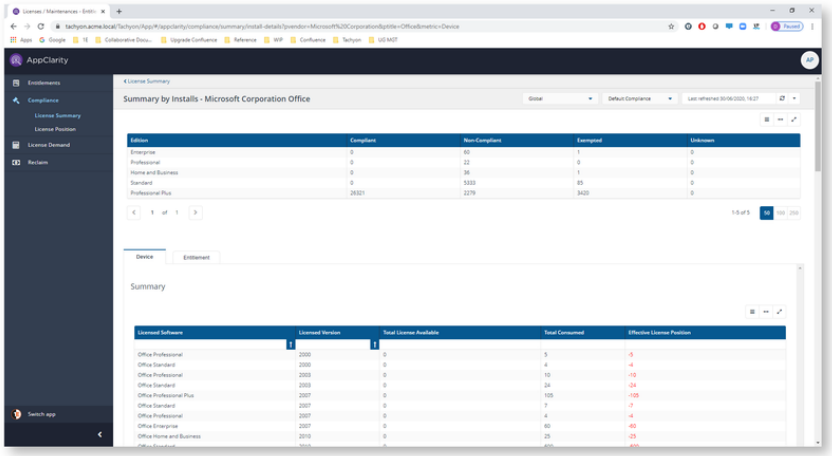
Consumed

Remaining

Column Actions

Column sort

Column filter



Field	Description
Management Group Selector	Certain pages in AppClarity have a management groups selector. This drop-down lets you select the management group you are interested in. By default this is set to **Global**.
Repository Selector	This field lets you select the repository where the compliance data displayed on the page comes from. By default this is set to **Default Compliance**. If you have created your own compliance repositories, click on the name to select these from the drop-down list.
Report Refresh	You can refresh reports from individual AppClarity screens as well as using the Settings App. Where this is available you can do this by using the refresh icon next to the **Last Refreshed** box:
Edition Table	The following table shows the column headings in the **Edition** table:

Column	Description
Edition	The edition portion of the vendor, title, version and edition attributes that are used to identify which software product the compliance status relates to.
Compliant	This column provides a count of the compliant installations for the product. When the number is not zero this is a link to a list of devices where the product is installed.

Field	Description	
	Non-Compliant	This column provides a count of the non-compliant installations for the product.
	Exempted	This column provides a count of the exempted installations that are associated with an exemption management group. Please refer to Excluding devices from License Demand Calculation using Management Groups for more details.
	Unknown	This column provides a count of the installations for the product where there are details that are unknown, thereby implying a risk for compliance calculation.

Device Summary Table

The following table shows the column headings in the **Device Summary** table:

Column	Description
Licensed Software	The title portion of the vendor, title, version and edition attributes that are used to identify software products. For example, **Visio** or **Nomad**. You can sort on this column.
Licensed Version	The version portion of the vendor, title, version and edition attributes that are used to identify software products. For example, **11.0.3216.5614** or **6.3.100.0**. You can sort on this column.
Total License Available	Shows the total number of licenses available for this product from all the entitlements related to it.
Total Consumed	Shows the number of licenses consumed by installations from the total available for this product.
Effective License Position	The effective license position is a calculation of the entitlements for a particular software product against the installations for that product. It may be one of: a negative number, in which case there are more installations for that software product than entitlements zero where the numbers match exactly

Field	Description
	a positive number, which indicates you have paid for more licenses than you are using. Your ideal is to get the numbers positive but as close to zero as fits in with your current and predicted demand.
Device Detailed Table	The following table shows the column headings in the **Detailed** table:

Column	Description
Machine Name	The device name where the software is installed. The name is a link that navigates to the **Device Summary** page for the selected device in the **Inventory** application. You can filter on this column.
Management Group	Displays the number of Management Groups a device is associated with. Clicking on the number displays a popup listing the Management Groups. You can filter on this column.
Primary User	This column displays the user name for the primary user on a device. You can filter on this column.
Canonical Version	The canonical representation of the productversion installed on a device. You can filter on this column.
Edition	The edition portion of the vendor, title, version and edition attributes that are used to identify software products. For example, **Standard** or **-** (where no edition exists). You can filter on this column.
Licensed Software	The title for the software installed on a device. You can filter on this column.
License Demand	The license demand for the software on the device where the software is installed. You can filter on this column.

Field	Description
	License Consumed — This column shows the number of available licenses consumed by the software on the device where it is installed. You can filter on this column.
	Status — This column displays an indicator for the current compliance status for the product. You can filter on this column.
	Comments — This column provides comments on how the entitlement is applied to the installation. Currently this indicates whether the installation has been exempted or not. You can filter on this column.

This table also has the following action buttons:

Button	Description
Export	Pages in AppClarity that include an **Export all** button allow you to export all the data for any tables of information displayed on the page. This may also include columns that are not currently visible in the table display.

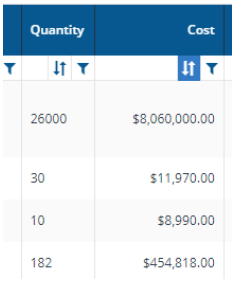
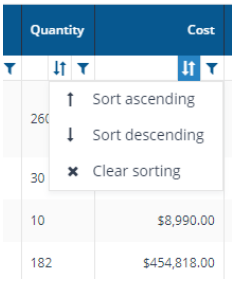
Entitlement Summary Table

The following table shows the column headings in the**Entitlement Summary**table:

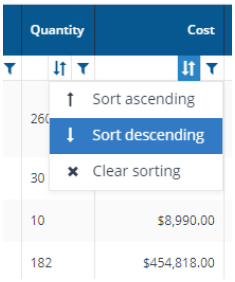
Column	Description
License Vendor	The vendor for the software as defined in the entitlement.
License Title	The title for the software as defined in the entitlement.
License Edition	The edition portion of the vendor, title, version and edition attributes that are used to identify software products. For example, **Standard** or **-** (where no edition exists).
License Metric	The metric type for a license or maintenance entitlement. This may be one of:

Field	Description		
		Type	Description
		Core	The metric for the license is related to the number of cores present on a device. For example, licenses for **Microsoft SQL database** are related to the number of cores on the server where **Microsoft SQL** is installed.
		Device	The metric for the license is for devices. For example licenses for **Microsoft Visio** are on a per device basis. This is the default type.
		Other	This can be used to reference your own license metric type.
		Processor	The metric for the license is related to the number of processors for a device. For example, licenses for certain **Oracle** products are related to the number of processors on the server where the **Oracle** product is installed.
		PVU	The metric for the license is related to the Processor Value Unit present on a device. For example. licenses for **IBM** products are related to the **Processor Value Unit (PVU)** for the device where the IBM product is installed.
		User	The metric for the license is related to the users for the product. For example, **Microsoft Office 365** licenses are related to users and not the devices the software is running on.
	Management Group	This column displays the names of the Management Groups an entitlement is associated with.	
	Total License Units	Shows the total number of licenses units available from an entitlement.	

Field	Description	
	Consumed	Shows the number of licenses consumed by installations from a particular entitlement.
	Remaining	Shows the number of licenses remaining for a particular entitlement after subtracting the **Consumed** licenses consumed from the **Total License Units**.
Column Actions	The following column actions are available on some table columns.	

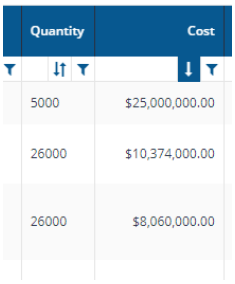
Column actions	Description
Column sort	**Using column sorts** The picture opposite shows an example taken from AppClarity. In our example we want to sort the table on the **Cost** column from the highest cost at the top to the lowest at the bottom.To sort the table on the **Cost** column: Click on the sort icon ⇅ just beneath the header row in the **Cost** column.  The sort popup is displayed.  Now select the sort direction. In our example this will be **Sort descending**.

Field	Description



After selecting this the data in the table is now sorted on the **Cost** column from highest to lowest and the sort icon has changed to a sort descending icon

.



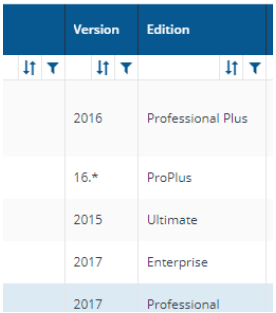
Clearing the sort

You can clear the sort by clicking on the sort icon again and selecting the **Clear sorting** menu item from the sorting popup.

Column filter

Using column filters

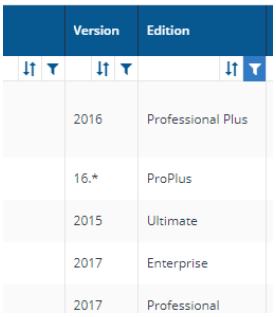
The picture opposite shows an example taken from AppClarity. In our example we want to filter the table to show only those items where the **Edition** contains the text **Prof**.



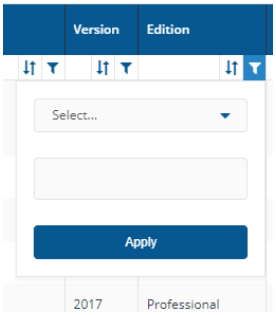
Field	Description

To filter the table on the **Edition** column:

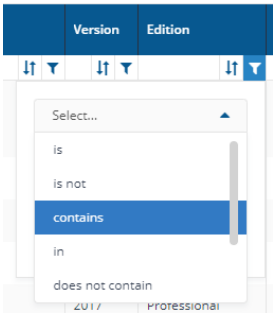
Click on the filter icon just beneath the header row in the **Edition** column.



The filter popup is displayed.

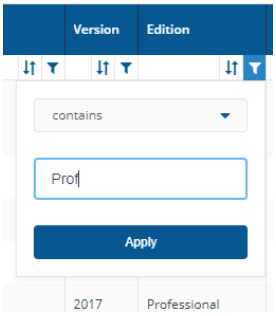


Now select the operator. In our example this will be **contains**.

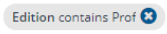


Then type the text **Prof** into the text field.

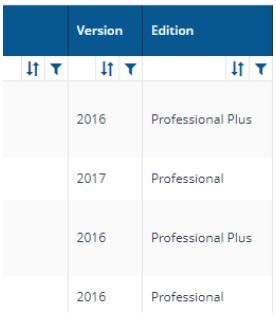
Field	Description



Click **Apply** and a new filter will be added to the table.

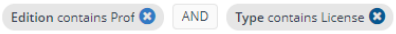


The table will be filtered to just those items whose **Edition** contains the text **Prof**.



Adding another filter

You can add another filter by clicking on the filter icon for any of the columns. The picture opposite shows another filter added selecting table rows where the **Type** also contains the text **License**. The table will also be filtered accordingly.



Removing filters

You can remove filters by clicking on the filter close icon at the end of the filter.

10.6.5.2.2 License Position page

A description of the fields on the **License Position** page.

Here you can view your License Summary. You get to this page by clicking the **AppClarity→Compliance→License Position** node in the navigation panel.

The fields on the **License Position** page are:

Management group

Compliance Repository

Report Refresh

Action buttons

Export

Compliance Details

License Position table

Vendor

Title

Canonical Version

Edition

Total Licensed Units

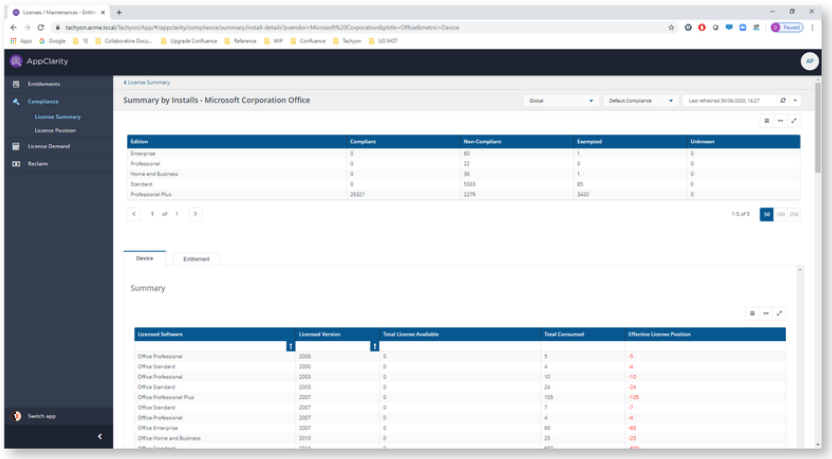
Total Units Consumed

License Position

Metric

Column sort

Column filter



Field	Description
Management group	Certain pages in AppClarity have a management groups selector. This drop-down lets you select the management group you are interested in. By default this is set to **Global**.
Compliance Repository	This field lets you select the repository where the compliance data displayed on the page comes from. By default this is set to **Default Compliance**. If you have created your own compliance repositories, click on the name to select these from the drop-down list.
Report Refresh	You can refresh reports from individual AppClarity screens as well as using the Settings App. Where this is available you can do this by using the refresh icon next to the **Last Refreshed** box:
Action buttons	The following table describes the action buttons displayed on the **License Position** page.

Button	Description
Export	Exports all the products currently displayed in the **License Position** table as a TSV file. This button takes the filters currently applied to the table into account, but not the sorting or the current selection.
Compliance Details	This button is only enabled when there is a single selection in the **License Position** table. Displays the License Summary page filtered to just display the information for the selected product.

License Position table

The following table describes the columns displayed in the **License Position** table:

Column	Description
Vendor	The vendor portion of the vendor, title, version and edition attributes that are used to identify software products. For example, **Microsoft Corporation** or **1E**.

Field	Description
Title	The title portion of the vendor, title, version and edition attributes that are used to identify software products. For example, **Visio** or **Nomad**.
Canonical Version	The canonical representation of the productversion installed on a device.
Edition	The edition portion of the vendor, title, version and edition attributes that are used to identify software products. For example, **Standard** or **-** (where no edition exists).
Total Licensed Units	Shows the total number of license units available from entitlements related to the product.
Total Units Consumed	Shows the total number of available license units that have been consumed by product installations.
License Position	Shows the license position for the product calculated by subtracting the value in the **Total Units Consumed** column from the value in the **Total Licensed Units** column. Negative numbers in red indicate a license deficit. Positive numbers in black indicates a license excess.
Metric	The metric type for a license or maintenance entitlement. This may be one of:

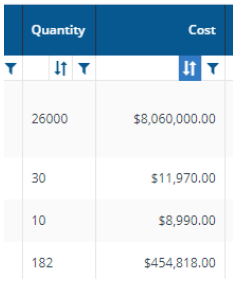
Type	Description
Core	The metric for the license is related to the number of cores present on a device. For example, licenses for **Microsoft SQL database** are related to the number of cores on the server where **Microsoft SQL** is installed.
Device	The metric for the license is for devices. For example licenses for **Microsoft Visio** are on a per device basis. This is the default type.

Field	Description	
	Other	This can be used to reference your own license metric type.
	Processor	The metric for the license is related to the number of processors for a device. For example, licenses for certain **Oracle** products are related to the number of processors on the server where the **Oracle** product is installed.
	PVU	The metric for the license is related to the Processor Value Unit present on a device. For example. licenses for **IBM** products are related to the **Processor Value Unit (PVU)** for the device where the IBM product is installed.
	User	The metric for the license is related to the users for the product. For example, **Microsoft Office 365** licenses are related to users and not the devices the software is running on.

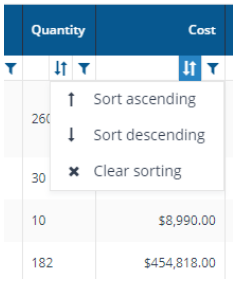
The following column actions are available on some table columns:

Column actions	Description
Column sort	**Using column sorts** The picture opposite shows an example taken from AppClarity. In our example we want to sort the table on the **Cost** column from the highest cost at the top to the lowest at the bottom.To sort the table on the **Cost** column: Click on the sort icon ↓↑ just beneath the header row in the **Cost** column.

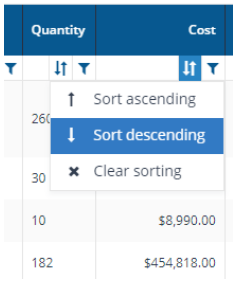
Field	Description



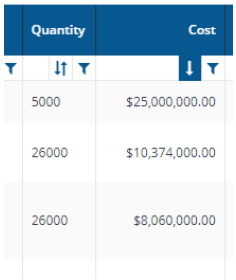
The sort popup is displayed.



Now select the sort direction. In our example this will be **Sort descending**.



After selecting this the data in the table is now sorted on the **Cost** column from highest to lowest and the sort icon has changed to a sort descending icon



Clearing the sort

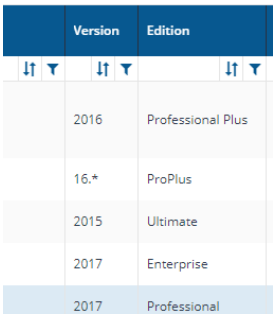
Field	Description

You can clear the sort by clicking on the sort icon again and selecting the **Clear sorting** menu item from the sorting popup.

Column filter

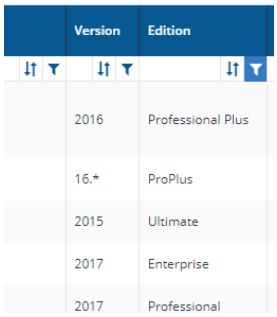
Using column filters

The picture opposite shows an example taken from AppClarity. In our example we want to filter the table to show only those items where the **Edition** contains the text **Prof**.

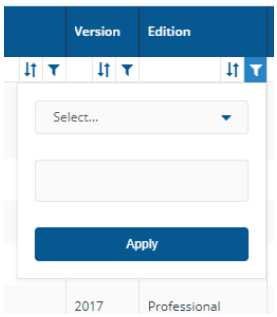


To filter the table on the **Edition** column:

Click on the filter icon just beneath the header row in the **Edition** column.

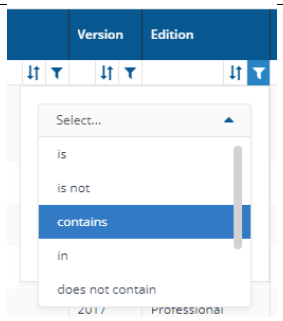


The filter popup is displayed.

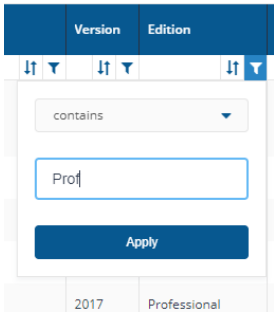


Now select the operator. In our example this will be **contains**.

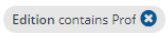
Field	Description



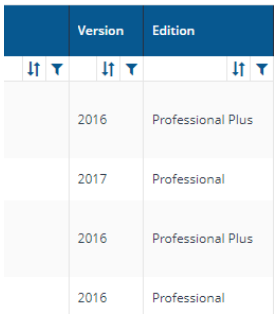
Then type the text **Prof** into the text field.



Click **Apply** and a new filter will be added to the table.



The table will be filtered to just those items whose **Edition** contains the text **Prof**.



Adding another filter

You can add another filter by clicking on the filter icon for any of the columns. The picture opposite shows another filter added selecting table rows where the **Type** also contains the text **License**. The table will also be filtered accordingly.

Field	Description
	Removing filters You can remove filters by clicking on the filter close icon at the end of the filter.

10.6.5.3 License Demand

A description of the fields on the **License Demand** page.

Here you can view the License Demand reports. You get to this page by clicking the **AppClarity→License Demand** node in the navigation panel.

The fields on the **License Demand** page are:

Management Group selector

Compliance Repository selector

Microsoft Core License Demand

Information

View Report

Refresh

IBM Processor Value Unit (PVU) License Demand

Information

View Report

Refresh

Oracle Processor License Demand

Information

View Report

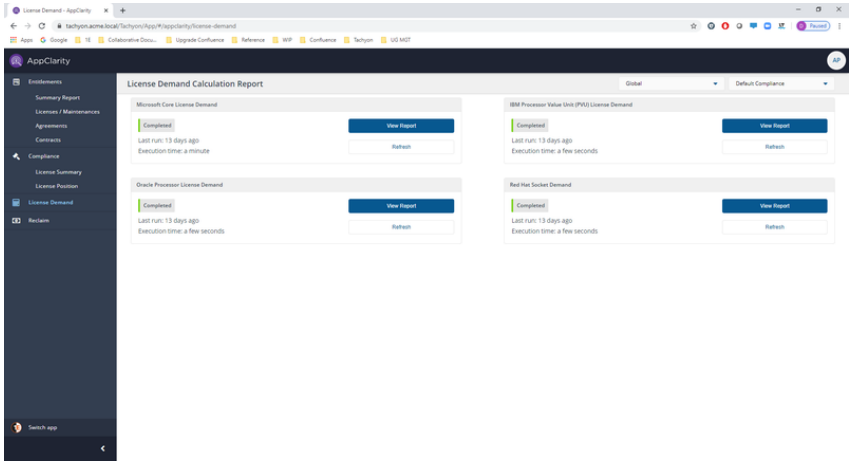
Refresh

Red Hat Socket Demand

Information

View Report

Refresh



Field	Description
Management Group selector	Certain pages in AppClarity have a management groups selector. This drop-down lets you select the management group you are interested in. By default this is set to **Global**.
Compliance Repository selector	This field lets you select the repository where the compliance data displayed on the page comes from. By default this is set to **Default Compliance**. If you have created your own compliance repositories, click on the name to select these from the drop-down list.
Microsoft Core License Demand	

Field	Description
Information	This section tells you if the report has been run, when it was last run and how long it took to run the report.
View Report	Clicking on this button displays the Microsoft Core License Demand page showing an overview of the data contained in the report.
Refresh	Clicking on this button runs the report.

IBM Processor Value Unit (PVU) License Demand

Field	Description
Information	This section tells you if the report has been run, when it was last run and how long it took to run the report.

Field	Description	
	View Report	Clicking on this button displays the IBM Processor Value Unit (PVU) License Demand page showing an overview of the data contained in the report.
	Refresh	Clicking on this button runs the report.
Oracle Processor License Demand	Field	Description
	Information	This section tells you if the report has been run, when it was last run and how long it took to run the report.
	View Report	Clicking on this button displays the Oracle Processor License Demand page showing an overview of the data contained in the report.
	Refresh	Clicking on this button runs the report.
Red Hat Socket Demand	Field	Description
	Information	This section tells you if the report has been run, when it was last run and how long it took to run the report.
	View Report	Clicking on this button displays the Red Hat Socket Demand page showing an overview of the data contained in the report.
	Refresh	Clicking on this button runs the report.

10.6.5.3.1 Microsoft Core License Demand page

A description of the fields on the **Microsoft Core License Demand** page.

This page provides an overview of the data in the **Microsoft Core License Demand** report. You get to this page by navigating to the **AppClarity→Licence Demand** node in the navigation panel and then clicking on the **View Report** button for the **Microsoft Core License Demand** report.

The fields on the **Microsoft Core License Demand** page are:

Management Group selector

Compliance Repository selector

[Report Refresh](#)

[Action buttons](#)

[Show Detailed Report](#)

[Column Picker](#)

[Microsoft Core License Demand table](#)

[Licensed Software](#)

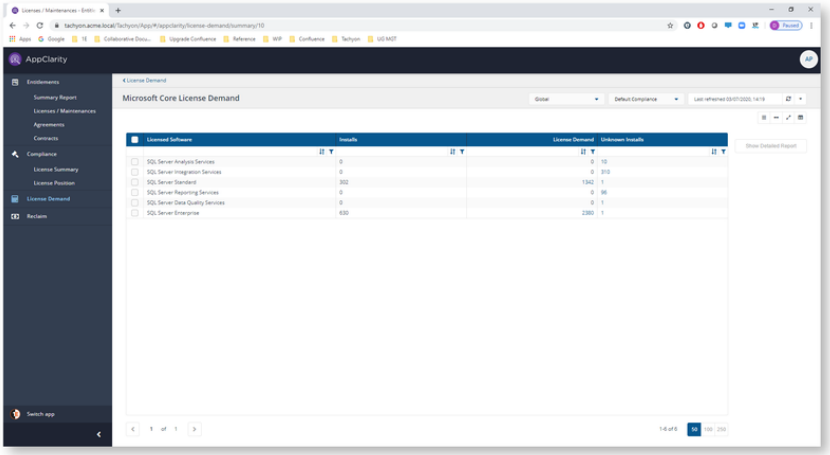
[Installs](#)

[License Demand](#)

[Unknown Installs](#)

[Column sort](#)

[Column filter](#)



Field	Description
Management Group selector	Certain pages in AppClarity have a management groups selector. This drop-down lets you select the management group you are interested in. By default this is set to **Global**.
Compliance Repository selector	This field lets you select the repository where the compliance data displayed on the page comes from. By default this is set to **Default Compliance**. If you have created your own compliance repositories, click on the name to select these from the drop-down list.

Field	Description
Report Refresh	You can refresh reports from individual AppClarity screens as well as using the Settings App. Where this is available you can do this by using the refresh icon next to the **Last Refreshed** box:
Action buttons	The following table describes the action buttons displayed on the **Microsoft Core License Demand** page: **Show Detailed Report**: This button is only enabled if there is a single selection in the **Microsoft Core License Demand** table. Clicking the button displays the Microsoft Core License Demand - Detailed Report page for the selected item.
Column Picker	**Using column picker**Where the column picker control is shown you can choose which columns are displayed. In the following example on the **Microsoft Core License Demand** page we hide the **Unknown Installs** column and move the **License Demand** column to the left of the page.To pick the displayed columns:Click on the Choose columns iconto the right of the header row to view the visible columns.To exclude **Unknown Installs**, select the Unknown Installs row and click **Exclude columns** button.The **Unknown Installs** column is now hidden.To move the **License Demand** column to the top of the list, hover your mouse over **License Demand** and using the direction control drag it to the top of the list.The Microsoft Core License Demand page has now been automatically updated with our changes.
Microsoft Core License Demand table	The following table describes the columns displayed in the **Microsoft Core License Demand** table: **Licensed Software**: Displays software titles that are part of the License Demand report, where that software also has installations present in the inventory. **Installs**: This column shows the number of installs for the software titles that are part of the License Demand report.

Field	Description
License Demand	This column shows the license demand for the software titles that are part of the License Demand report.
Unknown Installs	This column provides a count of the installations for the software titles that are part of the License Demand report where there are details that are unknown, thereby implying a risk for compliance calculation.

The following column actions are available on some table columns:

Column actions	Description
Column sort	Some tables contain column sorts that let you easily re-order the information displayed in the table.**Using column sorts**The picture opposite shows an example taken from AppClarity. In our example we want to sort the table on the **Cost** column from the highest cost at the top to the lowest at the bottom. To sort the table on the **Cost** column:Click on the sort iconjust beneath the header row in the **Cost** column.The sort popup is displayed.Now select the sort direction. In our example this will be **Sort descending**.After selecting this the data in the table is now sorted on the **Cost** column from highest to lowest and the sort icon has changed to a sort descending icon**Clearing the sort**You can clear the sort by clicking on the sort icon again and selecting the **Clear sorting** menu item from the sorting popup.
Column filter	Some tables contain a column filter that lets you easily filter the information displayed in the table.**Using column filters**The picture opposite shows an example taken from AppClarity. In our example we want to filter the table to show only those items where the **Edition** contains the text **Prof**.To filter the table on the **Edition** column:Click on the filter iconjust beneath the header row in the **Edition** column.The filter popup is displayed.Now select the operator. In our example this will be **contains**.Then type the text **Prof** into the text field.Click **Apply** and a new filter will be added to the table.The table will be filtered to just those items whose **Edition** contains the text **Prof**.**Adding another filter**You can add another filter by clicking on the filter icon for any of the columns. The picture opposite shows another filter added selecting table rows where the **Type** also contains the text **License**. The table will also be filtered

Field	Description
	accordingly.**Removing filters**You can remove filters by clicking on the filter close icon at the end of the filter.

10.6.5.3.1.1 Microsoft Core License Demand - Detailed Report page

A description of the fields on the **Microsoft Core License Demand - Detailed Report** page.

This page displays the data for a selected software title on the **Microsoft Core License Demand** page. You get to this page by navigating to the **AppClarity→Licence Demand** node in the navigation panel, selecting a row in the table and then clicking on the **Show Detailed Report** button.

The fields on the **Microsoft Core License Demand - Detailed Report** page are:

Management Group selector

Compliance Repository selector

Report Refresh

Column Picker

Action buttons

Export

Microsoft Core License Demand - Summary table

Licensed Software

Installs

License Demand

Unknown Installs

Microsoft Core License Demand - Detailed Report table

Cluster Name

Physical Host

Machine Name

Machine Type

Version

Colloquial Version

Licensed Software

Installs

License Demand

[Management Group]

[Classification]

[Sockets]

[Processors]

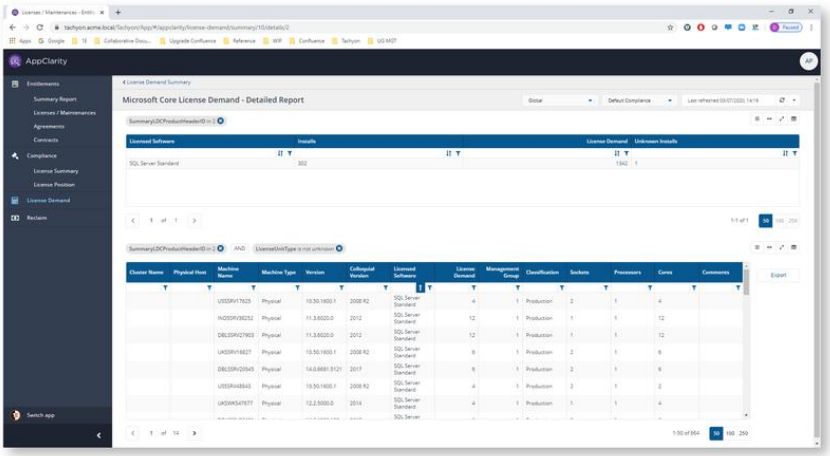
[Cores]

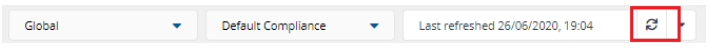
[Comments]

[Column actions]

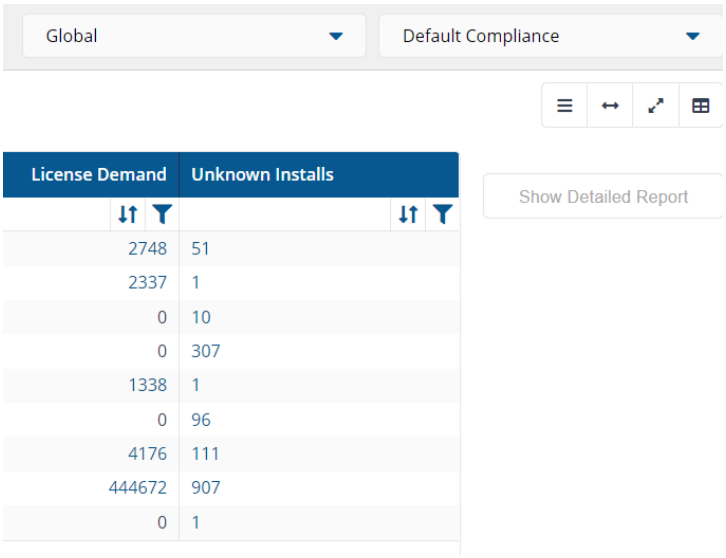
[Column sort]

[Column filter]



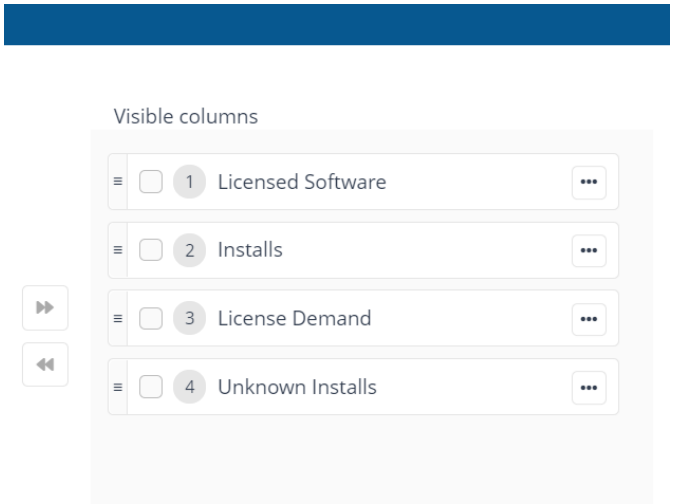
Field	Description
Management Group selector	Certain pages in AppClarity have a management groups selector. This drop-down lets you select the management group you are interested in. By default this is set to **Global**.
Compliance Repository selector	This field lets you select the repository where the compliance data displayed on the page comes from. By default this is set to **Default Compliance**. If you have created your own compliance repositories, click on the name to select these from the drop-down list.
Report Refresh	You can refresh reports from individual AppClarity screens as well as using the Settings App. Where this is available you can do this by using the refresh icon next to the **Last Refreshed** box: 

Field	Description
Column Picker	Where the column picker control is shown you can choose which columns are displayed. In the following example on the **Microsoft Core License Demand** page we hide the **Unknown Installs** column and move the **License Demand** column to the left of the page.



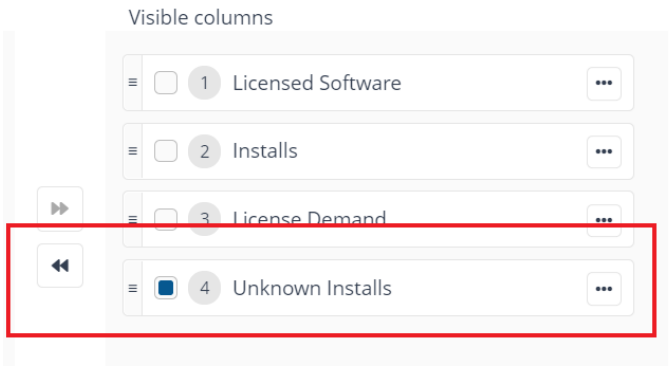
To pick the displayed columns:

Click on the Choose columns icon to the right of the header row to view the visible columns.

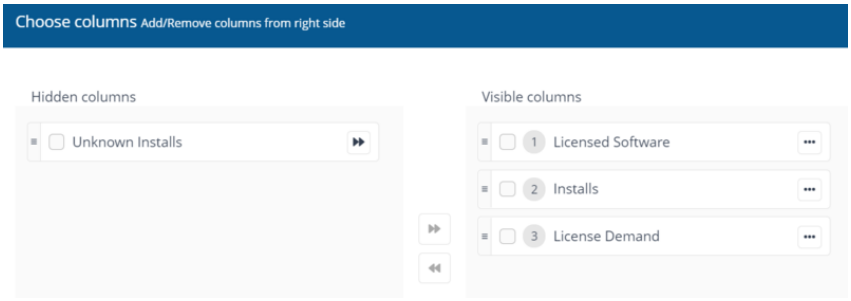


To exclude **Unknown Installs**, select the Unknown Installs row and click **Exclude columns** button.

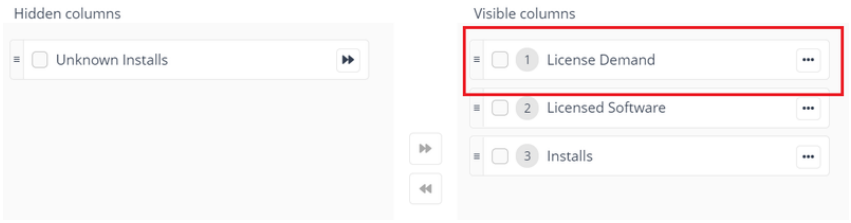
Field	Description



The **Unknown Installs** column is now hidden.



To move the **License Demand** column to the top of the list, hover your mouse over **License Demand** and using the direction control drag it to the top of the list.



The Microsoft Core License Demand page has now been automatically updated with our changes.

License Demand	Licensed Software	Installs
2748	Windows Server DataCenter	647
2337	SQL Server Enterprise	649
0	SQL Server Analysis Services	0
0	SQL Server Integration Services	0
1338	SQL Server Standard	300
0	SQL Server Reporting Services	0
4176	Windows Server Enterprise	265
444672	Windows Server Standard	4019
0	SQL Server Data Quality Services	0

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Action buttons</td><td>The following table describes the action buttons displayed on the Microsoft Core License Demand - Detailed Report page:

<table><tr><th>Button</th><th>Description</th></tr><tr><td>Export</td><td>Exports all the entries currently displayed in the Microsoft Core License Demand - Detailed Report table as a TSV file. This button takes the filters currently applied to the table into account, but not the sorting or the current selection.</td></tr></table></td></tr>
<tr><td>Microsoft Core License Demand - Summary table</td><td>This table displays a summary of the rows displayed in the Microsoft Core License Demand - Detailed Report table. The following table describes the columns displayed in the Microsoft Core License Demand Summary table:

<table><tr><th>Column</th><th>Description</th></tr><tr><td>Licensed Software</td><td>Displays software titles that are part of the License Demand report, where that software also has installations present in the inventory.</td></tr><tr><td>Installs</td><td>This column shows the number of installs for the software titles that are part of the License Demand report.</td></tr><tr><td>License Demand</td><td>This column shows the license demand for the software titles that are part of the License Demand report.</td></tr><tr><td>Unknown Installs</td><td>This column provides a count of the installations for the software titles that are part of the License Demand report where there are details that are unknown, thereby implying a risk for compliance calculation.</td></tr></table></td></tr>
<tr><td>Microsoft Core License Demand - Detailed Report table</td><td>The following table describes the columns displayed in the Microsoft Core License Demand - Detailed Report table:

<table><tr><th>Column</th><th>Description</th></tr><tr><td>Cluster Name</td><td>The Cluster Name, if any, where the software in the License Demand report is installed.</td></tr></table></td></tr>
</table>

Field	Description
Physical Host	The Physical Host, if any, where the software in the License Demand report is installed.
Machine Name	The device name, if any, where the software in the License Demand report is installed.
Machine Type	The type of the device where the software in the License Demand report is installed. This may be one of: Machine Type Cluster Physical Physical Host Virtual
Version	The version portion of the vendor, title, version and edition attributes that are used to identify software products. For example, **11.0.3216.5614** or **6.3.100.0**.
Colloquial Version	The colloquial version name for the product. For example, **2003**, **2016** etc. This is an additional attribute to the vendor, title, version and edition for a software product that may identify a range of versions.
Licensed Software	Displays software titles that are part of the License Demand report, where that software also has installations present in the inventory.
Installs	This column shows the number of installs for the software titles that are part of the License Demand report.
License Demand	This column shows the license demand for the software titles that are part of the License Demand report.

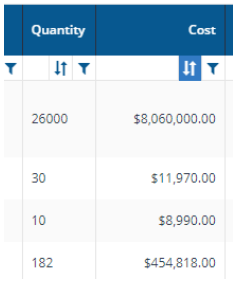
Field	Description
	Management Group — Displays the number of Management Groups a device is associated with. Clicking on the number displays a popup listing the Management Groups.
	Classification — Displays the classification for the device where the software is installed. If set this may be one of:

Classification
Production
Test

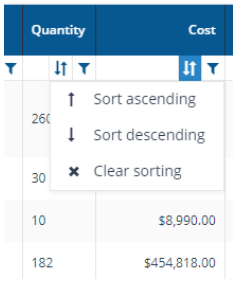
	Sockets — Displays the number of processor sockets available on the mainboard for the device where the software is installed.
	Processors — Displays the number of processors available on the mainboard for the device where the software is installed.
	Cores — Displays the number of processor cores available on the mainboard for the device where the software is installed.
	Comments — Provides recommendations on how to license the software to achieve the optimum license demand.
Column actions	The following column actions are available on some table columns:

Column actions	Description
Column sort	**Using column sorts** The picture shows an example taken from AppClarity. In our example we want to sort the table on the **Cost** column from the highest cost at the top to the lowest at the bottom. To sort the table on the **Cost** column: Click on the sort icon ⇅ just beneath the header row in the **Cost** column.

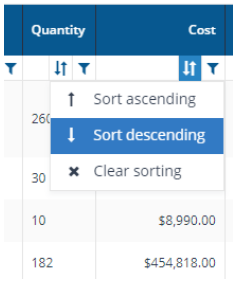
Field	Description



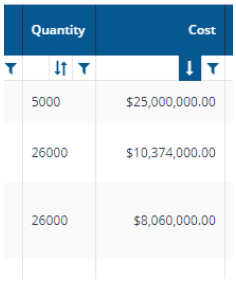
The sort popup is displayed.



Now select the sort direction. In our example this will be **Sort descending**.

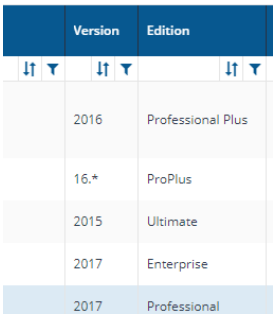


After selecting this the data in the table is now sorted on the **Cost** column from highest to lowest and the sort icon has changed to a sort descending icon



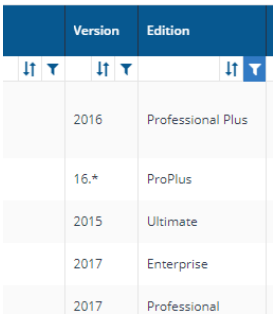
Clearing the sort

Field	Description
	You can clear the sort by clicking on the sort icon again and selecting the **Clear sorting** menu item from the sorting popup.
Column filter	**Using column filters** The picture opposite shows an example taken from AppClarity. In our example we want to filter the table to show only those items where the **Edition** contains the text **Prof**.

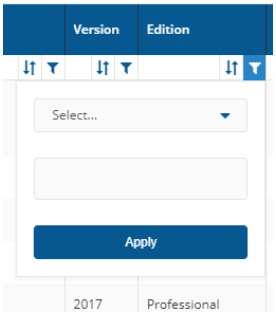


To filter the table on the **Edition** column:

Click on the filter icon just beneath the header row in the **Edition** column.

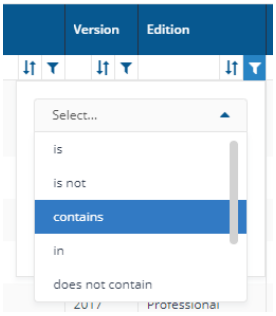


The filter popup is displayed.

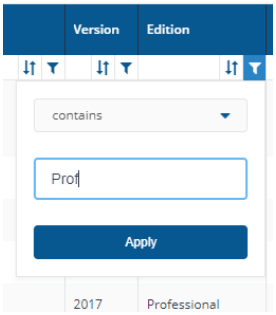


Now select the operator. In our example this will be **contains**.

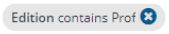
Field	Description



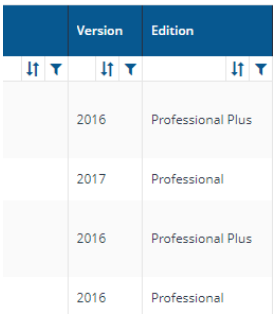
Then type the text **Prof** into the text field.



Click **Apply** and a new filter will be added to the table.



The table will be filtered to just those items whose **Edition** contains the text **Prof**.



Adding another filter

You can add another filter by clicking on the filter icon for any of the columns. The picture opposite shows another filter added selecting table rows where the **Type** also contains the text **License**. The table will also be filtered accordingly.

Field	Description
	Removing filters You can remove filters by clicking on the filter close icon at the end of the filter.

10.6.5.3.2 IBM Processor Value Unit (PVU) License Demand page

A description of the fields on the **IBM Processor Value Unit (PVU) License Demand** page.

This page provides an overview of the data in the **IBM Processor Value Unit (PVU) License Demand** report. You get to this page by navigating to the **AppClarity→Licence Demand** node in the navigation panel and then clicking on the **View Report** button for the **IBM Processor Value Unit (PVU) License Demand** report.

The fields on the **IBM Processor Value Unit (PVU) License Demand** page are:

Management Group selector

Compliance Repository selector

Report Refresh

Column Picker

Action buttons

Show Detailed Report

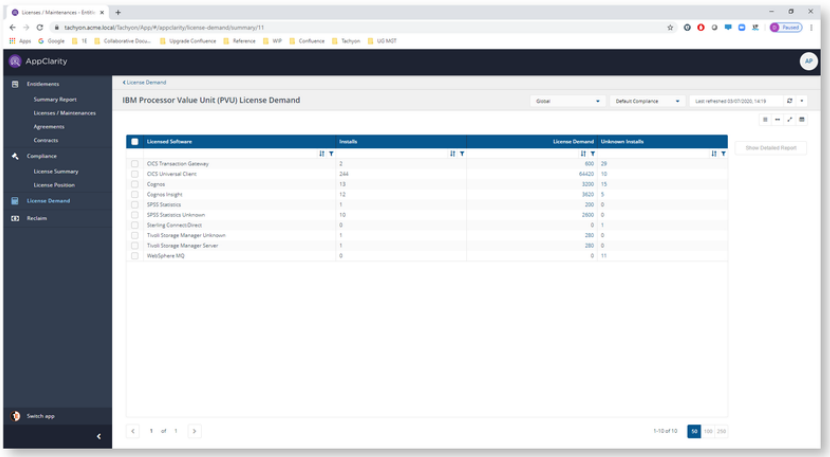
IBM Processor Value Unit (PVU) License Demand table

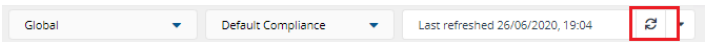
Licensed Software

Installs

License Demand

Unknown Installs



Field	Description
Management Group selector	Certain pages in AppClarity have a management groups selector. This drop-down lets you select the management group you are interested in. By default this is set to **Global**.
Compliance Repository selectorJust	This field lets you select the repository where the compliance data displayed on the page comes from. By default this is set to **Default Compliance**. If you have created your own compliance repositories, click on the name to select these from the drop-down list.
Report Refresh	You can refresh reports from individual AppClarity screens as well as using the Settings App. Where this is available you can do this by using the refresh icon next to the **Last Refreshed** box: 
Column Picker	**Using column picker**Where the column picker control is shown you can choose which columns are displayed. In the following example on the **Microsoft Core License Demand** page we hide the **Unknown Installs** column and move the **License Demand** column to the left of the page.To pick the displayed columns:Click on the Choose columns iconto the right of the header row to view the visible columns.To exclude **Unknown Installs**, select the Unknown Installs row and click **Exclude columns** button.The **Unknown Installs** column is now hidden.To move the **License Demand** column to the top of the list, hover your mouse over **License Demand** and using the direction control drag it to the top of the list.The Microsoft Core License Demand page has now been automatically updated with our changes.
Action buttons	The following table describes the action buttons displayed on the **IBM Processor Value Unit (PVU) License Demand** page:

Button	Description
Show Detailed Report	This button is only enabled if there is a single selection in the **IBM Processor Value Unit (PVU) License Demand** table. Clicking the button displays the IBM Processor Value Unit (PVU) License Demand - Detailed Report page for the selected item.

IBM Processor Value Unit	The following table describes the columns displayed in the **IBM Processor Value Unit (PVU) License Demand** table:

Field	Description	
(PVU) License Demand table	Column	Description
	Licensed Software	Displays software titles that are part of the License Demand report, where that software also has installations present in the inventory.
	Installs	This column shows the number of installs for the software titles that are part of the License Demand report.
	License Demand	This column shows the license demand for the software titles that are part of the License Demand report.
	Unknown Installs	This column provides a count of the installations for the software titles that are part of the License Demand report where there are details that are unknown, thereby implying a risk for compliance calculation.

10.6.5.3.2.1 IBM Processor Value Unit (PVU) License Demand - Detailed Report page

A description of the fields on the
IBM Processor Value Unit (PVU) License Demand - Detailed Report page.

This page displays the data for a selected software title on the **IBM Processor Value Unit (PVU) License Demand** page. You get to this page by navigating to the **AppClarity→License Demand** node in the navigation panel, selecting a row in the table and then clicking on the **Show Detailed Report** button.

The fields on the **IBM Processor Value Unit (PVU) License Demand - Detailed Report** page are:

Management Group selector

Compliance Repository selector

Report Refresh

Column Picker

Action buttons

Export

IBM Processor Value Unit (PVU) License Demand - Summary table

Licensed Software

Installs

License Demand

[Unknown Installs]

[IBM Processor Value Unit (PVU) License Demand - Detailed Report table]

[Cluster Name]

[Physical Host]

[Machine Name]

[Machine Type]

[Version]

[Colloquial Version]

[Licensed Software]

[Installs]

[License Demand]

[Management Group]

[Classification]

[Sockets]

[Processors]

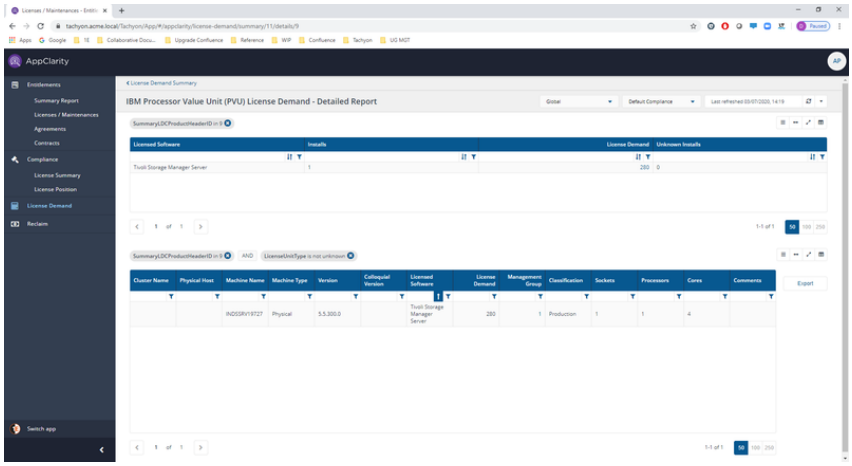
[Cores]

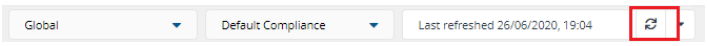
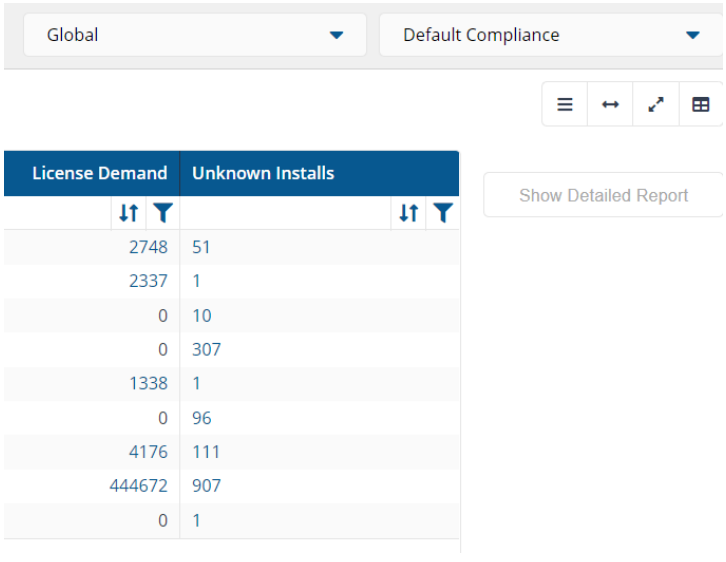
[Comments]

[Column actions]

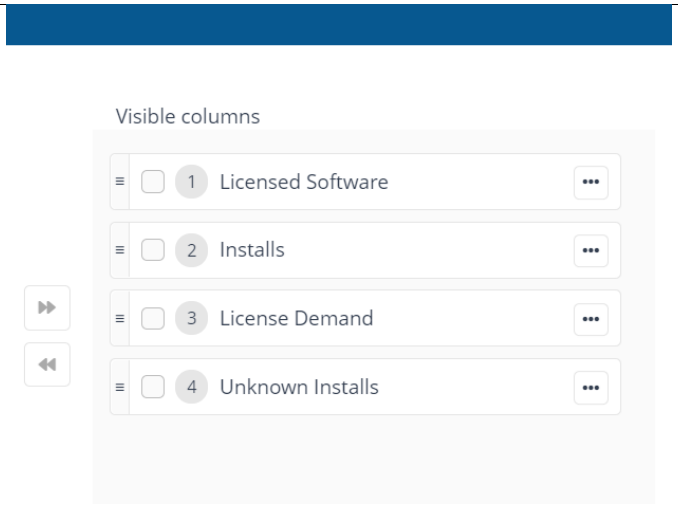
[Column sort]

[Column filter]

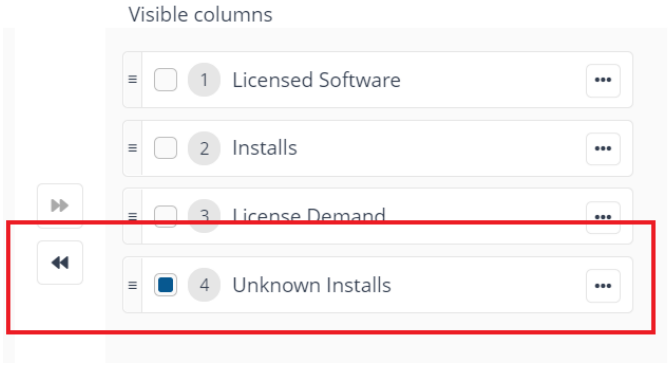


Field	Description
Management Group selector	Certain pages in AppClarity have a management groups selector. This drop-down lets you select the management group you are interested in. By default this is set to **Global**.
Compliance Repository selector	This field lets you select the repository where the compliance data displayed on the page comes from. By default this is set to **Default Compliance**. If you have created your own compliance repositories, click on the name to select these from the drop-down list.
Report Refresh	You can refresh reports from individual AppClarity screens as well as using the Settings App. Where this is available you can do this by using the refresh icon next to the **Last Refreshed** box: 
Column Picker	Where the column picker control is shown you can choose which columns are displayed. In the following example on the **Microsoft Core License Demand** page we hide the **Unknown Installs** column and move the **License Demand** column to the left of the page.  To pick the displayed columns: Click on the Choose columns icon to the right of the header row to view the visible columns.

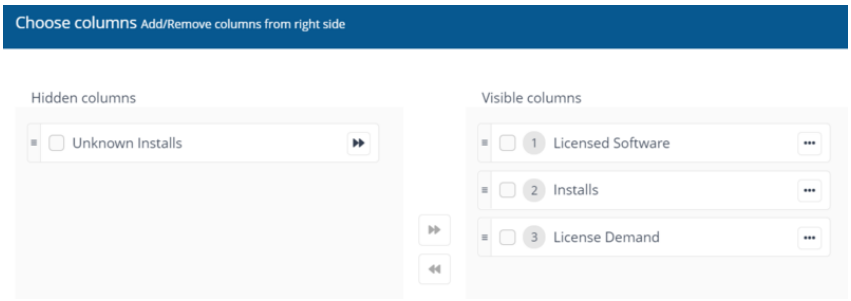
Field	Description



To exclude **Unknown Installs**, select the Unknown Installs row and click **Exclude columns** button.

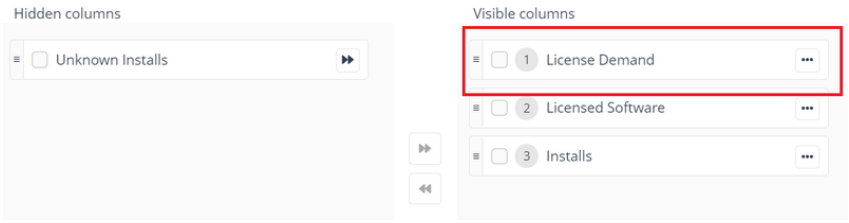


The **Unknown Installs** column is now hidden.



To move the **License Demand** column to the top of the list, hover your mouse over **License Demand** and using the direction control drag it to the top of the list.

Field	Description



The Microsoft Core License Demand page has now been automatically updated with our changes.

License Demand	Licensed Software	Installs
2748	Windows Server DataCenter	647
2337	SQL Server Enterprise	649
0	SQL Server Analysis Services	0
0	SQL Server Integration Services	0
1338	SQL Server Standard	300
0	SQL Server Reporting Services	0
4176	Windows Server Enterprise	265
444672	Windows Server Standard	4019
0	SQL Server Data Quality Services	0

Action buttons

The following table describes the action buttons displayed on the **IBM Processor Value Unit (PVU) License Demand - Detailed Report** page:

Button	Description
Export	Exports all the entries currently displayed in the **IBM Processor Value Unit (PVU) License Demand - Detailed Report** table as a TSV file. This button takes the filters currently applied to the table into account, but not the sorting or the current selection.

IBM Processor Value Unit (PVU) License Demand - Summary table

This table displays a summary of the rows displayed in the **IBM Processor Value Unit (PVU) License Demand - Detailed Report** table. The following table describes the columns displayed in the **IBM Processor Value Unit (PVU) License Demand Summary** table:

Column	Description
Licensed Software	Displays software titles that are part of the License Demand report, where that software also has installations present in the inventory.
Installs	This column shows the number of installs for the software titles that are part of the License Demand report.

Field	Description	
	License Demand	This column shows the license demand for the software titles that are part of the License Demand report.
	Unknown Installs	This column provides a count of the installations for the software titles that are part of the License Demand report where there are details that are unknown, thereby implying a risk for compliance calculation.

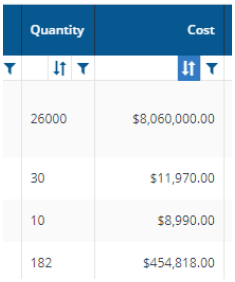
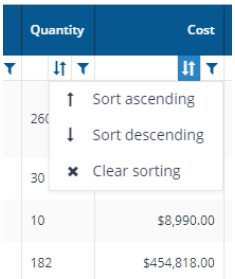
IBM Processor Value Unit (PVU) License Demand - Detailed Report table

The following table describes the columns displayed in the **IBM Processor Value Unit (PVU) License Demand - Detailed Report** table:

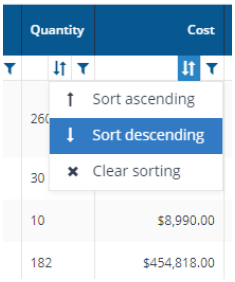
Column	Description
Cluster Name	The Cluster Name, if any, where the software in the License Demand report is installed.
Physical Host	The Physical Host, if any, where the software in the License Demand report is installed.
Machine Name	The device name, if any, where the software in the License Demand report is installed.
Machine Type	The type of the device where the software in the License Demand report is installed. This may be one of: Machine Type Cluster Physical Physical Host Virtual
Version	The version portion of the vendor, title, version and edition attributes that are used to identify software products. For example, **11.0.3216.5614** or **6.3.100.0**.

Field	Description
Colloquial Version	The colloquial version name for the product. For example, **2003**, **2016** etc. This is an additional attribute to the vendor, title, version and edition for a software product that may identify a range of versions.
Licensed Software	Displays software titles that are part of the License Demand report, where that software also has installations present in the inventory.
Installs	This column shows the number of installs for the software titles that are part of the License Demand report.
License Demand	This column shows the license demand for the software titles that are part of the License Demand report.
Management Group	Displays the number of Management Groups a device is associated with. Clicking on the number displays a popup listing the Management Groups.
Classification	Displays the classification for the device where the software is installed. If set this may be one of: Classification Production Test
Sockets	Displays the number of processor sockets available on the mainboard for the device where the software is installed.
Processors	Displays the number of processors available on the mainboard for the device where the software is installed.
Cores	Displays the number of processor cores available on the mainboard for the device where the software is installed.
Comments	Provides recommendations on how to license the software to achieve the optimum license demand.

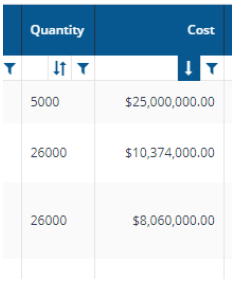
Field	Description
Column actions	The following column actions are available on some table columns:

Column actions	Description
Column sort	**Using column sorts** The picture opposite shows an example taken from AppClarity. In our example we want to sort the table on the **Cost** column from the highest cost at the top to the lowest at the bottom. To sort the table on the **Cost** column: Click on the sort icon ⇅ just beneath the header row in the **Cost** column.  The sort popup is displayed.  Now select the sort direction. In our example this will be **Sort descending**.

Field	Description



After selecting this the data in the table is now sorted on the **Cost** column from highest to lowest and the sort icon has changed to a sort descending icon



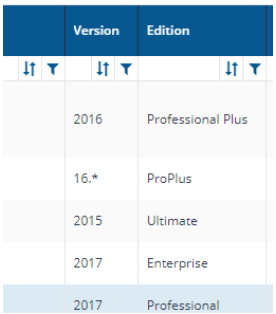
Clearing the sort

You can clear the sort by clicking on the sort icon again and selecting the **Clear sorting** menu item from the sorting popup.

Column filter

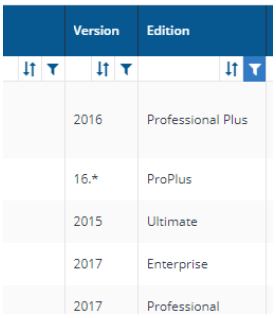
Using column filters

The image shows an example taken from AppClarity. In our example we want to filter the table to show only those items where the **Edition** contains the text **Prof**.

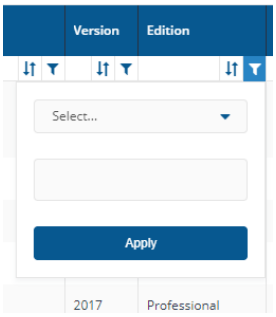


To filter the table on the **Edition** column:

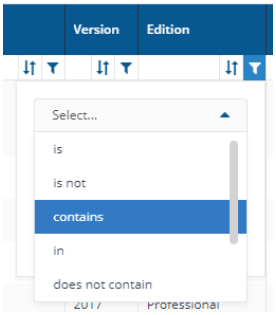
Field	Description
	Click on the filter icon just beneath the header row in the **Edition** column.



The filter popup is displayed.

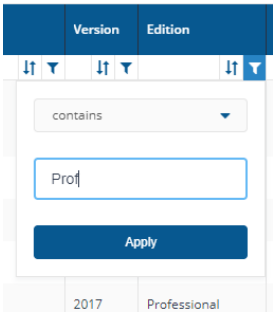


Now select the operator. In our example this will be **contains**.

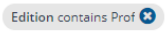


Then type the text **Prof** into the text field

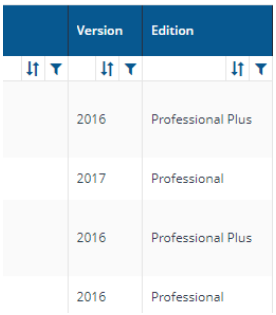
Field	Description



Click **Apply** and a new filter will be added to the table.

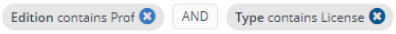


The table will be filtered to just those items whose **Edition** contains the text **Prof**.



Adding another filter

You can add another filter by clicking on the filter icon for any of the columns. The picture opposite shows another filter added selecting table rows where the **Type** also contains the text **License**. The table will also be filtered accordingly.



Removing filters

You can remove filters by clicking on the filter close icon at the end of the filter.

10.6.5.3.3 Oracle Processor License Demand page

A description of the fields on the **Oracle Processor License Demand** page.

This page provides an overview of the data in the **Oracle Processor License Demand** report. You get to this page by navigating to the **AppClarity**→**Licence Demand** node in the navigation panel and then clicking on the **View Report** button for the **Oracle Processor License Demand** report.

The fields on the **Oracle Processor License Demand** page are:

Management Group selector

Compliance Repository selector

Report Refresh

Column Picker

Action buttons

Show Detailed Report

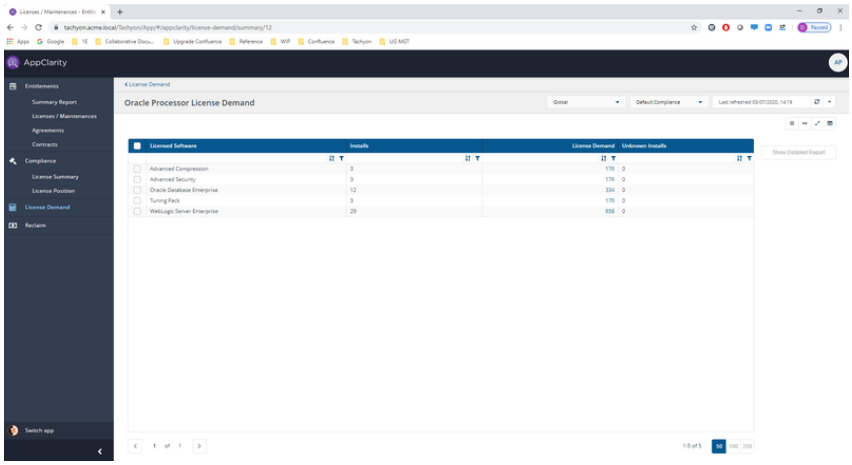
Oracle Processor License Demand table

Licensed Software

Installs

License Demand

Unknown Installs



Field	Description
Management Group selector	Certain pages in AppClarity have a management groups selector. This drop-down lets you select the management group you are interested in. By default this is set to **Global**.
Compliance Repository selector	This field lets you select the repository where the compliance data displayed on the page comes from. By default this is set to **Default Compliance**.

Field	Description
	If you have created your own compliance repositories, click on the name to select these from the drop-down list.
Report Refresh	You can refresh reports from individual AppClarity screens as well as using the Settings App. Where this is available you can do this by using the refresh icon next to the **Last Refreshed** box:
Column Picker	**Using column picker**Where the column picker control is shown you can choose which columns are displayed. In the following example on the **Microsoft Core License Demand** page we hide the **Unknown Installs** column and move the **License Demand** column to the left of the page.To pick the displayed columns:Click on the Choose columns iconto the right of the header row to view the visible columns.To exclude **Unknown Installs**, select the Unknown Installs row and click **Exclude columns** button.The **Unknown Installs** column is now hidden.To move the **License Demand** column to the top of the list, hover your mouse over **License Demand** and using the direction control drag it to the top of the list.The Microsoft Core License Demand page has now been automatically updated with our changes.
Action buttons	The following table describes the action buttons displayed on the **Oracle Processor License Demand** page:

Button	Description
Show Detailed Report	This button is only enabled if there is a single selection in the **Oracle Processor License Demand** table. Clicking the button displays the Oracle Processor License Demand - Detailed Report page for the selected item.

Oracle Processor License Demand table

The following table describes the columns displayed in the **Oracle Processor License Demand** table:

Column	Description
Licensed Software	Displays software titles that are part of the License Demand report, where that software also has installations present in the inventory.

Field	Description
Installs	This column shows the number of installs for the software titles that are part of the License Demand report.
License Demand	This column shows the license demand for the software titles that are part of the License Demand report.
Unknown Installs	This column provides a count of the installations for the software titles that are part of the License Demand report where there are details that are unknown, thereby implying a risk for compliance calculation.

10.6.5.3.3.1 Oracle Processor License Demand - Detailed Report page

A description of the fields on the **Oracle Processor License Demand - Detailed Report** page.

This page displays the data for a selected software title on the **Oracle Processor License Demand** page. You get to this page by navigating to the **AppClarity→Licence Demand** node in the navigation panel, selecting a row in the table and then clicking on the **Show Detailed Report** button.

The fields on the **Oracle Processor License Demand - Detailed Report** page are:

Management Group selector

Compliance Repository selector

Report Refresh

Column Picker

Action buttons

Export

Oracle Processor License Demand - Summary table

Licensed Software

Installs

License Demand

Unknown Installs

Oracle Processor License Demand - Detailed Report table

Cluster Name

Physical Host

Machine Name

Machine Type

Version

Colloquial Version

Licensed Software

Installs

License Demand

Management Group

Classification

Sockets

Processors

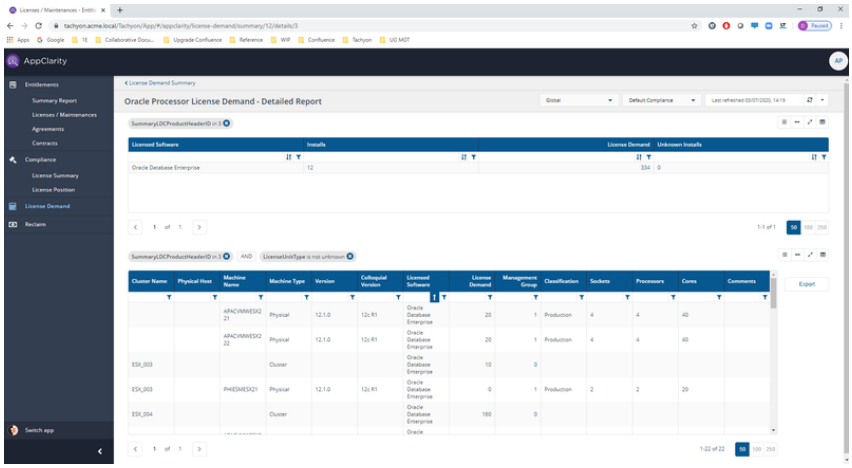
Cores

Comments

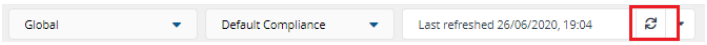
Column actions

Column sort

Column filter



Field	Description
Management Group selector	Certain pages in AppClarity have a management groups selector. This drop-down lets you select the management group you are interested in. By default this is set to **Global**.

Field	Description
Compliance Repository selector	This field lets you select the repository where the compliance data displayed on the page comes from. By default this is set to **Default Compliance**. If you have created your own compliance repositories, click on the name to select these from the drop-down list.
Report Refresh	You can refresh reports from individual AppClarity screens as well as using the Settings App. Where this is available you can do this by using the refresh icon next to the **Last Refreshed** box: 
Column Picker	**Using column picker**Where the column picker control is shown you can choose which columns are displayed. In the following example on the **Microsoft Core License Demand** page we hide the **Unknown Installs** column and move the **License Demand** column to the left of the page.To pick the displayed columns:Click on the Choose columns iconto the right of the header row to view the visible columns.To exclude **Unknown Installs**, select the Unknown Installs row and click **Exclude columns** button.The **Unknown Installs** column is now hidden.To move the **License Demand** column to the top of the list, hover your mouse over **License Demand** and using the direction control drag it to the top of the list.The Microsoft Core License Demand page has now been automatically updated with our changes.
Action buttons	The following table describes the action buttons displayed on the **Oracle Processor License Demand - Detailed Report** page:

Button	Description
Export	Exports all the entries currently displayed in the **Oracle Processor License Demand - Detailed Report** table as a TSV file. This button takes the filters currently applied to the table into account, but not the sorting or the current selection.

Oracle Processor License Demand - Summary table	This table displays a summary of the rows displayed in the **Oracle Processor License Demand - Detailed Report** table. The following table describes the columns displayed in the **Oracle Processor License Demand Summary** table:

Field	Description

Column	Description
Licensed Software	Displays software titles that are part of the License Demand report, where that software also has installations present in the inventory.
Installs	This column shows the number of installs for the software titles that are part of the License Demand report.
License Demand	This column shows the license demand for the software titles that are part of the License Demand report.
Unknown Installs	This column provides a count of the installations for the software titles that are part of the License Demand report where there are details that are unknown, thereby implying a risk for compliance calculation.

Oracle Processor License Demand - Detailed Report table

The following table describes the columns displayed in the **Oracle Processor License Demand - Detailed Report** table:

Column	Description
Cluster Name	The Cluster Name, if any, where the software in the License Demand report is installed.
Physical Host	The Physical Host, if any, where the software in the License Demand report is installed.
Machine Name	The device name, if any, where the software in the License Demand report is installed.
Machine Type	The type of the device where the software in the License Demand report is installed. This may be one of: Machine Type --- Cluster Physical

Field	Description
	Physical Host Virtual
Version	The version portion of the vendor, title, version and edition attributes that are used to identify software products. For example, **11.0.3216.5614** or **6.3.100.0**.
Colloquial Version	The colloquial version name for the product. For example, **2003**, **2016** etc. This is an additional attribute to the vendor, title, version and edition for a software product that may identify a range of versions.
Licensed Software	Displays software titles that are part of the License Demand report, where that software also has installations present in the inventory.
Installs	This column shows the number of installs for the software titles that are part of the License Demand report.
License Demand	This column shows the license demand for the software titles that are part of the License Demand report.
Management Group	Displays the number of Management Groups a device is associated with. Clicking on the number displays a popup listing the Management Groups.
Classification	Displays the classification for the device where the software is installed. If set this may be one of: Classification --- Production Test
Sockets	Displays the number of processor sockets available on the mainboard for the device where the software is installed.

Field	Description	
	Processors	Displays the number of processors available on the mainboard for the device where the software is installed.
	Cores	Displays the number of processor cores available on the mainboard for the device where the software is installed.
	Comments	Provides recommendations on how to license the software to achieve the optimum license demand.

Column actions The following column actions are available on some table columns:

Column actions	Description
Column sort	Some tables contain column sorts that let you easily re-order the information displayed in the table.**Using column sorts**The picture opposite shows an example taken from AppClarity. In our example we want to sort the table on the **Cost** column from the highest cost at the top to the lowest at the bottom. To sort the table on the **Cost** column:Click on the sort iconjust beneath the header row in the **Cost** column.The sort popup is displayed.Now select the sort direction. In our example this will be **Sort descending**.After selecting this the data in the table is now sorted on the **Cost** column from highest to lowest and the sort icon has changed to a sort descending icon**Clearing the sort**You can clear the sort by clicking on the sort icon again and selecting the **Clear sorting** menu item from the sorting popup.
Column filter	Some tables contain a column filter that lets you easily filter the information displayed in the table.**Using column filters**The picture opposite shows an example taken from AppClarity. In our example we want to filter the table to show only those items where the **Edition** contains the text **Prof**.To filter the table on the **Edition** column:Click on the filter iconjust beneath the header row in the **Edition** column.The filter popup is displayed.Now select the operator. In our example this will be **contains**.Then type the text **Prof** into the text field.Click **Apply** and a new filter will be added to the table.The table will be filtered to just those items whose **Edition** contains the text **Prof**.**Adding another filter**You can add another filter by clicking on the filter icon for any of the columns. The picture opposite

Field	Description
	shows another filter added selecting table rows where the **Type** also contains the text **License**. The table will also be filtered accordingly.**Removing filters**You can remove filters by clicking on the filter close icon at the end of the filter.

10.6.5.3.4 Red Hat Socket Demand page

A description of the fields on the **Red Hat Socket Demand** page.

This page provides an overview of the data in the **Red Hat Socket Demand** report. You get to this page by navigating to the **AppClarity**→**Licence Demand** node in the navigation panel and then clicking on the **View Report** button for the **Red Hat Socket Demand** report.

The fields on the **Red Hat Socket Demand** page are:

Management Group selector

Compliance Repository selector

Report Refresh

Column Picker

Action buttons

Show Detailed Report

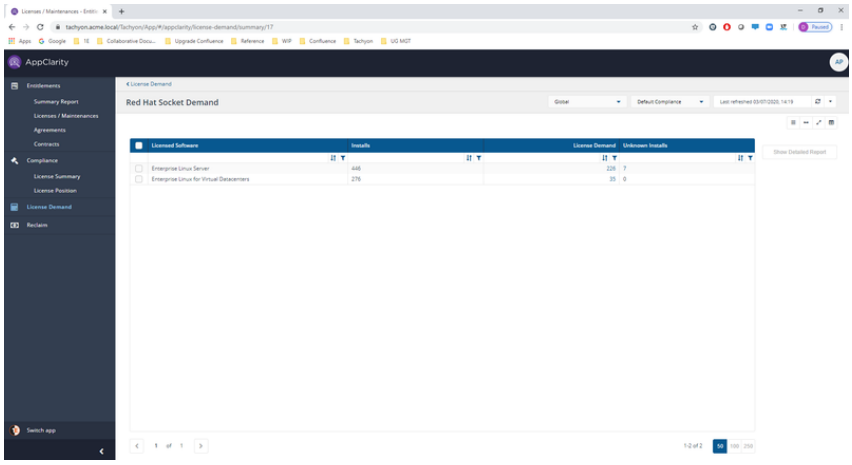
Red Hat Socket Demand table

Licensed Software

Installs

License Demand

Unknown Installs



Field	Description
Management Group selector	Certain pages in AppClarity have a management groups selector. This drop-down lets you select the management group you are interested in. By default this is set to **Global**.
Compliance Repository selector	This field lets you select the repository where the compliance data displayed on the page comes from. By default this is set to **Default Compliance**. If you have created your own compliance repositories, click on the name to select these from the drop-down list.
Report Refresh	You can refresh reports from individual AppClarity screens as well as using the Settings App. Where this is available you can do this by using the refresh icon next to the **Last Refreshed** box:
Column Picker	Where the column picker control is shown you can choose which columns are displayed. In the following example on the **Microsoft Core License Demand** page we hide the **Unknown Installs** column and move the **License Demand** column to the left of the page. To pick the displayed columns: Click on the Choose columns icon to the right of the header row to view the visable columns. To exclude **Unknown Installs**, select the Unknown Installs row and click **Exclude columns** button. The **Unknown Installs** column is now hidden. To move the **License Demand** column to the top of the list, hover your mouse over **License Demand** and using the direction control drag it to the top of the list.

Field	Description
	The Microsoft Core License Demand page has now been automatically updated with our changes.
Action buttons	The following table describes the action buttons displayed on the **Red Hat Socket Demand** page:

Button	Description
Show Detailed Report	This button is only enabled if there is a single selection in the **Red Hat Socket Demand** table. Clicking the button displays the Red Hat Socket Demand - Detailed Report page for the selected item.

Red Hat Socket Demand table

The following table describes the columns displayed in the **Red Hat Socket Demand** table:

Column	Description
Licensed Software	Displays software titles that are part of the License Demand report, where that software also has installations present in the inventory.
Installs	This column shows the number of installs for the software titles that are part of the License Demand report.
License Demand	This column shows the license demand for the software titles that are part of the License Demand report.
Unknown Installs	This column provides a count of the installations for the software titles that are part of the License Demand report where there are details that are unknown, thereby implying a risk for compliance calculation.

10.6.5.3.4.1 Red Hat Socket Demand - Detailed Report page

A description of the fields on the **Red Hat Socket Demand - Detailed Report** page.

This page displays the data for a selected software title on the **Red Hat Socket Demand** page. You get to this page by navigating to the **AppClarity→Licence Demand** node in the navigation panel, selecting a row in the table and then clicking on the **Show Detailed Report** button.

The fields on the **Red Hat Socket Demand - Detailed Report** page are:

Management Group selector

Compliance Repository selector

Report Refresh

Column Picker

Action buttons

Export

Red Hat Socket Demand - Summary table

Licensed Software

Installs

License Demand

Unknown Installs

Red Hat Socket Demand - Detailed Report table

Cluster Name

Physical Host

Machine Name

Machine Type

Version

Colloquial Version

Licensed Software

Installs

License Demand

Management Group

Classification

Sockets

Processors

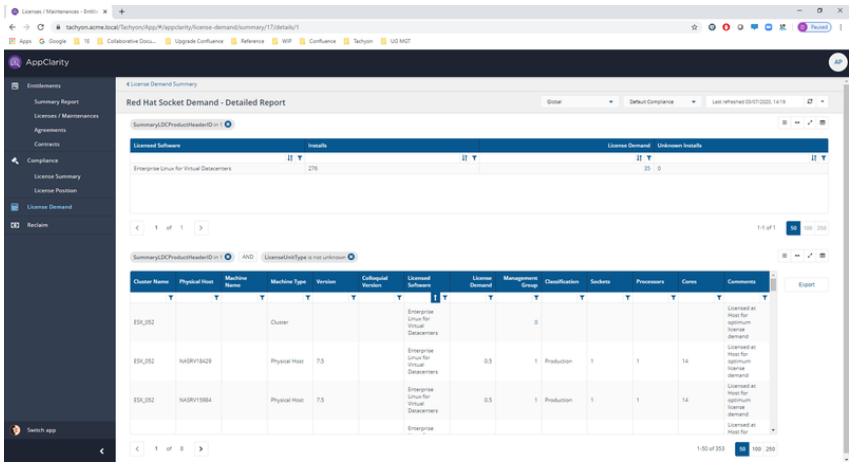
Cores

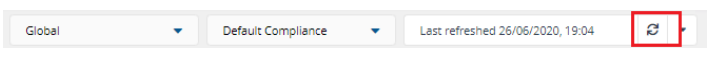
Comments

Column actions

Column sort

Column filter



Field	Description
Management Group selector	Certain pages in AppClarity have a management groups selector. This drop-down lets you select the management group you are interested in. By default this is set to **Global**.
Compliance Repository selector	This field lets you select the repository where the compliance data displayed on the page comes from. By default this is set to **Default Compliance**. If you have created your own compliance repositories, click on the name to select these from the drop-down list.
Report Refresh	You can refresh reports from individual AppClarity screens as well as using the Settings App. Where this is available you can do this by using the refresh icon next to the **Last Refreshed** box: 
Column Picker	**Using column picker**Where the column picker control is shown you can choose which columns are displayed. In the following example on the **Microsoft Core License Demand** page we hide the **Unknown Installs** column and move the **License Demand** column to the left of the page.To pick the displayed columns:Click on the Choose columns iconto the right of the header row to view the visible columns.To exclude **Unknown Installs**, select the Unknown Installs row and click **Exclude columns** button.The **Unknown Installs** column is now hidden.To move the

Field	Description
	License Demand column to the top of the list, hover your mouse over **License Demand** and using the direction control drag it to the top of the list.The Microsoft Core License Demand page has now been automatically updated with our changes.
Action buttons	The following table describes the action buttons displayed on the **Red Hat Socket Demand - Detailed Report** page:

Button	Description
Export	Exports all the entries currently displayed in the **Red Hat Socket Demand - Detailed Report** table as a TSV file. This button takes the filters currently applied to the table into account, but not the sorting or the current selection.

Red Hat Socket Demand - Summary table

This table displays a summary of the rows displayed in the **Red Hat Socket Demand - Detailed Report** table. The following table describes the columns displayed in the **Red Hat Socket Demand Summary** table:

Column	Description
Licensed Software	Displays software titles that are part of the License Demand report, where that software also has installations present in the inventory.
Installs	This column shows the number of installs for the software titles that are part of the License Demand report.
License Demand	This column shows the license demand for the software titles that are part of the License Demand report.
Unknown Installs	This column provides a count of the installations for the software titles that are part of the License Demand report where there are details that are unknown, thereby implying a risk for compliance calculation.

Red Hat Socket Demand - Detailed Report table

The following table describes the columns displayed in the **Red Hat Socket Demand - Detailed Report** table:

Field	Description

Column	Description
Cluster Name	The Cluster Name, if any, where the software in the License Demand report is installed.
Physical Host	The Physical Host, if any, where the software in the License Demand report is installed.
Machine Name	The device name, if any, where the software in the License Demand report is installed.
Machine Type	The type of the device where the software in the License Demand report is installed. This may be one of: Machine Type --- Cluster Physical Physical Host Virtual
Version	The version portion of the vendor, title, version and edition attributes that are used to identify software products. For example, **11.0.3216.5614** or **6.3.100.0**.
Colloquial Version	The colloquial version name for the product. For example, **2003**, **2016** etc. This is an additional attribute to the vendor, title, version and edition for a software product that may identify a range of versions.
Licensed Software	Displays software titles that are part of the License Demand report, where that software also has installations present in the inventory.
Installs	This column shows the number of installs for the software titles that are part of the License Demand report.

Field	Description
	License Demand This column shows the license demand for the software titles that are part of the License Demand report.
	Management Group Displays the number of Management Groups a device is associated with. Clicking on the number displays a popup listing the Management Groups.
	Classification Displays the classification for the device where the software is installed. If set this may be one of: Classification Production Test
	Sockets Displays the number of processor sockets available on the mainboard for the device where the software is installed.
	Processors Displays the number of processors available on the mainboard for the device where the software is installed.
	Cores Displays the number of processor cores available on the mainboard for the device where the software is installed.
	Comments Provides recommendations on how to license the software to achieve the optimum license demand.

Column actions The following column actions are available on some table columns:

Column actions	Description
Column sort	Some tables contain column sorts that let you easily re-order the information displayed in the table.**Using column sorts**The picture opposite shows an example taken from AppClarity. In our example we want to sort the table on the **Cost** column from the highest cost at the top to the lowest at the bottom. To sort the table on the **Cost** column:Click on the sort iconjust beneath the header row in the **Cost** column.The sort popup is displayed.Now select the sort direction. In our example this will

Field	Description
	be **Sort descending**.After selecting this the data in the table is now sorted on the **Cost** column from highest to lowest and the sort icon has changed to a sort descending icon**Clearing the sort**You can clear the sort by clicking on the sort icon again and selecting the **Clear sorting** menu item from the sorting popup.
Column filter	Some tables contain a column filter that lets you easily filter the information displayed in the table.**Using column filters**The picture opposite shows an example taken from AppClarity. In our example we want to filter the table to show only those items where the **Edition** contains the text **Prof**.To filter the table on the **Edition** column:Click on the filter iconjust beneath the header row in the **Edition** column.The filter popup is displayed.Now select the operator. In our example this will be **contains**.Then type the text **Prof** into the text field.Click **Apply** and a new filter will be added to the table.The table will be filtered to just those items whose **Edition** contains the text **Prof**.**Adding another filter**You can add another filter by clicking on the filter icon for any of the columns. The picture opposite shows another filter added selecting table rows where the **Type** also contains the text **License**. The table will also be filtered accordingly.**Removing filters**You can remove filters by clicking on the filter close icon at the end of the filter.

10.6.5.4 Reclaim

A reference for the fields and tables on the pages under the **Reclaim** node in the **AppClarity** application.

10.6.5.4.1 Usage Summary page

A description of the fields on the **Usage Summary** page.

Here you can browse reclaimable products from your inventory according to their usage. You get to this page by clicking the **Reclaim→Usage Summary** node in the navigation panel.

The fields on the **Usage Summary** page are:

Management Groups selector

Compliance repository selector

Report Refresh

Usage Category chart

[Top 5 Software Category by Installs chart]

[Top 10 Saving Opportunities ($) chart]

[Licensable toggle]

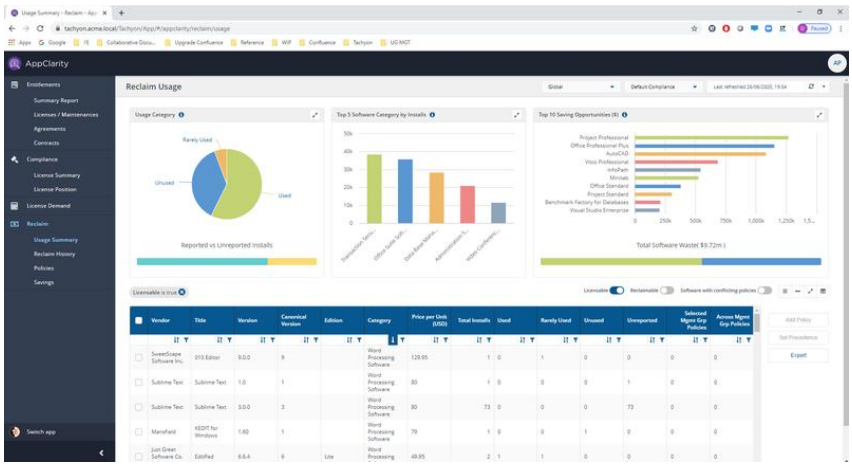
[Reclaimable toggle]

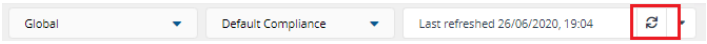
[Software with conflicting policies toggle]

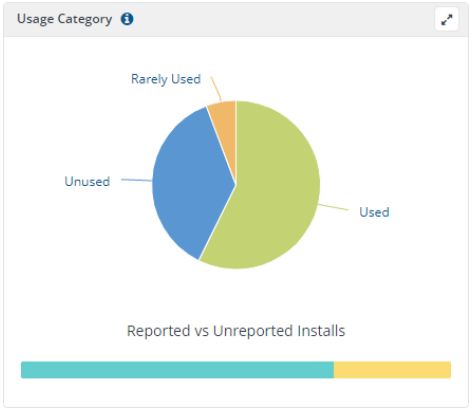
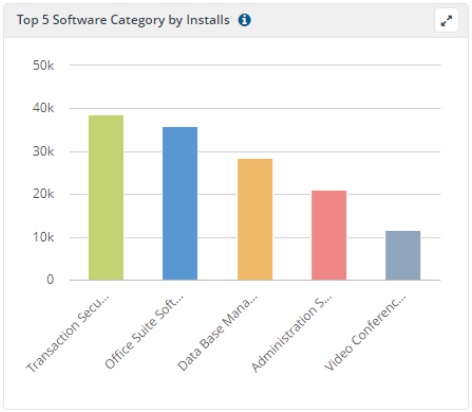
[Column Picker]

[Action buttons]

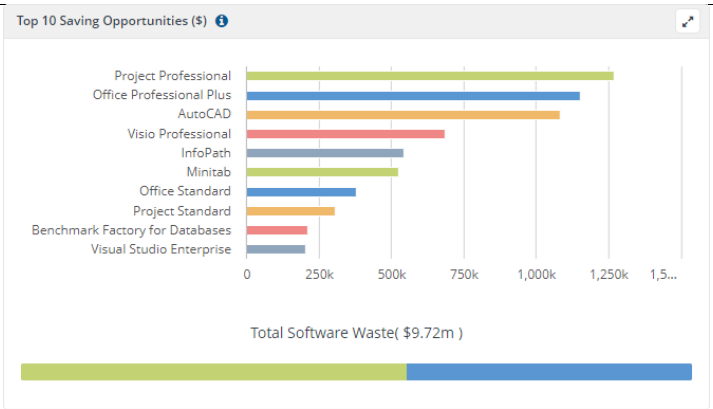
[Usage Summary table]



Field	Description
Management Groups selector	Certain pages in AppClarity have a management groups selector. This drop-down lets you select the management group you are interested in. By default this is set to **Global**.
Compliance repository selector	This field lets you select the repository where the compliance data displayed on the page comes from. By default this is set to **Default Compliance**. If you have created your own compliance repositories, click on the name to select these from the drop-down list.
Report Refresh	You can refresh reports from individual AppClarity screens as well as using the Settings App. Where this is available you can do this by using the refresh icon next to the **Last Refreshed** box: 

Field	Description
Usage Category chart	This chart shows the distribution of installations into the three usage categories: User, Rarely Used and Unused as a percentage of the total installations that reported usage. The bar at the bottom shows the number of installations with reported versus unreported usage as a percentage of the total number of installations. 
Top 5 Software Category by Installs chart	This chart shows the top five categories according to the numbers of installations. This chart disregards Operating Systems and Internet Browser categories. 
Top 10 Saving Opportunities ($) chart	This chart shows the top ten products that offer the best savings opportunities in USD. It is calculated by multiplying each product's unit price and the sum of unused and rarely used installations. The bar at the bottom shows the total opportunity in USD split into unused and rarely used installations.

Field	Description



Licensable toggle	The **Licensable** toggle adds a filter when it's turned on that filters the table to only display the products that are licensable, according to the catalog.
Reclaimable toggle	The **Reclaimable** toggle adds a filter when it's turned on that filters the table to only display the products that have a reclaim policy associated with them.
Software with conflicting policies toggle	The **Software with conflicting policies** toggle adds a filter when it's turned on that filters the table to only display the products that have reclaim policies that conflict.
Column Picker	**Using column picker**Where the column picker control is shown you can choose which columns are displayed. In the following example on the **Microsoft Core License Demand** page we hide the **Unknown Installs** column and move the **License Demand** column to the left of the page.To pick the displayed columns:Click on the Choose columns iconto the right of the header row to view the visible columns.To exclude **Unknown Installs**, select the Unknown Installs row and click **Exclude columns** button.The **Unknown Installs** column is now hidden.To move the **License Demand** column to the top of the list, hover your mouse over **License Demand** and using the direction control drag it to the top of the list.The Microsoft Core License Demand page has now been automatically updated with our changes.
Action buttons	The following table describes the action buttons displayed on the**Usage Summary**page:

Button	Description
Add Policy	This button is only enabled when there is a single selection in the **Usage Summary** table.

Field	Description	
		Creates a new reclaim policy for the selected product and opens the **New Policy** page with the details of the product pre-filled. Please refer to for more details.
	Set Precedence	This button is only enabled when a product with conflicting reclaim policies is selected in the **Usage Summary** table. Opens the Precedence page showing the conflicting reclaim policies allowing you to set their precedence.
	Export	Exports all the entries currently displayed in the **Usage Summary** table as a TSV file. This button takes the filters currently applied to the table into account, but not the sorting or the current selection.
Usage Summary table	The following table describes the columns displayed in the**Usage Summary**table:	

Column	Description
Vendor	The vendor portion of the vendor, title, version and edition attributes that are used to identify software products. For example, **Microsoft Corporation** or **1E**.
Title	The title portion of the vendor, title, version and edition attributes that are used to identify software products. For example, **Visio** or **Nomad**.
Version	The version portion of the vendor, title, version and edition attributes that are used to identify software products. For example, **11.0.3216.5614** or **6.3.100.0**.
Canonical Version	The canonical representation of the productversion installed on a device.
Edition	The edition portion of the vendor, title, version and edition attributes that are used to identify software products. For example, **Standard** or **-** (where no edition exists).

Field	Description
Category	The **Category** column shows the category for each product.
Price per Unit (USD)	The **Price per Unit (USD)** shows the cost in USD for each license of a product.
Total Installs	The **Total Installs** column shows the total number of installations for each product.
Used	The **Used** column shows the number of installations for each product that have been reported as being used.
Rarely Used	The **Rarely Used** column shows the number of installations for each product that have been reported as being rarely used.
Unused	The **Unused** column shows the number of installations for each product that have been reported as not being used.
Unreported	The **Unreported** column shows the number of installations for each product where no recent usage data has been reported.
Selected Mgmt Grp Policies	The **Selected Mgmt Grp Policies** column shows the number of reclaim policies for a product in the currently selected Management Group.
Across Mgmt Grp Policies	The **Across Mgmt Grp Policies** column shows the number of policies for a product across all management groups.

The following column actions are available on some table columns:

Column actions	Description
Column sort	Some tables contain column sorts that let you easily re-order the information displayed in the table.**Using column sorts**The picture opposite shows an example taken from AppClarity. In our example we want to sort the table on the **Cost** column from the highest cost at the top to the lowest at the bottom. To sort

Field	Description
	the table on the **Cost** column:Click on the sort iconjust beneath the header row in the **Cost** column.The sort popup is displayed.Now select the sort direction. In our example this will be **Sort descending**.After selecting this the data in the table is now sorted on the **Cost** column from highest to lowest and the sort icon has changed to a sort descending icon**Clearing the sort**You can clear the sort by clicking on the sort icon again and selecting the **Clear sorting** menu item from the sorting popup.
Column filter	Some tables contain a column filter that lets you easily filter the information displayed in the table.**Using column filters**The picture opposite shows an example taken from AppClarity. In our example we want to filter the table to show only those items where the **Edition** contains the text **Prof**.To filter the table on the **Edition** column:Click on the filter iconjust beneath the header row in the **Edition** column.The filter popup is displayed.Now select the operator. In our example this will be **contains**.Then type the text **Prof** into the text field.Click **Apply** and a new filter will be added to the table.The table will be filtered to just those items whose **Edition** contains the text **Prof**.**Adding another filter**You can add another filter by clicking on the filter icon for any of the columns. The picture opposite shows another filter added selecting table rows where the **Type** also contains the text **License**. The table will also be filtered accordingly.**Removing filters**You can remove filters by clicking on the filter close icon at the end of the filter.

10.6.5.4.1.1 Precedence page

A description of the fields on the **Precedence** page.

Here you can set the precedence for overlapping reclaim policies. You get to this page by:

Navigate to the **AppClarity**→**Reclaim**→**Usage Summary** node in the navigation panel

Select a product with conflicting reclaim policies

Click on the **Set Precedence** button.

The fields on the **Precedence** page are:

Compliance Repository selector

Conflicting reclaim policies table

Vendor

Title

Edition

Versions

Colloquial Version

Is Enabled

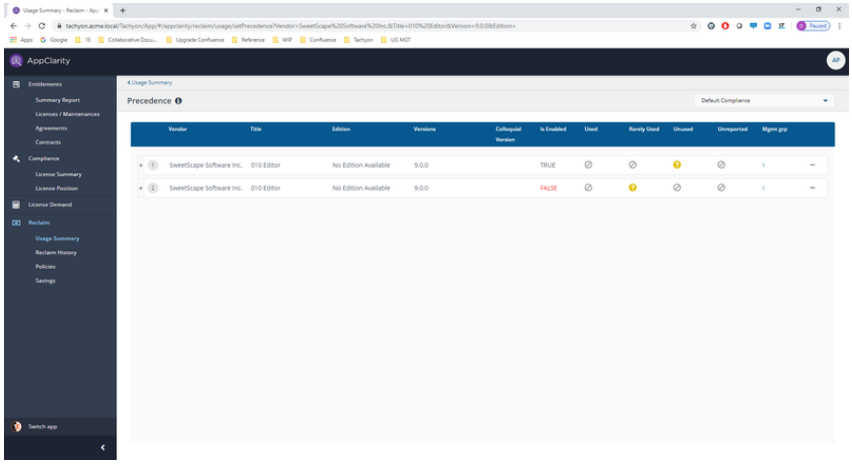
Used

Rarely Used

Unused

Unreported

Mgmt grp



10.6.5.4.1.1.1 Setting the precedence

This page lets you set the precedence for multiple policies that cover the same product. Initially this page will display the overlapping reclaim policies in the order they were created, with the most recently created having the lowest precedence. Policies at the top of the page have the highest precedence. Policies are considered in order from the top of the table to the bottom, and you can reorder the rows by clicking and dragging each row up or down. The way that the policies apply to specific products on specific devices are described in the following bullet points:

Just one of the reclaim policies shown on this page will be applied to a product, as defined by the **Matched Vendor**, **Matched Title**, **Editions** and versions for the policy, on any given device.

Whether a particular policy displayed in the list applies to that device also depends on the management group(s) the policy is active for.

If a device with a matching product belongs to more than one management group it will use the first policy it comes to that is active on one of its management groups.

Once the precedence is set, it triggers a **Reclaim Consolidation** report to make any necessary changes. You need to ensure you have identified which policy to set at the highest precedence, you can use the **Move to top** option from the 3 dots on the right side of the policy to do this.

> **Warning**
>
> When you subsequently publish a reclaim policy this will automatically change its precedence to be the lowest. i.e. it will appear at the bottom of the precedence list. Beware that simply viewing a page and clicking Publish to exit will reset that reclaim policy's precedence.

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Compliance Repository selector</td><td>This field lets you select the repository where the compliance data displayed on the page comes from. By default this is set to Default Compliance.

If you have created your own compliance repositories, click on the name to select these from the drop-down list.</td></tr>
<tr><td>Conflicting reclaim policies table</td><td>The following table describes the columns in the table that can be used to identify each conflicting policy:

<table>
<tr><th>Column</th><th>Description</th></tr>
<tr><td>Vendor</td><td>On the reclaim policy pages, this displays the vendor for the product the reclaim policy will be aimed at.</td></tr>
<tr><td>Title</td><td>On the reclaim policy pages, this displays the title for the product the reclaim policy will be aimed at.</td></tr>
<tr><td>Edition</td><td>On the reclaim pages in AppClarity an Editions column is sometimes displayed. This shows a list of editions that determine which products the reclaim policy will be aimed at.</td></tr>
<tr><td>Versions</td><td>The version portion of the vendor, title, version and edition attributes for the product that the reclaim policy applies to.</td></tr>
<tr><td>Colloquial Version</td><td>The colloquial version name for the product. For example, 2003, 2016 etc. This is an additional attribute to the vendor, title, version and edition for a software product that may identify a range of versions.</td></tr>
</table>
</td></tr>
</table>

Field	Description
Is Enabled	This column shows whether the **Enabled** checkbox has been set for the reclaim policy.
Used	Displays the action that will be taken by a reclaim policy for software with a usage category of used. Please refer to Usage categories for more details.
Rarely Used	Displays the action that will be taken by a reclaim policy for software with a usage category of rarely used. Please refer to Usage categories for more details.
Unused	Displays the action that will be taken by a reclaim policy for software with a usage category of unused. Please refer to Usage categories for more details.
Unreported	Displays the action that will be taken by a reclaim policy for software with a usage category of unreported. Please refer to Usage categories for more details.
Mgmt grp	This column contains a **Show** link, which displays a popup containing a list of the Management Group(s) the reclaim policy applies to.

10.6.5.4.2 Reclaim History page

A description of the fields on the **Reclaim History** page.

Here you can view the reclaim policies that have been published. You get to this page by clicking the **AppClarity→Reclaim→Reclaim History** node in the navigation panel.

The fields on the **Reclaim History** page are:

Management Group selector

Compliance Repository selector

Report Refresh

Column Picker

Action buttons

Export

Reclaim History table

Vendor

[Title]

[Version]

[Edition]

[Host Name]

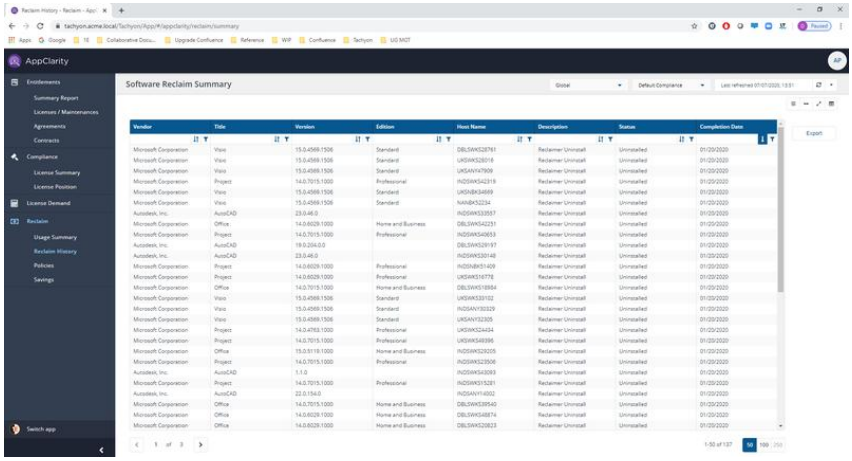
[Description]

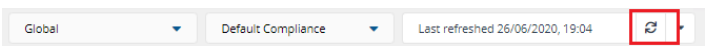
[Status]

[Completion Date]

[Column sort]

[Column filter]



Field	Description
Management Group selector	Certain pages in AppClarity have a management groups selector. This drop-down lets you select the management group you are interested in. By default this is set to **Global**.
Compliance Repository selector	This field lets you select the repository where the compliance data displayed on the page comes from. By default this is set to **Default Compliance**. If you have created your own compliance repositories, click on the name to select these from the drop-down list.
Report Refresh	You can refresh reports from individual AppClarity screens as well as using the Settings App. Where this is available you can do this by using the refresh icon next to the **Last Refreshed** box: 

Field	Description
Column Picker	**Using column picker**Where the column picker control is shown you can choose which columns are displayed. In the following example on the **Microsoft Core License Demand** page we hide the **Unknown Installs** column and move the **License Demand** column to the left of the page.To pick the displayed columns:Click on the Choose columns iconto the right of the header row to view the visible columns.To exclude **Unknown Installs**, select the Unknown Installs row and click **Exclude columns** button.The **Unknown Installs** column is now hidden.To move the **License Demand** column to the top of the list, hover your mouse over **License Demand** and using the direction control drag it to the top of the list.The Microsoft Core License Demand page has now been automatically updated with our changes.
Action buttons	The following table describes the action buttons displayed on the **Policies** page:

Button	Description
Export	Exports all the records currently displayed in the **Reclaim History** table as a TSV file. This button takes the filters currently applied to the table into account, but not the sorting or the current selection.

Reclaim History table

The following table describes the columns displayed in the **Reclaim History** table:

Column	Description
Vendor	On the reclaim policy pages, this displays the vendor for the product the reclaim policy will be aimed at.
Title	On the reclaim policy pages, this displays the title for the product the reclaim policy will be aimed at.
Version	The version portion of the vendor, title, version and edition attributes that are used to identify software products. For example, **11.0.3216.5614** or **6.3.100.0**.
Edition	On the reclaim pages in AppClarity an **Editions** column is sometimes displayed. This shows a list of editions that determine which products the reclaim policy will be aimed at.

Field	Description
Host Name	Displays the host name for the device where the software was reclaimed.
Description	Describes the action taken to reclaim the software.
Status	Shows the final state of the reclaim.
Completion Date	Displays the date the reclaim completed.

The following column actions are available on some table columns:

Column actions	Description
Column sort	Some tables contain column sorts that let you easily re-order the information displayed in the table.**Using column sorts**The picture opposite shows an example taken from AppClarity. In our example we want to sort the table on the **Cost** column from the highest cost at the top to the lowest at the bottom. To sort the table on the **Cost** column:Click on the sort iconjust beneath the header row in the **Cost** column.The sort popup is displayed.Now select the sort direction. In our example this will be **Sort descending**.After selecting this the data in the table is now sorted on the **Cost** column from highest to lowest and the sort icon has changed to a sort descending icon**Clearing the sort**You can clear the sort by clicking on the sort icon again and selecting the **Clear sorting** menu item from the sorting popup.
Column filter	Some tables contain a column filter that lets you easily filter the information displayed in the table.**Using column filters**The picture opposite shows an example taken from AppClarity. In our example we want to filter the table to show only those items where the **Edition** contains the text **Prof**.To filter the table on the **Edition** column:Click on the filter iconjust beneath the header row in the **Edition** column.The filter popup is displayed.Now select the operator. In our example this will be **contains**.Then type the text **Prof** into the text field.Click **Apply** and a new filter will be added to the table.The table will be filtered to just those items whose **Edition** contains the text **Prof**.**Adding another filter**You can add another filter by clicking on the filter icon for any of the columns. The picture opposite

Field	Description
	shows another filter added selecting table rows where the **Type** also contains the text **License**. The table will also be filtered accordingly.**Removing filters**You can remove filters by clicking on the filter close icon at the end of the filter.

10.6.5.4.3 Policies page

A description of the fields on the **Policies** page.

Here you can view the reclaim policies that have been published. You get to this page by clicking the **AppClarity**→**Reclaim**→**Policies** node in the navigation panel.

The fields on the **Policies** page are:

Compliance Repository selector

Report Refresh

Active Policies Only toggle

Column Picker

Action buttons

New Policy

Edit

Publish

Clone

Move to Draft

Delete

Manage Associations

Export

Policies table

Vendor

Title

Version

Colloquial Version

Edition

Is Enabled

Used

Rarely Used

Unused

Unreported

Admin Actions

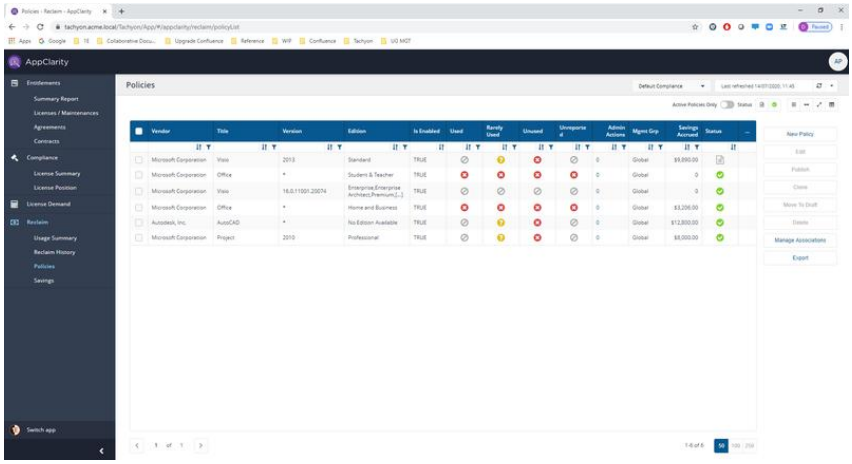
SCCM Collection Type

Savings Accrued

Status

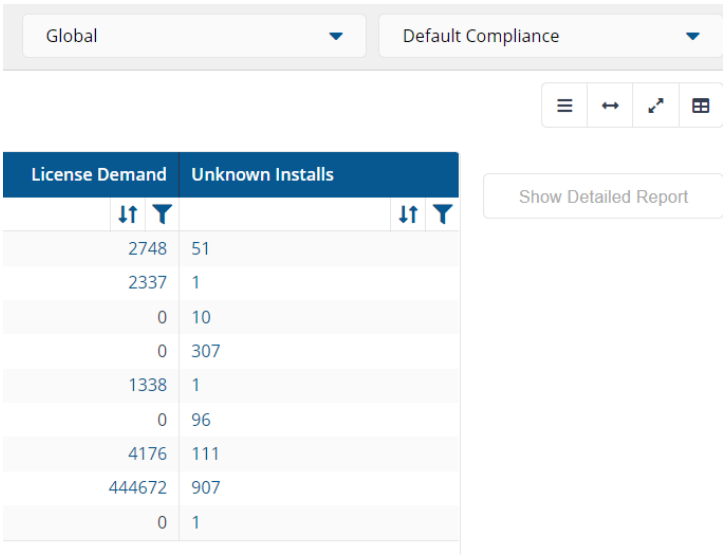
Column sort

Column filter



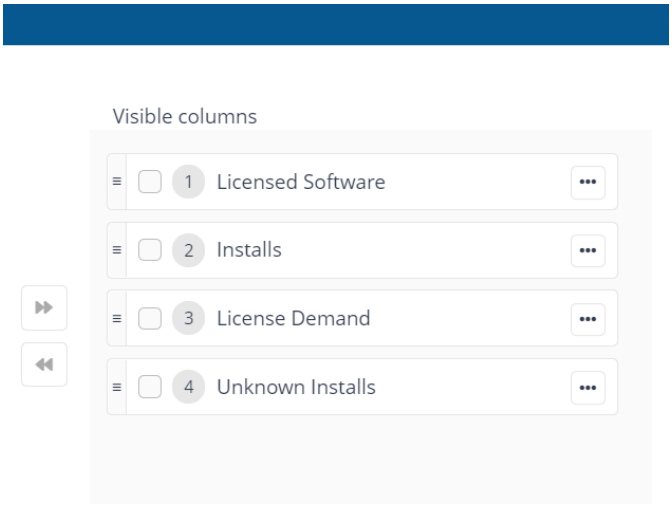
Field	Description
Compliance Repository selector	This field lets you select the repository where the compliance data displayed on the page comes from. By default this is set to **Default Compliance**. If you have created your own compliance repositories, click on the name to select these from the drop-down list.
Report Refresh	You can refresh reports from individual AppClarity screens as well as using the Settings App. Where this is available you can do this by using the refresh icon next to the **Last Refreshed** box:

Field	Description
Active Policies Only toggle	The **Active Policies Only** toggle adds a filter when it's turned on that filters the table to only display the reclaim policies that have been published and their status is set to enabled.
Column Picker	Where the column picker control is shown you can choose which columns are displayed. In the following example on the **Microsoft Core License Demand** page we hide the **Unknown Installs** column and move the **License Demand** column to the left of the page.



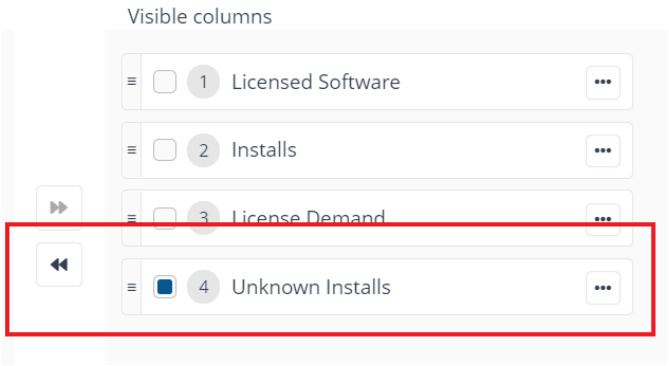
To pick the displayed columns:

Click on the Choose columns icon to the right of the header row to view the visible columns.

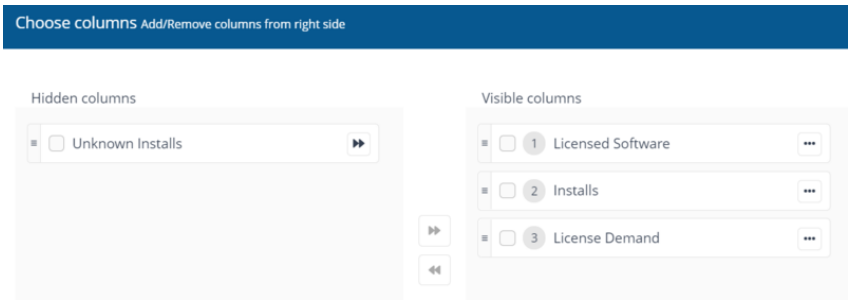


Field	Description

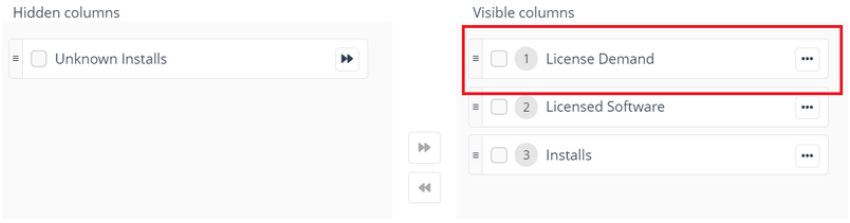
To exclude **Unknown Installs**, select the Unknown Installs row and click **Exclude columns** button.



The **Unknown Installs** column is now hidden.



To move the **License Demand** column to the top of the list, hover your mouse over **License Demand** and using the direction control drag it to the top of the list.



The Microsoft Core License Demand page has now been automatically updated with our changes.

Field	Description

License Demand	Licensed Software	Installs
2748	Windows Server DataCenter	647
2337	SQL Server Enterprise	649
0	SQL Server Analysis Services	0
0	SQL Server Integration Services	0
1338	SQL Server Standard	300
0	SQL Server Reporting Services	0
4176	Windows Server Enterprise	265
444672	Windows Server Standard	4019
0	SQL Server Data Quality Services	0

Action buttons

The following table describes the action buttons displayed on the **Policies** page:

Button	Description
New Policy	Creates a new policy. Please refer to New Policy page for more details.
Edit	This button is only enabled when there is a single selection in the Policies table. Edits the selected policy and opens the Edit Policy page. Please refer to New Policy page for more details.
Publish	This button is enabled when there is at least one selection in the **Policies** table. Publishes the selected policies.
Clone	This button is only enabled when there is a single selection in the **Policies** table. Clones the selected policy and opens the Edit Policy page with a clone of the details from the policy. Please refer to New Policy page for more details.
Move to Draft	This button is enabled when there is at least one selection in the **Policies** table. Moves the selected policies to Draft.
Delete	This button is enabled when there is at least one selection in the **Policies** table. Deletes the selected policies.

Field	Description	
	Manage Associations	Clicking this link navigates to **Inventory→Manage Associations→Product to CM** page in the Inventory application.
	Export	Exports all the policies currently displayed in the **Policies** table as a TSV file. This button takes the filters currently applied to the table into account, but not the sorting or the current selection.

Policies table

The following table describes the columns displayed in the **Policies** table:

Column	Description
Vendor	On the reclaim policy pages, this displays the vendor for the product the reclaim policy will be aimed at.
Title	On the reclaim policy pages, this displays the title for the product the reclaim policy will be aimed at.
Version	The version portion of the vendor, title, version and edition attributes that are used to identify software products. For example, **11.0.3216.5614** or **6.3.100.0**.
Colloquial Version	The colloquial version name for the product. For example, **2003**, **2016** etc. This is an additional attribute to the vendor, title, version and edition for a software product that may identify a range of versions.
Edition	On the reclaim pages in AppClarity an **Editions** column is sometimes displayed. This shows a list of editions that determine which products the reclaim policy will be aimed at.
Is Enabled	This column shows whether the **Enabled** checkbox has been set for the reclaim policy.
Used	Displays the action that will be taken by a reclaim policy for software with a usage category of used. Please refer to Usage categories for more details.

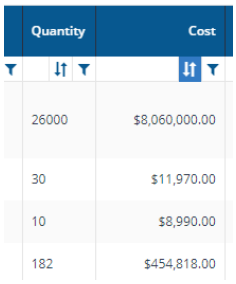
Field	Description
Rarely Used	Displays the action that will be taken by a reclaim policy for software with a usage category of rarely used. Please refer to Usage categories for more details.
Unused	Displays the action that will be taken by a reclaim policy for software with a usage category of unused. Please refer to Usage categories for more details.
Unreported	Displays the action that will be taken by a reclaim policy for software with a usage category of unreported. Please refer to Usage categories for more details.
Admin Actions	This link takes you to the Administration page for the reclaim policy. From there you can monitor the progress of the reclaim and respond to any end-user requests to opt-out of optional reclaim policies.
Mgmt Grp	Displays the Management Group the policy is associated with.
SCCM Collection Type	Displays the Configuration Manager collection type that will be used to manage the reclaims.
Savings Accrued	Displays the savings accrued to date as a result of running the reclaim policy.
Status	Indicates whether the policy is in published or draft state.

The following column actions are available on some table columns:

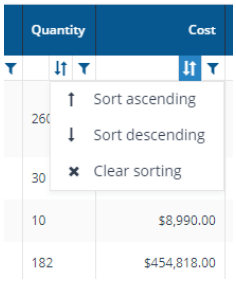
Column actions	Description
Column sort	**Using column sorts** The picture opposite shows an example taken from AppClarity. In our example we want to sort the table on the **Cost** column from the highest cost at the top to the lowest at the bottom. To sort the table on the **Cost** column:

Field	Description

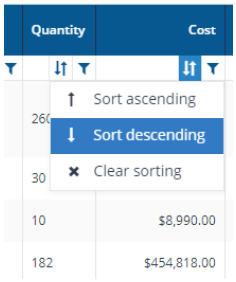
Click on the sort icon ⇅ just beneath the header row in the **Cost** column.



The sort popup is displayed.

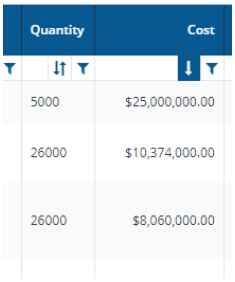


Now select the sort direction. In our example this will be **Sort descending**.



After selecting this the data in the table is now sorted on the **Cost** column from highest to lowest and the sort icon has changed to a sort descending icon ⬇

Field	Description



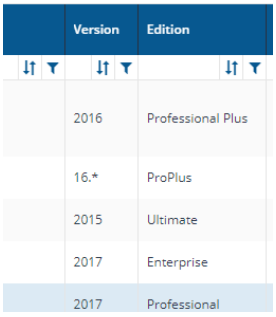
Clearing the sort

You can clear the sort by clicking on the sort icon again and selecting the **Clear sorting** menu item from the sorting popup.

Column filter

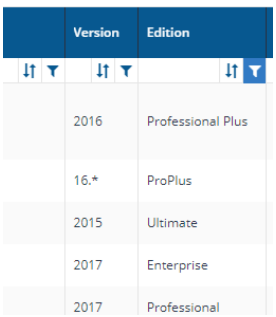
Using column filters

The picture opposite shows an example taken from AppClarity. In our example we want to filter the table to show only those items where the **Edition** contains the text **Prof**.



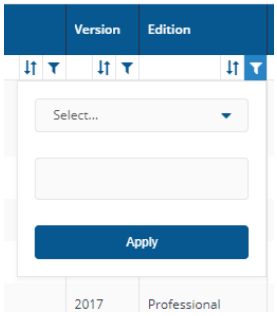
To filter the table on the **Edition** column:

Click on the filter icon just beneath the header row in the **Edition** column.

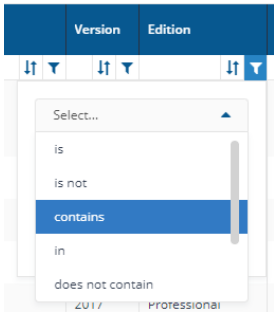


The filter popup is displayed.

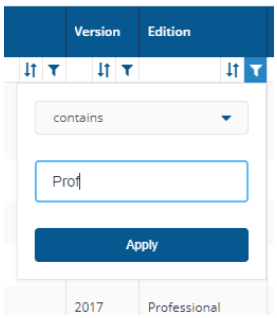
Field	Description



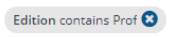
Now select the operator. In our example this will be **contains**.



Then type the text **Prof** into the text field.

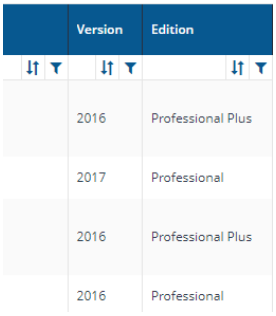


Click **Apply** and a new filter will be added to the table.



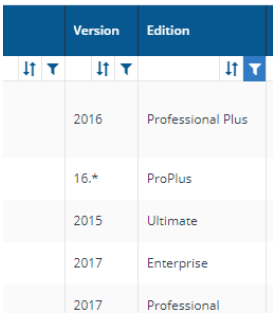
The table will be filtered to just those items whose **Edition** contains the text **Prof**.

Field	Description



Adding another filter

You can add another filter by clicking on the filter icon for any of the columns. The picture opposite shows another filter added selecting table rows where the **Type** also contains the text **License**. The table will also be filtered accordingly.



Removing filters

You can remove filters by clicking on the filter close icon at the end of the filter.

10.6.5.4.3.1 New Policy page

A description of the fields on the **Reclaim Policies** page.

Here you can create a Reclaim Policy for a specific product. You get to this page by any of the following ways:

Clicking the **Reclaim→Policies** node in the navigation panel, then clicking the **New Policy** button

Clicking on the **Add Policy** button on the side of a product entry in the Usage Summary page. If this method is selected the page will be pre-filled with the details of the product.

Clicking on the **Edit** button on the Policies page. When this is done the **Reclaim Policy** page will be pre-filled with the contents of the selected reclaim policy.

Clicking on the **Clone** link on the Policies page. When this is done the **Reclaim Policy** page will be pre-filled with the contents of the selected reclaim policy and when you subsequently click **Draft** or **Publish** a copy of the original reclaim policy will be saved including any changes you have made.

The fields on the **Reclaim Policy** page are:

Policy Summary

Basic Information

Product

Version Expansion

Uninstall Criteria

Basic Information

Management Group

Global

Override Allowed

Enabled

Product

Vendor

Title

Edition

Colloquial Version

Version Expansion

Versions

Version Expansion

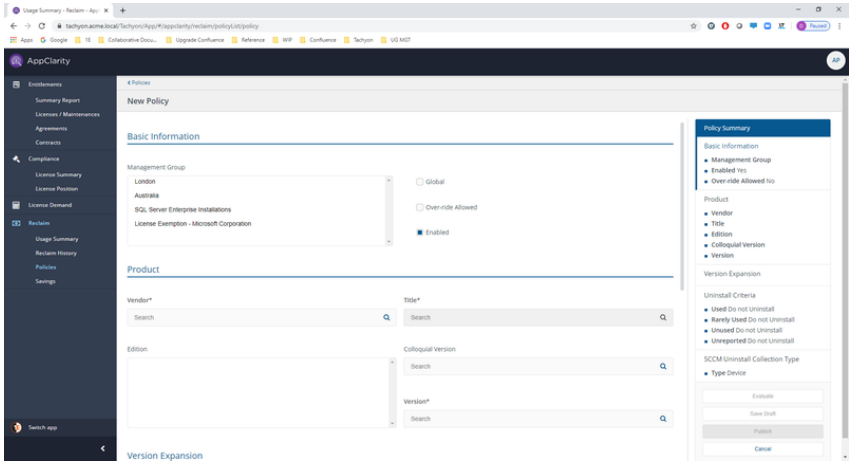
Evaluate

Save draft

Publish

Cancel

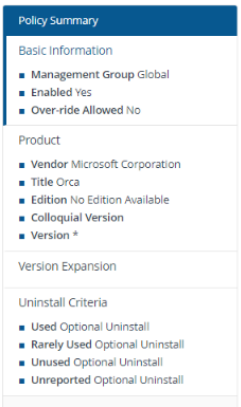
SCCM Uninstall Collection Type



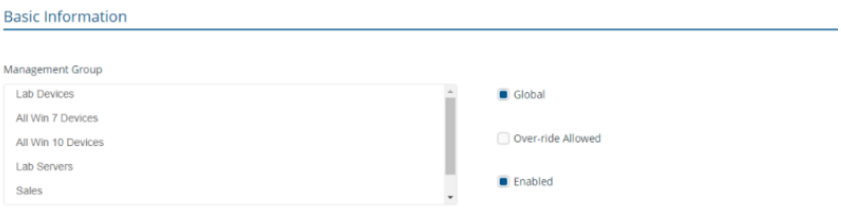
10.6.5.4.3.1.1 Policy Summary

This table to the right shows you the information about the policy as you are building the policy or if you are editing a policy. This is useful because the policy pane is larger than can be seen on one screen. Each of these sections are hyperlinks to that specific area of the policy page.

Field	Description
Basic Information	Details about the Management Group, if the policy is enabled and if Over-ride is allowed
Product	Give Vendor, Title, Edition, Colloquial Version and Version for the software in the policy
Version Expansion	No details here, just a hyperlink to the Version Expansion area
Uninstall Criteria	Details each usage category and the action that Reclaimer will take

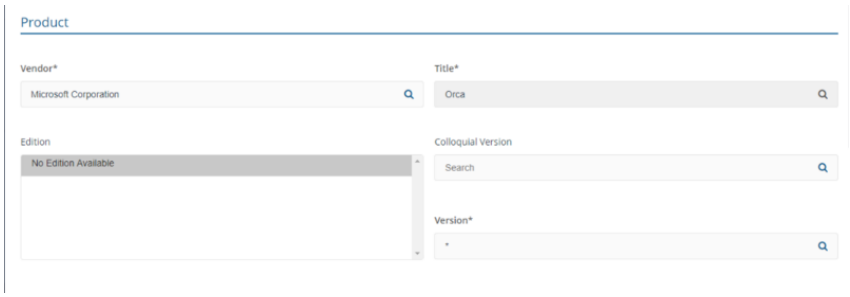


10.6.5.4.3.1.2 Basic Information



Field	Description
Management Group	This field displays a list of the current management groups, you can select all the management groups that you want this reclaim policy to apply to. You must select at least one management group or set the reclaim policy to global.
Global	This checkbox determines whether the reclaim policy will be applied to all products matching the vendor, title, version and edition information regardless of which management groups they belong to.
Override Allowed	This checkbox is only displayed when the **Global** checkbox has been checked. When **Override Allowed** is checked: Subsequent reclaim policies for the same product can be defined in global and other management groups. Those policies will be warned on publishing that a similar policy is already present. When**Override Allowed**is unchecked: Subsequent reclaim policies for the same product can still be published in global. Those policies will be warned on publishing that a similar policy is already present. However, subsequent reclaim policies for the same product cannot be published in other management groups. Those policies will notified that asimilar policy for Global is already present which cannot be overridden and the publish will not be allowed to continue.
Enabled	This checkbox determines whether the policy is enabled or not, even if it is published. You can use this to disable policies that are no longer in use, or re-enable policies that have been disabled previously.

10.6.5.4.3.1.3 Product

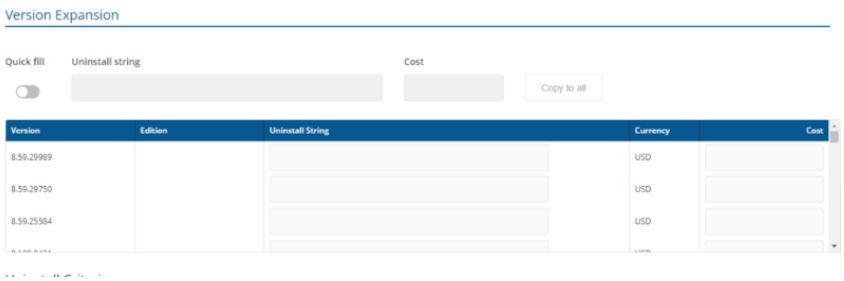


Field	Description
Vendor	The vendor part of the vendor, title, version and edition for a product. This must be filled out before any other fields. Suggested suitable vendors that match your text are displayed as you type into the field, which you can select to auto-complete the entry.
Title	The title part of the vendor, title, version and edition for a product. Suggested suitable titles from the selected vendor that match your text are displayed as you type into the field, which you can select to auto-complete the entry.
Edition	Sets the edition for the product to be reclaimed. This field displays a list of editions that match the selected **Vendor** and **Title** fields. **Note** You must ensure that you select at least one edition from the**Edition**list. If the list shows**No edition available**, then you must ensure that you select that option.
Colloquial Version	This field is optional and sets the colloquial version for the product to be reclaimed.

Note

When manually entering the information on the **Reclaim Policy** page you must enter the values in the order they are presented, as each subsequent field is dependent on the fields above it.

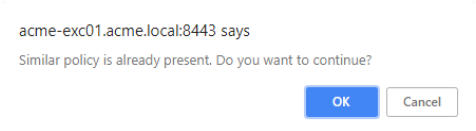
10.6.5.4.3.1.4 Version Expansion



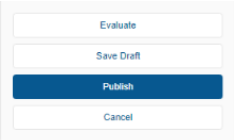
Field	Description
Versions	Here you select the versions of the software you want the reclaim policy to apply to. Enter a value and then select one from the list of versions displayed. This is taken into account in addition to the vendor, title and edition. This field accepts the asterisk character * as a wildcard. For example. This field could be set to: * to specify all versions for the selected vendor, title and edition. 11.* to specify all sub-versions of version 11. 11.0.* to specify all sub-sub-versions of 11.0 and so on.
Version Expansion	This field will expand all the individual matching versions for the vendor, title, edition and version. The expansion is done according to the wildcards in the **Versions** string: If that string contains no wildcards the **Version Expansion** field will contain a single entry for that specific version. If the **Versions** string contains just an asterisk ***** then the **Version Expansion** field will contain all the versions for the selected vendor, title and edition. If the **Versions** string contains a number followed by *****, for example **11.***, then the **Version Expansion** field will contain all the versions starting with that number and so on. There are four fields for each matching version row displayed in the **Version Expansion** field, as described in the following table:

Field	Description
Version	The expanded version number for this row

Field	Description
Edition	The matching edition for the vendor, title and version
Uninstall String	This string can be used if the version requires a custom uninstall string. **Note** The quick fill can be used to populate all uninstall strings and cost with the same information. If the no custom uninstall string is required leave this field blank.
Currency	The currency for the cost. Default is US Dollar.
Cost	The estimated cost savings that would be made by retrieving the license covered by this reclaim.

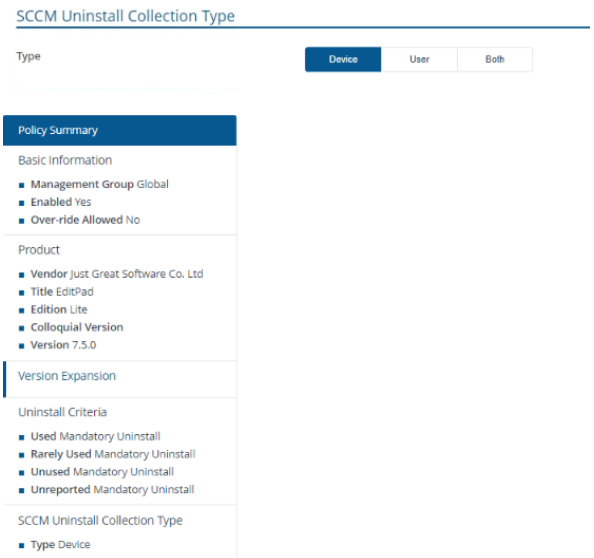
Field	Description
Evaluate	Click this button to run the evaluation report for the reclaim policy to see which devices and software installations would be affected by the policy. Clicking this button creates a report that is downloaded by the browser as a TSV file. **Note** You may need to enable popups on the Tachyon site to enable the download to proceed.
Save draft	Click this button if want to save a copy of the policy you are currently working on. Clicking this button does not close the **Reclaim Policy** page.
Publish	Click this button to publish the policy. **Note** When you publish the policy a check will be made to see if it overlaps with any other existing policy. If it does, you will see a popup similar to the following: 

Field	Description
	If you decide to proceed with the publishing you will subsequently need to set the precedence for the policies to decide which one should be preferred. This is done on the Precedence page but can only be done for live policies. This means that you will have to refresh the **reclaim consolidation** report first, which can be done from the Policies page.
Cancel	Click this button to leave without making any changes to the policy.



10.6.5.4.3.1.5 SCCM Uninstall Collection Type

When you have the SCCM Uninstall Provider configured you are presented with an additional section in your Policy Summary. This will allow the Reclaimer to use the SCCM Uninstall for the Reclaimer. The Reclaimer will create a device collection, a user collection or one of each. Based on the setting in the picture below (from the policy). When the Reclaimer runs either the device or the user or both is added to the collection. The Reclaimer also creates deployments for the Program or the Application model for the uninstallation.



10.6.5.4.3.2 Administration page

A description of the fields on the reclaim policy **Adminstration** page.

Here you can view the current progress and status for the selected reclaim policy. You get to this page by clicking the **AppClarity**→**Reclaim**→**Policies** node in the navigation panel and then clicking on the **Number** link in the **Admin Actions** column.

The fields on the **Administration** page are:

Report Refresh

Vendor

Title

Reclaims completed under this policy

User rejected

Failed

Succeeded

Reclaims in progress for this policy

Optional

Mandatory

Reclaim Override Management

Domain Name

Host Name

Edition

Version

Colloquial Version

Click User

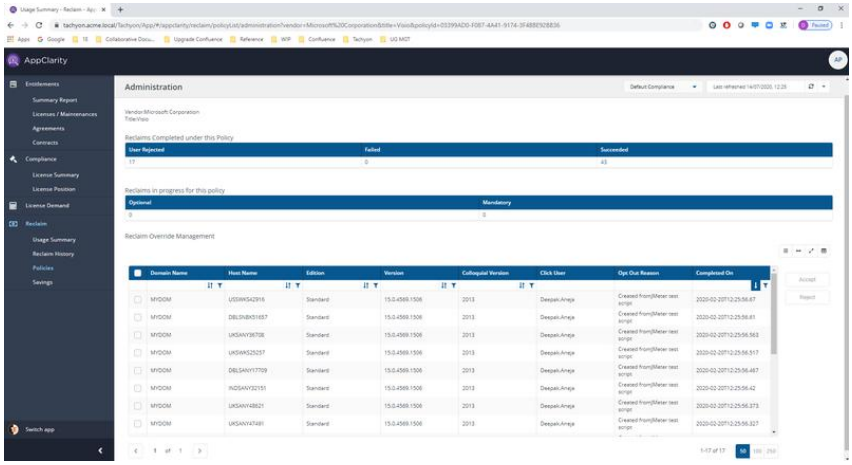
Opt Out Reason

Completed On

Accept

Reject

Column Picker



Field	Description
Report Refresh	You can refresh reports from individual AppClarity screens as well as using the Settings App. Where this is available you can do this by using the refresh icon next to the **Last Refreshed** box:
Vendor	Displays the vendor for the target product related to the selected reclaim policy
Title	Displays the software title for the target product related to the selected reclaim policy
Reclaims completed under this policy	This table shows the reclaims that have been completed by this reclaim policy. The columns of the table are as follows: **Column** — **Description** **User rejected** — Shows the number of reclaims where the user has requested to keep the product. **Failed** — Shows the number of reclaims where the attempt to uninstall the software failed. **Succeeded** — Shows the number of reclaims where the software was successfully uninstalled.

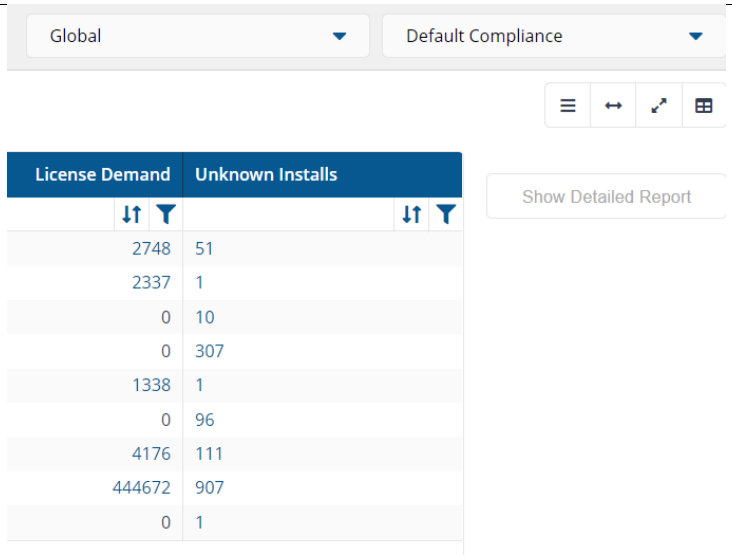
Field	Description
Reclaims in progress for this policy	This table shows the number of reclaims currently in progress for this reclaim policy. The columns of the table are as follows: **Optional** — Shows the number of reclaim policies currently under way that allow the end-user to opt out of the reclaim. **Mandatory** — Shows the number of reclaim policies currently under way where the software will be uninstalled without end-user interaction.
Reclaim Override Management	This table shows the reclaims that must be processed by the administrator. This is where the user has opted to keep the software and provided a suitable reason for it and that reason must be approved or rejected by the administrator. The columns of the table are as follows: **Domain Name** — The domain name for the target device. **Host Name** — The host name for the target device. **Edition** — The edition of the software being reclaimed. **Version** — The version of the software being reclaimed. **Colloquial Version** — The colloquial version of the software being reclaimed (if any). **Click User** — The end-user who requested to keep the software. **Opt Out Reason** — The reason given by the end-user why they should be allowed to keep the software. **Completed On** — The time and date the administrator responded.

Field	Description
	There are also two buttons below the table that determine the action to take on the selected rows in the table: Button — Description **Accept** — Clicking this means that the administrator has approved the end-user's reasons for keeping the software. The reclaim will not go ahead and the end-user will retain the software. **Reject** — Clicking this means that the administrator has rejected the end-user's reasons for keeping the software. The reclaim will be changed to mandatory and the software will be removed without any further end-user interaction.

The three buttons above Accept and Reject

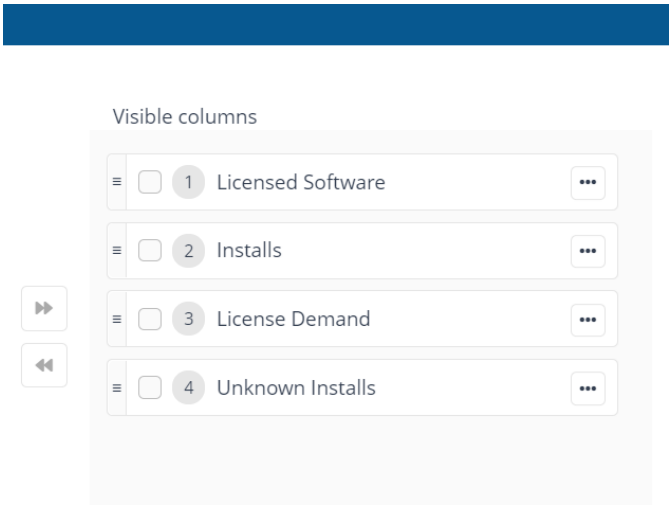
Icon	Name	Description
	Toggle compact rows	Allows the rows to have slightly more space for easier viewing.
	Toggle action buttons	Allows the action buttons (Accept and Reject) to be displayed as a hamburger menu only. This expansion of the table allows for easier viewing.
	View fullscreen	Allows the table only to be viewed in the full browser window. Clicking the button while in fullscreen mode will collapse it back to default.
	Column Picker	Where the column picker control is shown you can choose which columns are displayed. In the following example on the **Microsoft Core License Demand** page we hide the **Unknown Installs** column and move the **License Demand** column to the left of the page.

Icon	Name	Description



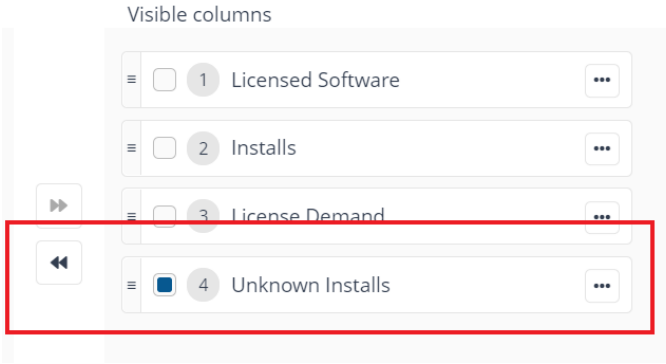
To pick the displayed columns:

Click on the Choose columns icon to the right of the header row to view the visible columns.

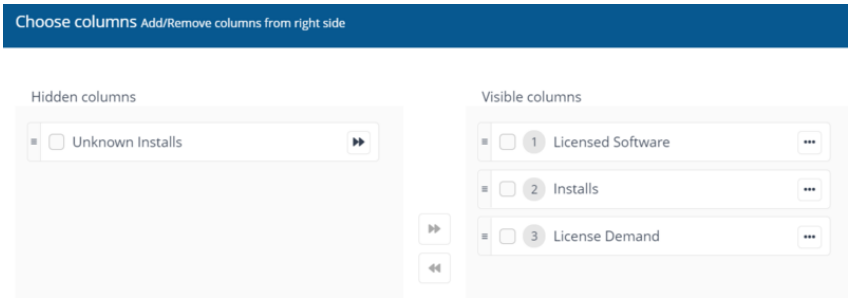


To exclude **Unknown Installs**, select the Unknown Installs row and click **Exclude columns** button.

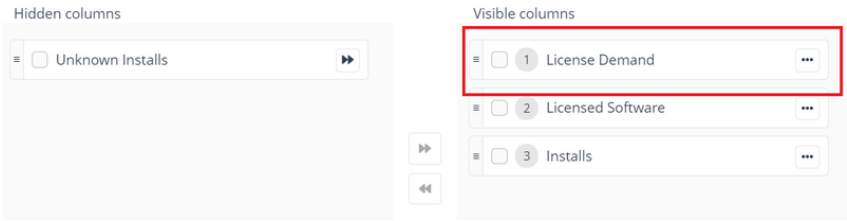
Icon	Name	Description



The **Unknown Installs** column is now hidden.



To move the **License Demand** column to the top of the list, hover your mouse over **License Demand** and using the direction control drag it to the top of the list.



The Microsoft Core License Demand page has now been automatically updated with our changes.

License Demand	Licensed Software	Installs
2748	Windows Server DataCenter	647
2337	SQL Server Enterprise	649
0	SQL Server Analysis Services	0
0	SQL Server Integration Services	0
1338	SQL Server Standard	300
0	SQL Server Reporting Services	0
4176	Windows Server Enterprise	265
444672	Windows Server Standard	4019
0	SQL Server Data Quality Services	0

10.6.5.4.4 Savings page

A description of the fields on the **Savings** page.

Here you can review an estimate of the cost savings made by applying particular reclaim policies, that is, on successful reclaims. You get to this page by clicking the **AppClarity→Reclaim→Savings** node in the navigation panel.

> **Note**
>
> Please Execute a**Generate Report - Reclaim Reporting**action for your compliance repository, before viewing this screen.

The fields on the **Savings** page are:

Management Groups

Compliance repository selector

Report Refresh

Back

Column Picker

Export All

Savings table

Vendor

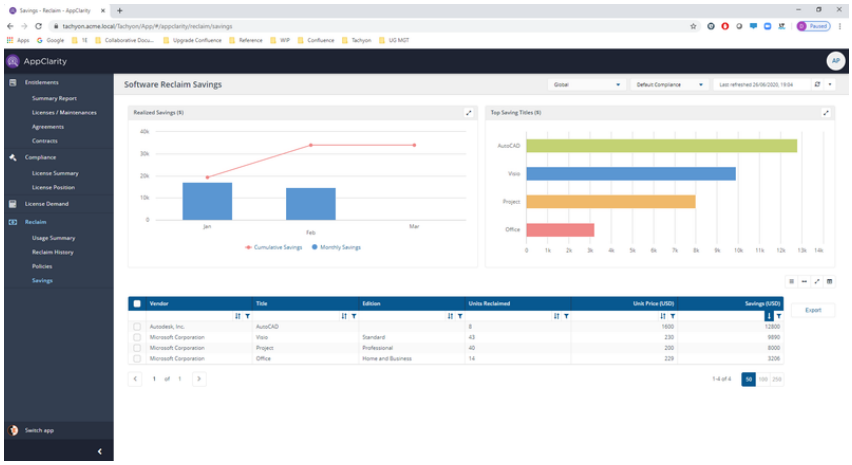
Title

Edition

Units Reclaimed

Unit Price (USD)

Savings (USD)



Field	Description
Management Groups	Certain pages in AppClarity have a management groups selector. This drop-down lets you select the management group you are interested in. By default this is set to **Global**.
Compliance repository selector	This field lets you select the repository where the compliance data displayed on the page comes from. By default this is set to **Default Compliance**. If you have created your own compliance repositories, click on the name to select these from the drop-down list.
Report Refresh	You can refresh reports from individual AppClarity screens as well as using the Settings App. Where this is available you can do this by using the refresh icon next to the **Last Refreshed** box:
Back	Each page in AppClarity has a back link on the page. Clicking this link takes you back to the previous page you were browsing, and works differently to the browser's back button for this application in that it takes you to the last page you were on in the application.
Column Picker	**Using column picker**Where the column picker control is shown you can choose which columns are displayed. In the following example on the **Microsoft Core License Demand** page we hide the **Unknown Installs** column and move the **License Demand** column to the left of the page.To pick the displayed columns:Click on the Choose columns iconto the right of the header row to view the visible columns.To exclude **Unknown Installs**, select the Unknown Installs row and click **Exclude columns** button.The **Unknown Installs** column is now hidden.To move the **License Demand** column to the top of the list, hover your mouse over **License Demand** and using the direction control drag it to the top of the list.The Microsoft Core License Demand page has now been automatically updated with our changes.
Export All	Pages in AppClarity that include an **Export all** button allow you to export all the data for any tables of information displayed on the page. This may also include columns that are not currently visible in the table display. Click this button to export all of the software reclaim summary details.
Savings table	The **Savings** table contains the following columns:

Field	Description

Column	Description
Vendor	The vendor portion of the vendor, title, version and edition attributes that are used to identify which software product the reclaim policy was applied to.
Title	The title portion of the vendor, title, version and edition attributes that are used to identify which software product the reclaim policy was applied to.
Edition	The edition portion of the vendor, title, version and edition attributes that are used to identify which software product the reclaim policy was applied to.
Units Reclaimed	A count of the number of reclaims performed by applying this policy.
Unit Price (USD)	Shows the unit price in USD for the product associated with the policy.
Savings (USD)	The sum of the estimated savings made by applying this reclaim policy.

10.6.6 Usage categories

Definitions of the four usage categories in the Product Usage report.

Please refer to 1E platform - Usage categories for details.

10.6.7 Entitlement import files

Definitions of each type of record that may be imported into an AppClarity entitlement repository.

The following tables show each category, sub-category, and the record types that can be imported. The 11 sub-categories are visible as tabs in the home page of an entitlement repository.

> **Note**
>
> The **Manual upload**feature available in AppClarity 6.1 no longer exists in AppClarity 7.x . When importing entitlements you must use the Entitlement.tsv connector.

Entitlement information is managed using various fields, in 11 sub-categories (one of which is not used), which map directly to columns in a import file. **TSV** and **CSV** files are both supported, but the documentation here refers to **TSV**.

Import files must have the following:

All columns must have column headings

Column headings must not have spaces

The Version column must be named Version and not Version/Number as it did in some older export files

Please note the following:

When using a simple editor like notepad ensure you leave the tab/comma delimiters between headings

Any column heading with an incorrect name is ignored; this allows additional columns to be used as notes or extra information

Columns can be in any order; it may help you to standardize on the column order listed below

In the tables below, mandatory means the column and value are expected. If a mandatory column or value is omitted you will see caveats reported

Ensure date formats are correct. When editing a file using Excel, the date columns should have their number format set as**Text**instead of**Date**, otherwise you will see integers instead of dates when saved as a TSV/CSV file.**Text**ensures that whatever you type will remain unchanged.

Note

Use the ISO 8601 date format for date fields: **yyyy/mm/dd** or **yyyy-mm-dd**

When exporting dates from other SQL servers, the format may be different due to the region settings of the source server, for example **mm-dd-yyyy** for English (US). To ensure dates are imported correctly, changing the data format to ISO 8601 is recommended, or you should ensure the SQL Server instance hosting the AppClarity database uses the same or equivalent region settings. In most cases SQL Server will intelligently convert dates, but you should review your imports to be sure.

Tip

You should test your system with a few test entitlements before you do any bulk imports.

10.6.7.1 Base Entitlement (1)

Column	Mandatory	Default if not specified	Datatype	Notes
EntitlementId	No	Auto-generated GUID	String	Identity id of this entitlement. This is auto-generated as a GUID if this entitlement was created in the user-interface.

Column	Mandatory	Default if not specified	Datatype	Notes
ParentEntitlementId	No		String	Identity id of the parent entitlement linked to this entitlement. This is auto-generated as a GUID if this entitlement was created in the user-interface, and it is linked to a parent Entitlement. If **ParentEntitlementId** is specified, then you must have a matching **EntitlementId** earlier in the import file, or you already know the **EntitlementId** has been imported previously. From AppClarity 8.1 an entitlement can only have one parent or none. When exporting from AppClarity 5.2, if any entitlement has multiple parents then only one will be used, and the ParentEntitlementId of the others will exported into the comments column, and appear in the

Column	Mandatory	Default if not specified	Datatype	Notes
				comments field when imported into AppClarity 8.1. **Warning** Finding the **EntitlementId** from the database or UI is not supported currently.
EntitlementType	Yes		String	Valid values are: **License** **Maintenance Agreement** Once imported it can not be changed.
Identifier	No		String	Appears in pages as **Custom identifier**. Enter any alphanumeric text that will help identify the entitlement.
LicenseType	No	**Perpetual** for **License** and **Maintenance**.	String	Valid values are: **Perpetual** **Subscription**

Column	Mandatory	Default if not specified	Datatype	Notes
		NA for **Agreement**.		Agreement is always '**NA**'
StartDate	No	Calulated as EndDate - DurationInMonths for **Agreements** and **Subscription**. If neither is set then today's date. If DurationInMonths is not set, then 12 is the default. Today's date for **Perpetual**.	Date	When the entitlement starts applying.
EndDate	Yes/no depending on other fields.	Calculated as StartDate + DurationInMonths for **Agreements** and **Subscription**. If DurationInMonths is not set then 12 is the default. It is set only for **Agreements**	Date	This is last date of entitlement.

Column	Mandatory	Default if not specified	Datatype	Notes
		and **Subscription**.		
DurationInMonths	No	Calculated as EndDate - StartDate. If either of these are missing then 12 is the default. It is set only for **Agreements** and **Subscription**.	Decimal	For how long the entitlement is applicable after start date. For example, if start date if Jan 14, 2016 and Durationmonths is 24 months then end date would be Jan 14, 2018
ProductSKU	No		String	Product SKU
IsEntitlementProduct	No	FALSE	Boolean	Is the entitlement entered an SKU based from Catalog
Vendor	Yes if ProductSKU is not present for **License** and **Maintenance**. Yes for **Agreement**.		String	Vendor. The name of product Vendor.
Title	Yes if ProductSKU is not present for **License** and **Maintenance**. No for **Agreement**.		String	For license and maintenance pages, this is Product title; the name of the product.

Column	Mandatory	Default if not specified	Datatype	Notes
				For agreement page, this is Name.
Version	No		String	For license and maintenance pages, this is Version; the version of product. Version can be given in any format depending on chosen Version Type. For agreement page, this is Number.
VersionType	No	AllVersions	String	AllVersions DotFormat Colloquial NA - Agreements are always 'NA'
Edition	Yes if ProductSKU is not present for **License** and **Maintenance**. No for **Agreement**.		String	Edition. The name of product edition.
IsEditionBased	No	FALSE	Boolean	If edition is available then True otherwise False.
IsRenewal	No	FALSE	Boolean	Entitlement types that needs to be

Column	Mandatory	Default if not specified	Datatype	Notes
				renewed (has an end date).
IsUpgrade	No	FALSE	Boolean	This specifies rights, if upgrade rights are allowed.
IsQuantityUnlimited	No	FALSE	Boolean	If the number of licenses purchased is unlimited then True otherwise False. If True then Quantity is ignored.
Quantity	Yes if IsQuantityUnlimited is FALSE for **License** and **Maintenance**. No for **Agreement**.		Integer	Number of licenses purchased.
MetricType	No	Device	String	Valid values are: Device Processor Core PVU Other Agreement is always 'NA'
OtherMetric	No		String	Used only if Metric Type is 'Other'
IsVersionUpgradeRight	No	TRUE	Boolean	Whether the entitlement is

Column	Mandatory	Default if not specified	Datatype	Notes
				applicable on the later versions of chosen product version. Only applicable, and automatically enabled, if Vendor is Microsoft Corporation, and SA is selected.
IsVersionUpgradeRightPersistent	No	TRUE	Boolean	Version upgrade persists after maintenance is expired. If this right is False, then the license rights resets back to original version at the time of purchase of perpetual license when maintenance expires. Only applicable, and automatically enabled, Vendor is Microsoft Corporation, and SA is selected.
IsVersionDowngradeRight	No	FALSE	Boolean	Whether the entitlement is applicable on the previous versions of chosen product version. By default these rights are active

Column	Mandatory	Default if not specified	Datatype	Notes
IsVersionDowngradeRightPersistent	No	FALSE	Boolean	Version downgrade persists after maintenance is expired. If this right is False, then the license rights resets back to original version at the time of purchase of perpetual license when maintenance expires.
IsEditionDowngradeRight	No	FALSE	Boolean	Whether the entitlement is applicable on the previous editions of chosen product edition.
IsEditionDowngradeRightPersistent	No	FALSE	Boolean	Edition downgrade persists after maintenance is expired. If this right is False, then the license rights resets back to original edition at the time of purchase of perpetual license when maintenance expires.
IsMultiInstanceRight	No	FALSE	Boolean	Whether the same license is applicable on multiple installations.
IsSoftwareAssurance	No	FALSE	Boolean	SA is applicable only for Microsoft

Column	Mandatory	Default if not specified	Datatype	Notes
				Corporation products. On selecting SA Version upgrade rights are automatically set to True.
SecondaryUseCountRight	No	FALSE	Boolean/ Int	This refers to the use right to allow users to use same product on their second device free of cost (example one office desktop and one home laptop) with their single device-based license
Currency	No	USD	3 chars	ISO 4217 currency code. The code must match one of the codes already existing in the database. Please contact 1E if you need to add additional codes to the database. Code Symbol USD $ EUR € GBP £ JPY ¥

Column	Mandatory	Default if not specified	Datatype	Notes
				CAD C$ AUD A$ CNY ¥ CHF Fr. SGD S$ HKD HK$ ZAR R$
UnitCost	No	0	Decimal	Cost of licence per unit
TotalCost	Yes for **Agreement**.	For **License** and **Maintenance**, the value is automatically calculated if Unit Cost Type is **OnceOff**, and values are povided in Quantity and Unit Cost.	Decimal	For **Agreement**, this value must be supplied. It appears as **License Cost** in the Agreement page. For **License** and **Maintenance**, do not provide a value. It will be automatically calculated if Unit Cost Type is **OnceOff**, and values are povided in Quantity and Unit Cost.
UnitCostType	No	OnceOff	String	Valid values are: OnceOff

Column	Mandatory	Default if not specified	Datatype	Notes
				Monthly Quarterly Yearly
Comments	No		String	Used for any comments you want to import. If an AppClarity 5.2 entitlement includes any of the following product details, these will be exported in the comments field: Colloquial SubVersion Registration Key Persistent Id Entitlement Key Channel Type Product Family UNSPSC Code ParentEntitlementId - In AppClarity 7.0 an entitlement can only have one parent or none. When exporting from AppClarity 5.2, if any entitlement has multiple parents then only one will

Column	Mandatory	Default if not specified	Datatype	Notes
				be used in the ParentEntitlementId column, and the ParentEntitlementId of the others will appear here in the Comments column.
MasterAllocationPercentage	No		Integer	Not supported. This is to handle complex agreement scenarios; currently not supported. There are Agreements where total amount is fixed and can be distributed among various entitlements in that agreement. This defines the percentage of that amount allocated to this entitlement.

10.6.7.2 FOSSDetail (3)

Column	Mandatory	Default	Datatype	Notes
FossDetail.FossDetailId	No		String	**Warning** Do not use for imports.
FossDetail.IsFoss	No		Boolean	This value is true only if the granted rights fulfil the requirements of the definition of free software

Column	Mandatory	Default	Datatype	Notes
				maintained by the Free Software Foundation (FSF)
FossDetail.CopyLeft	No		String	This value provides information on whether derivative works (which are always allowed for open source software) are themselves required to be open source software. There are three allowed values: **strong** - that all kinds of derivative works are required to be open source software themselves **no** - means that for all kinds of derivative works, it is allowed to distribute the derivative work as proprietary software **weak** - the intermediate value means that there are some restrictions and the details are to be checked in the license
FossDetail.TrademarkRestrictions	No		String	FOSS trademark restrictions

10.6.7.3 Internal Order (4)

Column	Mandatory	Default	Datatype	Notes
InternalOrder.InternalOrderId	No		String	**Warning** Do not use for imports.

Column	Mandatory	Default	Datatype	Notes
InternalOrder.Number	No		String	Free text but recommendation is integer
InternalOrder.LineItemNumber	No		String	Free text but recommendation is integer
InternalOrder.Date	No		Date	Date

10.6.7.4 Licensor Detail (5)

Column	Mandatory	Default	Datatype	Notes
LicensorDetail.LicensorDetailId	No	NULL	String	**Warning** Do not use for imports.
LicensorDetail.Name	No	NULL	String	The name of the licensor, could be the vendor or a VAR
LicensorDetail.Number	No	NULL	String	This is intended as a reference to a licensor source other than an invoice, e.g. to an on-line portal of license purchases. Free text but recommendation is integer
LicensorDetail.Date	No	NULL	Date	Date

10.6.7.5 Miscellaneous Details (6)

Column	Mandatory	Default	Datatype	Notes
MiscellaneousDetail.MiscellaneousDetailId	No	NULL	String	**Warning** Do not use for imports.
MiscellaneousDetail.ManagementGroup	No	NULL	String	The entitlement can be associated with

Column	Mandatory	Default	Datatype	Notes
				the specified Management Group. **Warning** The management group must already exist. **Note** In the current version of AppClarity, associations with management groups do not affect compliance calculations. Calculations apply to all devices in the repository, irrespective of Management Groups.
MiscellaneousDetail.BusinessUnit	No	NULL	String	May be covered by Management Group, but may not - in the VA, this is the Pillar the software is

Column	Mandatory	Default	Datatype	Notes
				associated with. (Kapil Makhija)
MiscellaneousDetail.Sponsor	No	NULL	String	Name of the person who manages the budget associated with an agreement (likely used only on agreements, but could be extended to individual entitlements)

10.6.7.6 Audit Detail (7)

Column	Mandatory	Default	Datatype	Notes
AuditDetail.AuditDetailId	No	NULL	String	**Warning** Do not use for imports.
AuditDetail.Auditor	No	NULL	String	Names of organisations entitled to perform the audit including, if appropriate, the licensor organisation and third party organisations according to what was agreed in the contract.
AuditDetail.Frequency	No	NULL	String	Definition of the highest agreed frequency of the audit expressed in months
AuditDetail.Tool	No	NULL	String	Name of the tool(s) which are approved for use in the audit.
AuditDetail.NoticePeriod	No	NULL	Integer	Notice period expressed in months
AuditDetail.Scope	No	NULL	String	Defines what part of the software customer organisation is allowed to be audited.

Column	Mandatory	Default	Datatype	Notes
AuditDetail.Clause	No	NULL	String	Provides additional information on what could trigger the audit.

10.6.7.7 Contract (8)

Column	Mandatory	Default	Datatype	Notes
Contract.ContractId	No	NULL	String	Identity id of the contract. This is auto-generated as a GUID if the entitlement was created in the user-interface. **Warning** Do not use for imports.
Contract.Data	No	NULL	String	**Warning** Do not use for imports.
Contract.Name	No	NULL	String	Name of the contract.
Contract.Number	No	NULL	Integer	Contract number
Contract.StartDate	Yes	NULL	Date	When the contracts starts applying
Contract.Link	No	NULL	String	A link to a referenced contract (not uploaded)
Contract.Resource	No	NULL	String	Name of the person who manages the agreement (likely used only on agreements, but could be extended to individual entitlements)
Contract.TechnicalResource	No	NULL	String	Name of the person who knows the technical details behind licensing, or product information for an agreement (likely only used on

Column	Mandatory	Default	Datatype	Notes
				agreements, but could be extended to individual entitlements)
Contract.FileName		NULL		If there is any attachment - then what? (currently not supported through tsv file)

10.6.7.8 Direct Supplier (9)

Column	Mandatory	Default	Datatype	Notes
DirectSupplier.DirectSupplierId	No	NULL	String	**Warning** Do not use for imports.
DirectSupplier.Number	No	NULL	String	Free text but recommendation is integer
DirectSupplier.LineItemNumber	No	NULL	Integer	LineItemNumber
DirectSupplier.Date	No	NULL	Date	Date

10.6.7.9 Invoice Detail (10)

Column	Mandatory	Default	Datatype	Notes
InvoiceDetail.InvoiceDetailId	No	NULL	String	**Warning** Do not use for imports.
InvoiceDetail.Number	No	NULL	String	Free text but recommendation is integer
InvoiceDetail.LineItemNumber	No	NULL	Integer	Line item number
InvoiceDetail.Date	No	NULL	Date	Date

10.6.7.10 Purchase Order Detail (11)

Column	Mandatory	Default	Datatype	Notes
PurchaseOrderDetail.PurchaseOrderDetailId	No	NULL	String	**Warning** Do not use for imports.
PurchaseOrderDetail.Number	No	NULL	String	Free text but recommendation is integer
PurchaseOrderDetail.LineItemNumber	No	NULL	Integer	LineItemNumber
PurchaseOrderDetail.Date	No	NULL	Date	Date

10.6.8 AppClarity release information

10.6.8.1 AppClarity 8.1 Release Notes – last updated 05-August-2022

These notes contain late-breaking information about AppClarity that you need to have to successfully install and use the product. For the most up-to-date information, please see the online readme. You should read these release notes and the online documentation for AppClarity thoroughly before installing the software.

10.6.8.1.1 New features in AppClarity 8.1

Works with Tachyon Platform 8.1

No features or feature changes added in this release, but includes any hotfixes from previous versions.

10.6.8.2 Troubleshooting

10.6.8.2.1 Online help

Nomad comes with online help that shows you how to install, configure and use the product. Click the following link to view the help:

Introducing AppClarity

For support queries, please:

Use https://support.1e.com/ where you can search the KB or submit a support case.

Contact support@1e.com.

10.6.8.2.2 Known issues

The current known issues related to the installation and running of AppClarity can be found in the Troubleshooting Known issues page of the AppClarity documentation.

Known issues for the Platform and other applications can be found in the 1E platform - Known issues documentation.

10.6.8.3 AppClarity Release History

10.6.8.3.1 AppClarity 8.1.?.??? Web release (01 Mar 2022)

Works with Tachyon Platform 8.1

No features or feature changes added in this release, but includes any hotfixes from previous versions.

10.6.8.3.2 AppClarity 8.0.5.xx Web release (01 Nov 2021)

Works with Tachyon Platform 8.0

No features or feature changes added in this release, but includes any hotfixes from previous versions.

10.6.8.3.3 AppClarity 7.1.105.xx Web release (01 April 2021)

Works with Tachyon Platform 5.2

No features or feature changes added in this maintenance release.

10.6.8.3.4 AppClarity 7.1.0.95 Web release (27 July 2020)

Works with Tachyon 5.1

Windows Server OS LDC

Support for Currency Conversion

New UI controls

AppClarity is now included in Tachyon Setup and can be installed and maintained this way

Enhancements

Entitlement

License Demand

Compliance

Reclaim

10.6.8.3.5 AppClarity 7.0.0.206 Web release (17 Mar 2020)

Management Group view in LDC, Entitlements and Compliance

New UX with improved display and dashboards

RBAC feature to access screens and Reports

RHEL Server LDC

Custom SCCM Uninstall

User Based Compliance

Indirect and/or direct association of maintenance with license

Fallback approach to improve Compliance mechanism

Maintenance quantity consumption behavior is restructured

Device Exempted from LDC/Compliance

Performance Improvements in Reclaim Consolidation and Reporting

Improvements in entitlement connector (import from TSV and APC 5.2.300)

Wildcard support in entitlement

License Position (ELP) Report enhancements

Addition of User, Socket metrics in entitlement

10.6.8.3.6 AppClarity 6.1.100.57 Web release (14 Nov 2018)

Loading image jammed up on bulk publishing the entitlements.

Auto triggering the Entitlement and Reclaim consolidation on Publish.

Reclaim policy creation on any product exist in Catalog.

'Pending Administrative Actions' notification on Published Reclaim Policies.

Overlapping/Overriding reclaim policies Published as "Disabled", to set the precedence first.

'Management group names' information on Policy Precedence page.

Ability to refresh only one LDC at a time, instead of all LDC refresh.

License/Maintenance entitlements give option to view "Licensable" products only.

FIPS support.

Support for TLS 1.1 and TLS 1.2.

10.6.8.3.7 AppClarity 6.1.0.30 Web release (26 July 2018)

Entitlement

License Demand Calculation (LDC)

Reclaim

SLA Platform - the new AppClarity is built upon the SLA Platform

Tachyon powered

10.6.8.4 AppClarity features by release

10.6.8.4.1 Summary

List of AppClarity features organized by the release they were implemented in. Links through to the features have been provided for convenience.

10.6.8.4.2 New features in AppClarity 8.1

This main release contains the following features:

Works with Tachyon Platform 8.1

No features or feature changes added in this release, but includes any hotfixes from previous versions.

10.6.8.4.3 AppClarity 8.0

Works with Tachyon Platform 8.0

No features or feature changes added in this release, but includes any hotfixes from previous versions.

10.6.8.4.4 AppClarity 7.1

10.6.8.4.4.1 AppClarity 7.1.105

This maintenance release contains a number of bug fixes:

Works with Tachyon Platform 5.2

No features or feature changes added in this maintenance release.

10.6.8.4.4.2 Features in the AppClarity 7.1 main release

This release introduced the following features:

Works with Tachyon 5.1

Windows Server OS LDC

New license demand for core based licensing of Windows Server OS (calculated with-in Microsoft Core LDC)

Compliance calculation is now based on new license demand

Support for Currency Conversion

When you can set a default currency (other than USD) AppClarity now renders all reporting and financial numbers (or graphs) only in that set currency

New UI controls added to improve usability:

Report refresh - ability to refresh reports on individual pages, and the ability to view the status of the last report refresh

UI Controls - ability to choose columns as either shown or hidden on individual screens

Installation mode change

AppClarity is now included in Tachyon Setup and can be installed and maintained this way

Hotfixing capability

Enhancements

Entitlement

New Active Entitlements Only toggle filter on Entitlement Summary page

The ability to export entitlement summary data

License Demand

Device names are now shown as hyperlinks on LDC reports

Compliance

Improved logic for rendering installs, and a new "Exempt" status on the compliance detailed table

Effective License Position (ELP) displayed for SQL Server components as it is for SQL Server entitlement

Reclaim

Reclaim product usage screen loading time is optimized for quick page load.

10.6.8.4.5 AppClarity 7.0

10.6.8.4.5.1 AppClarity 7.0 will significantly enhance your Software Asset Management (SAM) capabilities.

Improved Usability

The New UI experience is more user friendly compared to previous version, applying sorting, filtering etc is much easier

There are additional navigation options for operational ease

There are interactive charts in the Entitlement and Reclaim sections and more detailed compliance reports

There are suggestions on Top 10 reclaim policies users should create for maximum savings

Compliance and usage are shown in same pane for users to make informed procurement decisions.

SaaS Monitoring

Manage Renewals - monitor usage and renew only active subscriptions

Reallocate licenses: Monitor usage and reallocate under utilized subscriptions to other users

Compare usage of competing products - if users use apps from multiple vendors to achieve same things, consolidate to one/fewer vendors based on usage.

AI Powered Autocuration

Removes the delay in software identification so there's no delay in identifying software

Increases productivity, so users no longer have to spend hundreds of hours curating software, AI can help automatically match majority of the software as soon as they appear in the estate.

Avoids human errors, the AI is a more reliable and accurate source normalization

Users can enable AI-powered Autocuration to automatically identify installed software in the estate if recognized at a very high confidence level

If the confidence is lower than the threshold, it appears as a suggestion for customers to quickly add review and add the match rules, making it extremely quick to manage the unknown/unmatched software.

User-based Compliance

Ability to show license demand per user

Optimize procurement - customers can save significant cost by identifying when same users have access to same apps on multiple devices

Audit defence - gives users the ability to report accurately on apps that are licensed per user when vendor audits take place

There is software which can be licensed on both device as well as user metrics, AppClarity 7.0 will use entitlements of both metrics (user and device) to compute compliance and effective license position.

Compliance by Management Group

Entitlements can now be affiliated to specific Management Groups, allowing users to compute and view license demand for those Management Groups

Software Audits, entitlements are valid to be used only in a particular region

Internal Chargeback, budgets/profitability of a specific cost center

Specific Management Group Owner, when specific users view/monitor compliance for a specific Management Group.

Exempt Device(s) from license demand & Compliance

Exempt Device(s) from license demand and compliance calculations using Management Groups – exempt devices for accurate License Demand Compliance (LDC) reporting

Accurate reporting allows users to input company specific context into AppClarity so they don't have to adjust the AppClarity report every time they need to assess their license position

Once the license exemptions are specified in the product, users do not need to worry about manually adjusting the numbers

MSDN: Devices used by MSDN subscribers for Dev purposes only

MSDN subscribers get umbrella access to numerous MS products including Visual Studio, Visio, Project, Office, SQL Server etc. These subscribers usually access a very well defined set of devices, which are used for development purposes only. Customers do not wish to count licenses for those software in LDC/Compliance reports as those are all covered under MSDN licenses.

Customers can exempt select devices, by adding those to a specific management group name (pre-defined template) to exempt those for Microsoft LDC and compliance reports

Helps customers compute accurate license demand for renewal/true-up

Test/Disaster Recovery/Admin/Third Party Devices - customers do not want certain devices to be considered for license/compliance calculations

There are devices purely used for Disaster Recovery, backups, testing, or belong to a third party and do not need to be licensed, customers can add exempt those devices (and all its installs) for a specific vendor or for ALL vendors by adding them to a specific Management Group.

The feature does not allow you to exempt devices for specific software, they can either exempt devices for all software from a particular vendor or all software of all installs.

RedHat LDC

Audit defence, users can respond to audits, compliance reports can help assess compliance position and mitigate risks

Optimization, reduce your software cost by applying the most efficient and cost effective way of licensing the estate

Renewal exercise, users can renew RedHat agreement using RedHat LDC reports

Users can compute license demand for RedHat products (LDC), counter on Sockets on devices

Users can compute Compliance position based on available entitlements and compute effective license position

Helps customers prepare for RedHat renewals/true-up exercise.

Role Based Access Control (RBAC), access to screens/actions as per role/permissions provided to user

Control Access, avoid unwanted access to different SAM team members, ensure data security and governance

Users will be able to control access to screens and actions (read/write/edit) on each screen for every role

There are a few pre-defined roles with appropriate permissions, however, users can create their custom roles by selecting from the list of permissions for each role.

Custom SCCM Uninstall

Offers an alternative way of uninstalling software, customers using SCCM and building custom packages can trigger SCCM-driven software uninstalls based on reclaim policies defined in AppClarity

If customers have created apps/packages in SCCM they want to use for uninstallation, they can use SCCM to Uninstall software, users can choose SCCM collection type as Device/User/or Both for a given policy.

Identify Vulnerabilities

Identify Vulnerabilities – end of support date, Software Category, and Latest Known Version fields have been exposed on UI for users to be able to identify vulnerabilities.

End of support (EoS) date - helps users identify installs nearing EoS or Past EoS, prompting users to upgrade

Latest Version Known for a software in 1E Catalog - allows users to see if they're on the latest version of the software release that's installed, once this new version is seen, other installations not updated will be identified as not on the latest version

Top Software Categories - shows you the number of different products you have in the same software category, for example, if users have 4 different BI products – that may be something like PowerBI, QlickView, Tableau and ThoughtSpot – it enables them to identify areas for consolidation and more effective negotiations for pricing on the consolidated title.

10.6.8.4.6 AppClarity 6.1

10.6.8.4.6.1 AppClarity 6.1.100

This maintenance release introduced the following enhancements:

Entitlement consolidation reports are automatically run when publishing entitlements.

Reclaim consolidation reports are automatically run when publishing reclaim policies.

Reclaim policies can now be created for any product that exists in the 1E Catalog, previously reclaim policies could only be created for software currently installed in the environment.

Pending administrative actions notifications are now displayed for Published Reclaim Policies when an action is expected of the AppClarity administrator. For example, the administrator needs to respond to a user opting out of a reclaim.

Overlapping/Overriding reclaim policies are now automatically published as disabled. This gives the administrator the opportunity to set the precedence before the reclaim policies become active.

Information on the Management Groups a reclaim policy applies to is now displayed on the Policy Precedence page. This gives the administrator the information they need in order to appropriately set the precedence for overlapping reclaim policies.

Ability to refresh only one License Demand Calculation (LDC) report at a time, previously refreshing an LDC also forced the refresh of the LDCs below it on the page.

License/Maintenance entitlements now provide an option to view **Licensable** products only.

FIPS support.

Support for TLS 1.1 and TLS 1.2.

10.6.8.4.6.2 Features in the AppClarity 6.1 main release

This release introduced the following features:

Entitlement - there are a whole set of features that help you model your organization's entitlements:

Create a centralized collection of all your entitlements in AppClarity, using an ISO 19770-3 aligned entitlement library

Create license, maintenance and agreement entitlements, with associated product usage rights. You can also attach Contracts, containing the proof of license ownership, to the entitlements

Bulk upload of entitlements using TSV files to create draft entitlements for verification, before bulk publishing them

Use SKU to create entitlements; SKU auto-populate product specifications and use-rights

Link one entitlement to another to help model complex agreements and contracts

Upload soft copies of contracts

Create separate sets of entitlements in different repositories

Schedule Entitlement consolidation to run at regular intervals

License Demand Calculation (LDC) Reports - AppClarity lets you calculate how many licenses you need for specific products with complex license requirements

Perform license demand calculations for complex license metrics. Currently related to Microsoft SQL Server, IBM PVUs, and Oracle Processors

Use LDCs to compute the optimum number of licenses required to cover your complex virtual/physical/clustered server environment, letting you see the best way to purchase new licenses or renew your subscription-based licenses

Review records that couldn't be processed by AppClarity for any reason to perform due diligence and mitigate risk

Schedule LDC consolidations to run at regular intervals

Compliance - these features let you gauge how well your entitlements cover your installations

View the compliance position of each software based on your entitlements

Optimally make use of licenses to compute your compliance position

Review records that couldn't be processed by AppClarity for any reason to perform due diligence and mitigate risk

View compliant and non-compliant installations

Create separate compliance repositories for separate environments by linking them to a unique set of Inventory and Entitlement repositories

Reclaim - these features let you reclaim software to minimize license costs or protect your devices

Reclaim software based on software usage

Create policies for software you want to reclaim

Create policies that are focused on particular management groups

If policies overlap across management groups, your can set their precedence to resolve conflict

Evaluate the impact of a policy by running a pre-flight report before putting it into production

View Software saving reports showing the value of software reclaims performed using Appclarity

Schedule reclaim consolidations to run at regular intervals so that you are viewing up to date information

SLA Platform - the new AppClarity is built upon the SLA Platform and is able to use its consolidated inventory data to derive software installations and usage.

SLA Platform now contains two new connectors:

Tachyon powered inventory - information gathered by Tachyon can be used to augment the software and hardware inventory and software usage data, normally found in Microsoft System Center Configuration Manager, or to enable AppClarity solutions to work in environments where no Configuration Manager or other inventory tools are available. Using the Tachyon inventory data source means that the information displayed in AppClarity will be more accurate and up-to-date than using Configuration Manager on its own. Each device will need to have the Tachyon Agent installed, which will enable Tachyon to bring inventory data where no other solution agents are present or where they are not responding. If you have Configuration Manager installed, but without the SQL MOF implemented, Tachyon will fill in the gaps in the Configuration Manager data to provide information about the SQL Server editions in your environment. Currently this is specific to SQL Server but will be extended to include more products in subsequent releases.

IBM BigFix inventory connector - an IBM BigFix connector has been added to the SLA Platform enabling AppClarity to work in environments where that product is being used to manage your computer software estate.

AppClarity Business Intelligence dashboard - The new Business Intelligence SLA Platform consumer provides several dashboard tiles that let you view and examine your AppClarity features graphically.

10.6.9 Glossary

A glossary of AppClarity terminology.

10.6.9.1 AppClarity alphabetical glossary

Term	Definition
Across Mgmt Grp Policies column	This column is displayed on the Usage Summary page. The **Across Mgmt Grp Policies** column shows the number of policies for a product across all management groups.
Active Agreements only	This toggle is displayed on the Agreements page. The **Active Agreements only** toggle adds a filter when it's turned on that filters the table to only display the agreements that have been published and not the ones that are in draft.

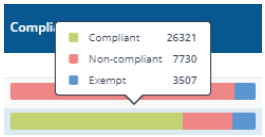
Term	Definition
toggle	
Active Entitlements only toggle	This toggle is displayed on the Licenses / Maintenances page and the Entitlements page. The **Active Entitlements only** toggle adds a filter when it's turned on that filters the table to only display the entitlements that have been published and not the ones that are in draft.
Active Policies Only toggle	This toggle is displayed on the Policies page. The **Active Policies Only** toggle adds a filter when it's turned on that filters the table to only display the reclaim policies that have been published and their status is set to enabled.
Agreement entitlement	An agreement entitlement type in AppClarity provides a structure to license and maintenance entitlements. Agreements can be used to model the contractual structure an organization uses for their purchasing process, or their internal software disbursement process.
AppClarity	AppClarity is a software asset management (SAM) tool that enables you to define entitlements and determine your license compliance position. It does this based on the software and hardware inventory data provided by the Software Lifecycle Automation (SLA) Platform that AppClarity is installed on. The software inventory also includes details of product usage which can be used by AppClarity as the basis for its policy-based software reclaim capabilities.
AppClarity administrator	These users are initially defined in SLA Platform by the primary SLA Platform administrator (typically the SLA Platform installation account). They are able to set up repositories, create connectors, defined schedules and run AppClarity reports etc.

Term	Definition
Application	Synonymous with software product. Also known as App.
Back link	Each page in AppClarity has a back link on the page. Clicking this link takes you back to the previous page you were browsing, and works differently to the browser's back button for this application in that it takes you to the last page you were on in the application.
Bundle	[ISO/IEC 19770-5, 3.1.4] A grouping of products which is the result of a marketing/licensing strategy to sell entitlements to multiple products as one purchased item. A bundle can be referred to as a “suite”, if the products are closely related and typically integrated (such as an office suite containing a spreadsheet, word processor, presentation and other related items). Bundles can also refer to software titles that are less closely related such as a game, a virus scanner and a utility “bundled” together with a new computer, or to groups of entitlements, such as multiple entitlements for a backup software product.
Canonical representation	In SLA Platform this specifically refers to representations of software products, devices and processors having all the attributes that they need to be used consistently. **Product canonical representation** Products consist of software vendor, title, version and edition entries in the catalog that are structured as follows.AttributeDescriptionVendorPublisher of the software title, for example Microsoft Corporation.TitleName of the software product, for example Visio.VersionFull version number of each release of the product.EditionIf the product is an edition based product, the editions of this specific version of the product.Edition Match rulesRules that link one or more inventory source data entries to this specific edition, of this version, of this product.End of support datesDate when this version of the product is due to go end of support.Colloquial versionIf the product uses colloquial versions, then the one related to this specific version, for example 2013.Version match rulesRules that link one or more inventory source data entries to this specific version of this product.UNSPSCUnited Nations Standard Products and Services Code for this product, for example 43233004 for operating systems. **Device canonical representation** AttributeDescriptionVendorDevice vendor, for example, Dell.Device TypeDevice type, for example Desktop.FamilyDevice family, for example, Inspiron.ModelDevice Model, for example, 400.Max Socket CountMaximum number of sockets for the device, for

Term	Definition
	example, 1.Device Match RulesRules that link one or more inventory source data entries to this specific device, device type, family and model. **Processor canonical representation** AttributeDescriptionVendorProcessor vendor, for example, Advanced Micro Devices Inc.Processor TypeProcessor type, for example, Desktop.FamilyProcessor family, for example, A10.ModelProcessor model, for example, 5700.FrequencyProcessor frequency, for example, 3,400.SocketThe socket type the processor uses, for example, FMZ.Core CountProcessor core count, for example, 4.Threads per coreThe number of threads per core for the processor, for example, 2.
Canonical Version column	The **Canonical Version** column is displayed on the **Device Detailed** table on the Summary by Installs page and on the License Position page.The canonical representation of the productversion installed on a device.
Category column	This column is displayed on the Usage Summary page.The **Category** column shows the category for each product.
Catalog curator	This user is responsible for curating the matching rules in the 1E Catalog.
Classification column	The **Classification** column is displayed on the following pages: Microsoft Core License Demand - Detailed Report page IBM Processor Value Unit (PVU) License Demand - Detailed Report page Oracle Processor License Demand - Detailed Report page Red Hat Socket Demand - Detailed Report page Displays the classification for the device where the software is installed. If set this may be one of:

Term	Definition
	Classification Production Test
Clear all filters link	On most pages in AppClarity where a filter can be set there is also a **Clear all filters** link, this enables you in a single-click to clear all of the filters set in the **FILTER BY** field.
Cluster Name column	The **Cluster Name** column is displayed on the following pages: Microsoft Core License Demand - Detailed Report page IBM Processor Value Unit (PVU) License Demand - Detailed Report page Oracle Processor License Demand - Detailed Report page Red Hat Socket Demand - Detailed Report page The Cluster Name, if any, where the software in the License Demand report is installed.
Colloquial version	The colloquial version name for the product. For example, **2003**, **2016** etc. This is an additional attribute to the vendor, title, version and edition for a software product that may identify a range of versions. See also Version.
Column filters	Some tables contain a column filter that lets you easily filter the information displayed in the table.**Using column filters**The picture opposite shows an example taken from AppClarity. In our example we want to filter the table to show only those items where the **Edition** contains the text **Prof**.To filter the table on the **Edition** column:Click on the filter iconjust beneath the header row in the **Edition** column.The filter popup is displayed.Now select the operator. In our example this will be **contains**.Then type the text **Prof** into the text field.Click **Apply** and a new filter will be added to the table.The table will be filtered to just those items whose **Edition** contains the text **Prof**.**Adding another filter**You can add another filter by clicking on the filter icon for any of the columns. The picture opposite shows another filter added selecting table rows where the **Type** also contains the text **License**. The table will also be filtered accordingly.**Removing filters**You can remove filters by clicking on the filter close icon at the end of the filter.

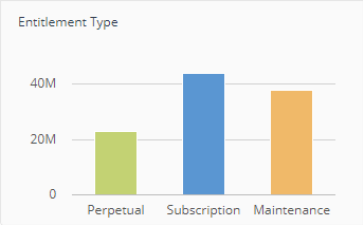
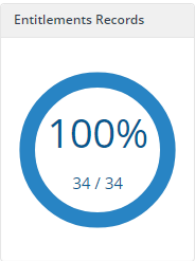
Term	Definition
Column Picker	**Using column picker**Where the column picker control is shown you can choose which columns are displayed. In the following example on the **Microsoft Core License Demand** page we hide the **Unknown Installs** column and move the **License Demand** column to the left of the page.To pick the displayed columns:Click on the Choose columns iconto the right of the header row to view the visible columns.To exclude **Unknown Installs**, select the Unknown Installs row and click **Exclude columns** button.The **Unknown Installs** column is now hidden.To move the **License Demand** column to the top of the list, hover your mouse over **License Demand** and using the direction control drag it to the top of the list.The Microsoft Core License Demand page has now been automatically updated with our changes.
Column sorts	Some tables contain column sorts that let you easily re-order the information displayed in the table.**Using column sorts**The picture opposite shows an example taken from AppClarity. In our example we want to sort the table on the **Cost** column from the highest cost at the top to the lowest at the bottom. To sort the table on the **Cost** column:Click on the sort iconjust beneath the header row in the **Cost** column.The sort popup is displayed.Now select the sort direction. In our example this will be **Sort descending**.After selecting this the data in the table is now sorted on the **Cost** column from highest to lowest and the sort icon has changed to a sort descending icon**Clearing the sort**You can clear the sort by clicking on the sort icon again and selecting the **Clear sorting** menu item from the sorting popup.
Comments column	The **Comments** column is displayed on the **Device Detailed** table on the Summary by Installs page. This column provides comments on how the entitlement is applied to the installation. Currently this indicates whether the installation has been exempted or not. The **Comments** column is displayed on the following Licence Demand Detailed Reports pages: Microsoft Core License Demand - Detailed Report page IBM Processor Value Unit (PVU) License Demand - Detailed Report page Oracle Processor License Demand - Detailed Report page Red Hat Socket Demand - Detailed Report page Provides recommendations on how to license the software to achieve the optimum license demand.
Completi	This column indicates the date the reclaim policy was applied and completed.

Term	Definition
on Date colu mn	
Com plian ce Cate gory colu mn	The **Compliance Category** column is displayed on the License Summary page. This column displays a compliance status bar for each product.  This bar displays a summary of the compliance status for the product installations in the selected compliance repository, taking into account any entitlements you have added. Hovering over the bar displays a summary of the compliance breakdown for the product. This is divided into **Compliant**, **Non-compliant** and **Exempt** installations. Clicking on the bar displays the Summary by Installs page for the selected product.
Com plian ce positi on	The compliance position describes the comparison between the installed versions of a product and the entitlements held for that product. In AppClarity you can view your compliance position using the License Summary page. For a description of how you would use that page please refer to Viewing product compliance.
Com plian ce repos itory	AppClarity extends SLA Platform to include two new repository types: compliance and entitlement. Compliance repositories have their own reports that combine information from an SLA Platform inventory repository with an entitlement repository to determine a company's compliance position.
Com plian ce repos itory selec tor	This field lets you select the repository where the compliance data displayed on the page comes from. By default this is set to **Default Compliance**. If you have created your own compliance repositories, click on the name to select these from the drop-down list.
Com plian ce	This column displays an indicator for the current compliance status for the product.

Term	Definition
Status column	
Compliant Installs column	This column provides a count of the compliant installations for the product. When the number is not zero this is a link to a list of devices where the product is installed.
Components	Components refer to the bundled software related to a license. For example you may have a bundle for **Microsoft BackOffice Small Business Server**, which would contain components for **Exchange Server**, **FrontPage**, **Internet Explorer** and **Outlook**.
Connectors	A feature which enables SLA Platform to communicate with external systems, usually data sources.
Consolidation	The process of taking raw inventory data from different inventory data sources and combining them into a single de-duplicated data set in SLA Platform. For example, taking software inventory from Tachyon, Big Fix and Configuration Manager into a single usable repository.
Consumed column	The **Consumed** column is displayed on the Summary by Installs page. Shows the number of licenses consumed by installations from a particular entitlement.
Contract entitlement	A contract entitlement type in AppClarity represents the evidence or proof that the license exists and is genuine. It is an artifact that can be virtually anything - it may be a scan of the signed contract for an enterprise agreement, for example, or it could be a PDF of the use rights for the software. Essentially the contract is where you will link file details that describe the specifics of an agreement.
Contract	This user validates that contracts have been entered properly and that all prioritized contracts are managed.

Term	Definition
manager	
Cores column	The **Cores** column is displayed on the following pages: Microsoft Core License Demand - Detailed Report page IBM Processor Value Unit (PVU) License Demand - Detailed Report page Oracle Processor License Demand - Detailed Report page Red Hat Socket Demand - Detailed Report page Displays the number of processor cores available on the mainboard for the device where the software is installed.
Cost column	The **Cost** column is displayed on the Licenses / Maintenances page:The **Cost** column displays the cost for each entitlement in the table.
Curation	Firstly, the process of defining the canonical representations in the 1E Catalog to be used by 1E companion products including: SLA Platform and AppClarity. Secondly, the process of defining the matching rules that will enable the normalization of the software products, processors and devices found in your environment into those canonical representations.
Description column	This column describes the reclaim action. Generally this is set to **Reclaimer Uninstall**.
Edition	The edition portion of the vendor, title, version and edition attributes that are used to identify software products. For example, **Standard** or **-** (where no edition exists).
Edition column	The **Edition** column in AppClarity pages displays information related to the edition of a product. Depending on the context this may show different things: On entitlement pages this will show:The edition portion of the vendor, title, version and edition attributes that are used to identify which software products the entitlement is for. For example, **Standard** or **-** (where no edition is specified or exists). On the License Position page this will show:

Term	Definition
	The edition portion of the vendor, title, version and edition attributes that are used to identify which software product the compliance status relates to. On the reclaim Usage Summary page and the Savings page this will show: The edition portion of the vendor, title, version and edition attributes that are used to identify which software product the reclaim policy was applied to.
Editions column	On the reclaim pages in AppClarity an **Editions** column is sometimes displayed. This shows a list of editions that determine which products the reclaim policy will be aimed at. The edition portion of the vendor, title, version and edition attributes that are used to identify software products. For example, **Standard** or **-** (where no edition exists).
Effective License Position column	The effective license position is a calculation of the entitlements for a particular software product against the installations for that product. It may be one of: a negative number, in which case there are more installations for that software product than entitlements zero where the numbers match exactly a positive number, which indicates you have paid for more licenses than you are using. Your ideal is to get the numbers positive but as close to zero as fits in with your current and predicted demand.
End Date column	The End Date column is displayed on the Licenses / Maintenances page: The **End Date** column shows the date the entitlement will end.
Entitlement	In AppClarity an entitlement refers to a license, maintenance or agreement that may be linked together to define the owned rights to use or install a particular software product. License entitlements count towards a companies compliance position against the number of installations of a particular product.
Entitlement repository	Entitlement repositories hold the entitlements entered by AppClarity users for specific software products.

Term	Definition
Entitlement type	The type for a particular entitlement. This may be one of: Perpetual Subscription Maintenance
Entitlement Type chart	The **Entitlement Type** chart is displayed on the Summary Report page. This chart shows the breakdown and numbers for the Entitlements Records in the selected Entitlements repository according to their Entitlement type: Perpetual, Subscription or Maintenance. 
Entitlements Records chart	The **Entitlements Records** chart is displayed on the Summary Report page. This chart shows the percentage of the total number of Entitlements Records in the selected Entitlements repository that are currently being displayed on this page as a result of the applied filters. The figures below the chart show the number of Entitlements Records being displayed over the total number of Entitlements Records in the selected Entitlements repository. 
Entitlements repository selector	This field lets you select the repository where the entitlements data displayed on the page comes from. By default this is set to **Default Entitlements**. If you have created your own entitlements repositories, click on the name to select any of these from the drop-down list.

Term	Definition
Entitlements Available	This column provides a count of the entitlements currently defined for the product.
Exempted column	The **Exempted** column is displayed on the Summary by Installs page. This column provides a count of the exempted installations that are associated with an exemption management group. Please refer to Excluding devices from License Demand Calculation using Management Groups for more details.
Export all button	Pages in AppClarity that include an **Export all** button allow you to export all the data for any tables of information displayed on the page. This may also include columns that are not currently visible in the table display.
Host Name column	The **Host Name** column is displayed on the Reclaim History page. Displays the host name for the device where the reclaim policy was applied.
Identifier column	The **Identifier** column is displayed on the Licenses / Maintenances page and Agreements page. Displays the **Identifier** information configured for the entitlement or agreement.
Installs column	The **Licensed Software** column displayed on the **License Demand** table for each of the following License Demand and License Demand - Detailed Reports:

License Demand Report	License Demand Detailed Report
Microsoft Core License Demand page	Microsoft Core License Demand - Detailed Report page
IBM Processor Value Unit (PVU) License Demand page	IBM Processor Value Unit (PVU) License Demand - Detailed Report page
Oracle Processor License Demand page	Oracle Processor License Demand - Detailed Report page

Term	Definition
	Red Hat Socket Demand page Red Hat Socket Demand - Detailed Report page This column shows the number of installs for the software titles that are part of the License Demand report.
Inventory	Inventory is the hardware, software and software usage information from your environment. This information is gathered by SLA Platform and placed into an Inventory repository for use by consumers, such as AppClarity.
Inventory repository	An inventory repository is a consolidated view containing inventory information from your network. SLA Platform uses connectors to fetch information from the inventory sources, which is then processed until it becomes usable by the consumers of the SLA Platform.
Lic Qty column	The **Lic Qty** column is displayed on the Summary Report page. The **Lic Qty** column shows the number of licenses related to each Entitlement in the table.
License Consumed column	The **License Consumed** column is displayed on the **Device Detailed** table on the Summary by Installs page. This column shows the number of available licenses consumed by the software on the device where it is installed.
License Demand Calculation reports	AppClarity provides a number of license demand calculation reports that show information on the license demand for complex product licensing. These reports are described in Calculating license demand.
License Demand	The **License Demand** column is displayed on the **Device Detailed** table on the Summary by Installs page. The license demand for the software on the device where the software is installed.

Term	Definition
column	The **Licensed Software** column displayed on the **License Demand** table for each of the following License Demand and License Demand - Detailed Reports: License Demand Report / License Demand Detailed Report Microsoft Core License Demand page / Microsoft Core License Demand - Detailed Report page IBM Processor Value Unit (PVU) License Demand page / IBM Processor Value Unit (PVU) License Demand - Detailed Report page Oracle Processor License Demand page / Oracle Processor License Demand - Detailed Report page Red Hat Socket Demand page / Red Hat Socket Demand - Detailed Report page This column shows the license demand for the software titles that are part of the License Demand report.
License Edition	The **License Edition** column is displayed on the **Entitlement Summary** table on the Summary by Installs page. The edition for the software as defined in the entitlement.
License entitlement	A license entitlement type in AppClarity specifies the rights and limitations of software and/or services that may be installed and/or used on an organizations computing devices. For example you could specify a license for Microsoft Visio 2016 and enable version downgrade rights to ensure that the license covers all versions up to 2016.
License Position column	The **License Position** column is displayed on the License Position page. Shows the license position for the product calculated by subtracting the value in the **Total Units Consumed** column from the value in the **Total Licensed Units** column. Negative numbers in red indicate a license deficit. Positive numbers in black indicates a license excess.
License Title	The **License Title** column is displayed on the **Entitlement Summary** table on the Summary by Installs page. The title for the software as defined in the entitlement.

Term	Definition
column	
License Vendor column	The **License Vendor** column is displayed on the **Entitlement Summary** table on the Summary by Installs page. The vendor for the software as defined in the entitlement.
Licensable toggle	This toggle is displayed on the Usage Summary page. The **Licensable** toggle adds a filter when it's turned on that filters the table to only display the products that are licensable, according to the catalog.
Licensed Software column	The **Licensed Software** column displayed on the **Device Detailed** table on the Summary by Installs page shows the following information. The title for the software installed on a device. The **Licensed Software** column displayed on the **License Demand** table for each of the following License Demand and License Demand - Detailed Reports:

License Demand Report	License Demand Detailed Report
Microsoft Core License Demand page	Microsoft Core License Demand - Detailed Report page
IBM Processor Value Unit (PVU) License Demand page	IBM Processor Value Unit (PVU) License Demand - Detailed Report page
Oracle Processor License Demand page	Oracle Processor License Demand - Detailed Report page
Red Hat Socket Demand page	Red Hat Socket Demand - Detailed Report page

On the these pages the following information is shown:Displays software titles that are part of the License Demand report, where that software also has installations present in the inventory.

Licenses Appli	The **Licenses Applied** column is displayed on the License Summary page.

Term	Definition
ed column	This column provides a count of the licenses that have been applied to the product. If this number is greater than zero it becomes a link to the Licenses / Maintenances page filtered to show the applied licenses.
Links column	The **Links** column is displayed on the Licenses / Maintenances page and Agreements page. Displays the **Parent**, **Associations** and **Children Links** to other entitlements, agreements or contracts configured for the entitlement or agreement.
Machine Name column	The **Machine Name** column is displayed on the Summary by Installs page. The device name where the software is installed. The name is a link that navigates to the **Device Summary** page for the selected device in the **Inventory** application.The **Machine Name** column is also displayed on the License Demand Detailed Reports pages: Microsoft Core License Demand - Detailed Report page IBM Processor Value Unit (PVU) License Demand - Detailed Report page Oracle Processor License Demand - Detailed Report page Red Hat Socket Demand - Detailed Report page The device name, if any, where the software in the License Demand report is installed.
Machine Type column	The **Machine Type** column is displayed on the following License Demand Detailed Reports pages: Microsoft Core License Demand - Detailed Report page IBM Processor Value Unit (PVU) License Demand - Detailed Report page Oracle Processor License Demand - Detailed Report page Red Hat Socket Demand - Detailed Report page The type of the device where the software in the License Demand report is installed. This may be one of: Machine Type --- Cluster Physical Physical Host

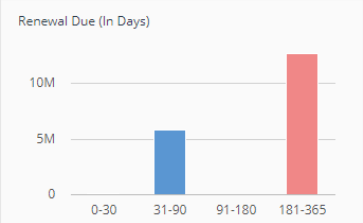
Term	Definition
	Virtual
Maintenance entitlement	A Maintenance entitlement type in AppClarity specifies the rights and limitations for an organization to install and/or use updated versions of software defined in a license. For example you could specify a maintenance entitlement for Microsoft Visio 2016 to cover all new versions from the current date for the next 3 years.
Management Group column	Displays all of the management groups the software reclaim policy is associated with.The **Management Group** column is displayed on the **Entitlement** table on the Summary by Installs page. This column displays the names of the Management Groups an entitlement is associated with.The **Management Group** column is displayed on the **Device Detailed** table on the Summary by Installs page. Displays the number of Management Groups a device is associated with. Clicking on the number displays a popup listing the Management Groups.
Management Group Names column	This column is displayed on the Precedence page. This column contains a **Show** link, which displays a popup containing a list of the Management Group(s) the reclaim policy applies to.
Management Groups	Management Groups are containers used to group devices and the software installed on those devices. Management Groups are defined using configurable rules that look at various properties of the devices and their installed software, these are then evaluated to determine the group membership. This means that Management Group membership adapts to changes to the devices and software in your environment.
Management Groups	Certain pages in AppClarity have a management groups selector. This drop-down lets you select the management group you are interested in. By default this is set to **Global**.

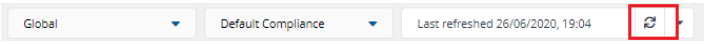
Term	Definition
selector	
Matched Title column	On the reclaim policy pages, this displays the title for the product the reclaim policy will be aimed at.
Matched Vendor column	On the reclaim policy pages, this displays the vendor for the product the reclaim policy will be aimed at.
Matching	The process of taking software product, processor and device data and comparing that with the data held in the 1E Catalog to find a suitable canonical representation. If a completely suitable matching canonical representation is found the software product, processor and device data is said to be normalized. If a suitable matching canonical representation cannot be found the data will be tagged as unmatched and the 1E Catalog will make its best guess at what the canonical representation could be. You can then go through the curation process to either create a new canonical representation or matching rule or both until all the data you need has been normalized.
Matching rules	Matching rules are used to match raw and varied inventory data, which may be imprecise or incomplete, into normalized canonical representations. Software product, processor and device types each have their own canonical schema that enables them to be uniquely identified sufficient for the purposes of the 1E Catalog and its consumers. As a result each of them has a corresponding type of matching rule.
Metric column	The metric type for a license or maintenance entitlement. This may be one of: Type: Core Description: The metric for the license is related to the number of cores present on a device. For example, licenses for **Microsoft SQL database** are related to the number of cores on the server where **Microsoft SQL** is installed.

Term	Definition	
	Device	The metric for the license is for devices. For example licenses for **Microsoft Visio** are on a per device basis. This is the default type.
	Other	This can be used to reference your own license metric type.
	Processor	The metric for the license is related to the number of processors for a device. For example, licenses for certain **Oracle** products are related to the number of processors on the server where the **Oracle** product is installed.
	PVU	The metric for the license is related to the Processor Value Unit present on a device. For example. licenses for **IBM** products are related to the **Processor Value Unit (PVU)** for the device where the IBM product is installed.
	User	The metric for the license is related to the users for the product. For example, **Microsoft Office 365** licenses are related to users and not the devices the software is running on.
Mnt Qty column	The **Mnt Qty** column is displayed on the Summary Report page. The **Mnt Qty** column shows the number of maintenance licenses related to each Entitlement int the table.	
Non-Compliant column	The **Non-Compliant** column is displayed on the Summary by Installs page. This column provides a count of the non-compliant installations for the product.	
Normalization	The process of taking raw inventory data and successfully assigning canonical representations for the software products, processors and devices contained in that data by matching with the 1E Catalog.	
Other Metric	A field in both the New License page and New Maintenance page. This field is only enabled if **Other** is selected in the **Metric Type** for entitlements and allows you to enter a metric that is not covered by the basic **Metric Type** options.	

Term	Definition
Physical Host column	The **Physical Host** column is displayed on the following pages: Microsoft Core License Demand - Detailed Report page IBM Processor Value Unit (PVU) License Demand - Detailed Report page Oracle Processor License Demand - Detailed Report page Red Hat Socket Demand - Detailed Report page The Physical Host, if any, where the software in the License Demand report is installed.
Price per Unit (USD) column	This column is displayed on the Usage Summary page. The **Price per Unit (USD)** shows the cost in USD for each license of a product.
Primary User column	The **Primary User** column is displayed on the **Device Detailed** table on the Summary by Installs page. This column displays the user name for the primary user on a device.
Processor Value Unit (PVU)	A license metric used for IBM products. This value is used by AppClarity to calculate license demand for IBM products. A Processor Value Unit (PVU) is a unit of measure used to differentiate licensing of software on distributed processor technologies (defined by Processor Vendor, Brand, Type and Model Number). IBM currently define a processor, for purposes of PVU-based licensing, to be each processor core on a chip (socket).
Processors column	The **Processors** column is displayed on the following pages: Microsoft Core License Demand - Detailed Report page IBM Processor Value Unit (PVU) License Demand - Detailed Report page Oracle Processor License Demand - Detailed Report page Red Hat Socket Demand - Detailed Report page Displays the number of processors available on the mainboard for the device where the software is installed.

Term	Definition
Product	A product refers to an item that has a known vendor, title, version and edition (VTVE). In AppClarity this is restricted to software products.
Product SKU column	The **Product SKU** column is displayed on the Licenses / Maintenances page. A SKU (pronounced 'skue') is an identification, usually alphanumeric, of a particular product that allows it to be tracked for inventory purposes. In AppClarity, via the 1E Catalog, a SKU is associated with the license metrics and use rights associated with a particular software product purchase.
Quantity column	The **Quantity** column is displayed on the Licenses / Maintenances page. The **Quantity** column displays the number of licenses covered by the entitlement.
Rarely Used column	This column is displayed on the Usage Summary page. The **Rarely Used** column shows the number of installations for each product that have been reported as being rarely used.
Rarely Used Reclaim Action column	Displays the action that will be taken by a reclaim policy for software with a usage category of rarely used. Please refer to Usage categories for more details.
Reclaim Count column	This column is displayed on the Savings page. A count of the number of reclaims performed by applying this policy.
Reclaim Polici	The **Reclaim Policies** column is displayed on the License Summary page.

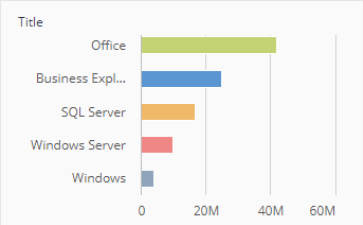
Term	Definition
es column	This column provides a count of the reclaim policies that have been associated with the product. If this number is greater than zero it becomes a link to the filtered to show the associated reclaim policies.
Reclaim policy	A reclaim policy is used to define how to reclaim specific software from specific devices under specific circumstances. There are two general types of reclaim possible: reclaims which are mandatory and reclaims where the user on the device can choose whether the reclaim goes ahead or not. Reclaim policies can also be tied to specific management groups to target specific devices.
Reclaim Savings column	This column is displayed on the Savings page. The sum of the estimated savings made by applying this reclaim policy.
Reclaimable toggle	This toggle is displayed on the Usage Summary page. The **Reclaimable** toggle adds a filter when it's turned on that filters the table to only display the products that have a reclaim policy associated with them.
Remaining column	The **Remaining** column is displayed on the Summary by Installs page. Shows the number of licenses remaining for a particular entitlement after subtracting the **Consumed** licenses consumed from the **Total License Units**.
Renewal Due (In Days) chart	The **Renewal Due (In Days)** chart is displayed on the Summary Report page. This chart shows the number of entitlement renewals that are due within certain numbers of days in the selected Entitlements repository. 

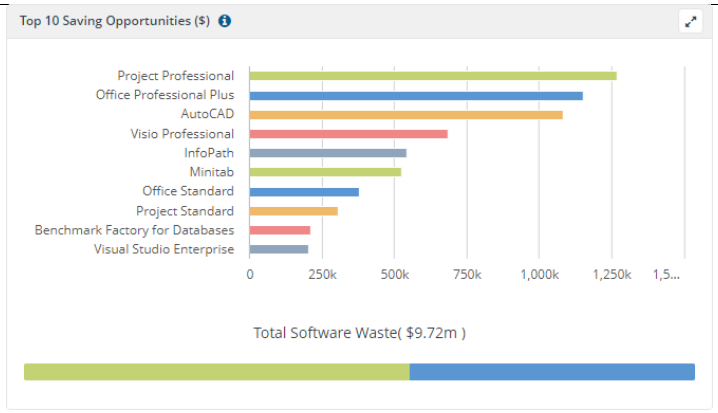
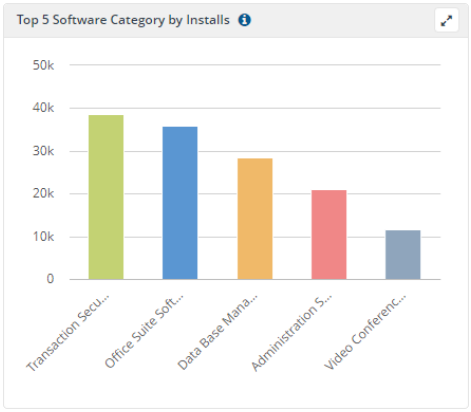
Term	Definition
Report Refresh	You can refresh reports from individual AppClarity screens as well as using the Settings App. Where this is available you can do this by using the refresh icon next to the **Last Refreshed** box: 
Repository	A repository is an SLA Platform term defining a container for specific types of data. There are three types of repository in AppClarity: Inventory (included with SLA Platform) Entitlement Compliance
Risk(Unknown) column	This column displays an indicator for the compliance risk associated with the product. This is based on whether there are certain aspects of the product that are unknown to AppClarity and therefore it cannot determine with certainty the product's compliance status.
Selected Mgmt Grp Policies column	This column is displayed on the Usage Summary page. The **Selected Mgmt Grp Policies** column shows the number of reclaim policies for a product in the currently selected Management Group.
SAM manager	The SAM manager ensures that the SAM team is properly managing their work priorities and creates, validates and distributes reports.
SAM report viewer	The SAM report viewer is a project manager, contract manager or team lead in the BU, who wants to know the costs of the entitlements used in their projects and to validate their compliance with licenses.
SAM team	The SAM team manage entitlement modifications as needed, based on the day-to-day business operations.

Term	Definition
Software Asset Management (SAM)	SAM is the process by which organizations collect data about entitlements, installation and usage of software and the devices the software runs on, how they use that data to ensure that the organization understands whether they are in compliance with their software licenses and if they are using their software assets efficiently. This data, and the tools used to manage the data, must be controlled and protected because the data is company confidential.
Software with conflicting policies toggle	This toggle is displayed on the Usage Summary page. The **Software with conflicting policies** toggle adds a filter when it's turned on that filters the table to only display the products that have reclaim policies that conflict.
Select all button	When AppClarity pages contain a **Select all** button this can be used to check all the checkboxes on the first column of a table, thereby selecting all the items currently displayed in the table.
Site-defined entry	Is an extension to the 1E catalog, which is a matching rule or canonical representation, added by a 1E Catalog curator using their on-site copy of the 1E Catalog.
Sockets column	The **Sockets** column is displayed on the following pages: Microsoft Core License Demand - Detailed Report page IBM Processor Value Unit (PVU) License Demand - Detailed Report page Oracle Processor License Demand - Detailed Report page Red Hat Socket Demand - Detailed Report page Displays the number of processor sockets available on the mainboard for the device where the software is installed.

Term	Definition
Spend (%) column	The **Spend (%)** column is displayed on the Summary Report page. The **Spend (%)** column shows the percentage of the overall spend for each Entitlement in the selected Entitlement repository. The complete bar represents the overall spend, the blue bar indicates the % spend for this Entitlement and the grey bar shows the % remainder.
Start Date column	The **Start Date** column is displayed on the Licenses / Maintenances page.The **Start Date** column shows the date the entitlement will start.
Status column	This column is displayed on the Reclaim History page. This displays the status for the reclaim policy. Status: Failed uninstall no retry — Description: A mandatory policy was run but failed to uninstall the software from the end-user's device. Status: Uninstalled — Description: A mandatory policy was run successfully and uninstalled the software from the end-user's device. Status: User Deferred — Description: For an opt-out reclaim policy the end-user has selected to defer the uninstallation of the software. Status: User OptOut Accept — Description: For an opt-out reclaim policy the end-user selected to keep the software, provided a reason and the AppClarity administrator accepted that reason. Status: User Remove Now — Description: For an opt-out reclaim policy the end-user has selected the Remove this software now button.
Status filter	These are displayed on the Licenses / Maintenances page and Agreements page. The Status filters are displayed in the top-right of the page and let you filter the table according to the status of the items in the table.

Term	Definition
	Clicking on an icon filters the table to display only items with that status, as described in the following table. Icon / Description Filters to show only items in Draft. Filters to show only items in Draft with errors. Filters to show only items in Draft with warnings. Filters to show only items that are Published.
Status icons	These are displayed on the Licenses / Maintenances page and Agreements page. The icon indicates the status of the entitlement or agreement: Icon / Description Draft. Draft with errors. Draft with warnings. Published.
Stock Keeping Unit (SKU)	A SKU (pronounced 'skue') is an identification, usually alphanumeric, of a particular product that allows it to be tracked for inventory purposes. In AppClarity, via the 1E Catalog, a SKU is associated with the license metrics and use rights associated with a particular software product purchase. SKUs are in widespread use throughout the software industry, where publishers refer to their software using a SKU. The SKU gets added to most purchase orders to indicate the software or package being bought. Even small differences between two software titles are indicated by different SKUs. The SKU also indicates the license metrics and maintenance terms associated with the purchase and any additional use rights covered by the purchased license. AppClarity uses the SKU data to automatically:

Term	Definition
	Prefill the settings in an entitlement with the product details, license metrics, and basic maintenance terms that are indicated by the SKU Set the additional use rights that are part of the license indicated by the SKU
Title	The title portion of the vendor, title, version and edition attributes that are used to identify software products. For example, **Visio** or **Nomad**.
Title chart	The **Title** chart is displayed on the Summary Report page. This chart shows the breakdown and numbers for the top 5 software Titles according to their total Entitlements costs in the selected Entitlements repository. 
Title column	The **Title** column in AppClarity pages display information related to the vendor of a product. Depending on the context this may show different things: On entitlement pages this will show:The title portion of the vendor, title, version and edition attributes that are used to identify which software products the entitlement is for. For example, **Visio** or **Nomad**. On the License Position page and License Summary page this will show:The title portion of the vendor, title, version and edition attributes that are used to identify which software product the compliance status relates to. On the Reclaim History page and the Savings page this will show:The title portion of the vendor, title, version and edition attributes that are used to identify which software product the reclaim policy was applied to.
Top 10 Saving Opportunities	This chart shows the top ten products that offer the best savings opportunities in USD. It is calculated by multiplying each product's unit price and the sum of unused and rarely used installations. The bar at the bottom shows the total opportunity in USD split into unused and rarely used installations.

Term	Definition
($) chart	
Top 5 Software Categories by Installs chart	This chart shows the top five categories according to the numbers of installations. This chart disregards Operating Systems and Internet Browser categories. 
Total Consumed column	The **Total Consumed** column is displayed on the Summary by Installs page.Shows the number of licenses consumed by installations from the total available for this product.
Total Cost column	The **Total Cost** column is displayed on the Summary Report page. The **Total Cost** column displays the total cost for the number of licenses and maintenances covered by each entitlement in the table.
Total Devices	The **Total Devices** column is displayed on the License Summary page.This column provides a total count of the devices where the product is installed. This may be different from the **Total Installs** column as some software may be installed more than once on a device.

Term	Definition
column	
Total Installs column	The **Total Installs** column is displayed on the License Summary page.This column provides a total count of the installations for the product. This may be different from the **Total Devices** column as some software, such as Microsoft SQL Server, may be installed more than once on a device.This column is displayed on the Usage Summary page.The **Total Installs** column shows the total number of installations for each product.
Total License Available column	The **Total License Available** column is displayed on the Summary by Installs page .Shows the total number of licenses available for this product from all the entitlements related to it.
Total License Units column	The **Total License Units** column is displayed on the Summary by Installs page.Shows the total number of licenses units available from an entitlement.
Total Licensed Units column	The **Total Licensed Units** column is displayed on the License Position page.Shows the total number of license units available from entitlements related to the product.
Total Units Consumed column	The **Total Units Consumed** column is displayed on the License Position page.Shows the total number of available license units that have been consumed by product installations.
Total Users	The **Total Users** column is displayed on the License Summary page.This column provides the total users accessing the software across all these devices.

Term	Definition
column	
Type column	The **Type** column is displayed on the Licenses / Maintenances page. The **Type** column displays the type of the entitlement in the table. This can be either **License** or **Maintenance**.
Underutilized Installs column	The **Underutilized Installs** column is displayed on the License Summary page. This column provides a count of the installations for the product where the product is rarely used or unused.
Unknown Installs column	The **Unknown Installs** column is displayed on the License Summary page. This column provides a count of the installations for the product where there are details that are unknown, thereby implying a risk for compliance calculation. The **Licensed Software** column displayed on the **License Demand** table for each of the following License Demand and License Demand - Detailed Reports:

License Demand Report	License Demand Detailed Report
Microsoft Core License Demand page	Microsoft Core License Demand - Detailed Report page
IBM Processor Value Unit (PVU) License Demand page	IBM Processor Value Unit (PVU) License Demand - Detailed Report page
Oracle Processor License Demand page	Oracle Processor License Demand - Detailed Report page
Red Hat Socket Demand page	Red Hat Socket Demand - Detailed Report page

This column provides a count of the installations for the software titles that are part of the License Demand report where there are details that are unknown, thereby implying a risk for compliance calculation.

Unreporte	This column is displayed on the Usage Summary page.

Term	Definition
d column	The **Unreported** column shows the number of installations for each product where no recent usage data has been reported.
Unreported Reclaim Action column	Displays the action that will be taken by a reclaim policy for software with a usage category of unreported. Please refer to Usage categories for more details.
Unselect all button	When AppClarity pages contain an **Unselect all** button this can be used to uncheck all the checkboxes on the first column of a table, thereby unselecting all the items currently displayed in the table.
Unused column	This column is displayed on the Usage Summary page. The **Unused** column shows the number of installations for each product that have been reported as not being used.
Unused Reclaim Action column	Displays the action that will be taken by a reclaim policy for software with a usage category of unused. Please refer to Usage categories for more details.
Usage categories	There are four usage categories: used, rarely used, unused and unreported. Usage categories... See Usage categories in Tachyon documentation for more detail. **Device Inventory Date** = maximum of device inventory dates for the consolidated device

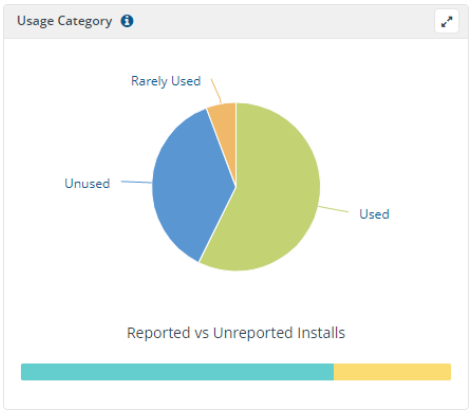
Term	Definition

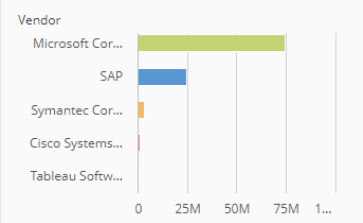
Last Usage Date = maximum of product usage date for the consolidated installation

End of Sync Date = maximum of device inventory dates and maximum usage dates excluding dates in the future

	Device Inventory Date (relative to End of Sync Date)	No Device Inventory Date				
Device Inventory Date < 30 days	Device Inventory Date >30 days	Device Inventory Date > End of Sync				
Last Usage Date (relative to End of Sync Date)	No Last Usage Date					
All Usage on Device > 30 days old since Device	Last Usage Date > End of Sync Date	<=30 days	31-89 days	>=90 da	Device usage	No Device Us

Term	Definition											
	Inventory			ys		age						
	Product Usage across estate	No Product Usage across estate										
	Install Date	Null	**Unreported** - Device stopped reporting usage	**Unreported** - Invalid Usage date	**Used**	**Rarely Used**	**Unused**	**Unused**	**Unreported** - No Product Usage	**Unreported** - No Device Usage	**Unreported** - Device inventory date too old	**Unreported** - Invalid Device inventory date	**Unreported** - No Device inventory date
	< 7 Days	**Unreported** - Recently installed										
	>=7 Days	**Unused**										
	In the future	**Unreported** - Invalid install date										
Usage Cate	The Usage Category chart is displayed on the Usage Summary page.											

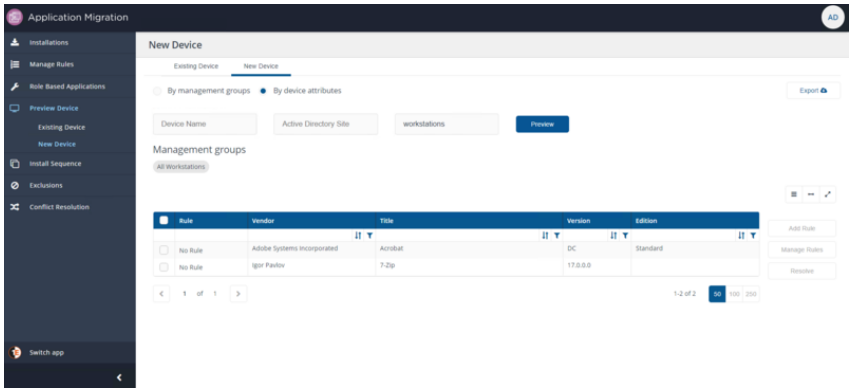
Term	Definition
gory chart	This chart shows the distribution of installations into the three usage categories: User, Rarely Used and Unused as a percentage of the total installations that reported usage. The bar at the bottom shows the number of installations with reported versus unreported usage as a percentage of the total number of installations. 
Used column	This column is displayed on the Usage Summary page. The **Used** column shows the number of installations for each product that have been reported as being used.
Used Reclaim Action column	Displays the action that will be taken by a reclaim policy for software with a usage category of used. Please refer to Usage categories for more details.
Vendor	The vendor portion of the vendor, title, version and edition attributes that are used to identify software products. For example, **Microsoft Corporation** or **1E**.
Vendor chart	The **Vendor** chart is displayed on the Summary Report page. This chart shows the breakdown and numbers for the top 5 Vendors according to their total Entitlements costs in the selected Entitlements repository.

Term	Definition
	
Vendor column	The **Vendor** column in AppClarity pages display information related to the vendor of a product. Depending on the context this may show different things: On entitlement pages this will show:The vendor portion of the vendor, title, version and edition attributes that are used to identify which software products the entitlement or agreement is for. For example, **Microsoft Corporation** or **1E**. On the License Position page and License Summary page this will show: The vendor portion of the vendor, title, version and edition attributes that are used to identify which software product the compliance status relates to. On the Savings page this will show: The vendor portion of the vendor, title, version and edition attributes that are used to identify which software product the reclaim policy was applied to.
Vendor, title, version and edition	The vendor, title, version and edition attributes are used to identify software products and to determine whether specific installations are related to that product.
Version	The version portion of the vendor, title, version and edition attributes that are used to identify software products. For example, **11.0.3216.5614** or **6.3.100.0**. See also Colloquial version.
Version column	The version column in AppClarity pages display information related to the version of a product. Depending on the context this may show different things: On reclaim policy pages this will show: On reclaim policy pages the version column shows the version string set for the policy. This may display a single version. On the

Term	Definition
	Precedence page this will show: The version portion of the vendor, title, version and edition attributes for the product that the reclaim policy applies to. On the Reclaim History page this will show: The version portion of the vendor, title, version and edition attributes that are used to identify which software product the reclaim policy was applied to.
VTVE	An AppClarity abbreviation for the vendor, title, version and edition of a software product.

11 Application Migration

Application Migration intelligently automates the migration of applications during a Configuration Manager OS deployment. Using migration rules (defined by an administrator), previously installed applications can be reinstalled, upgraded or replaced with an alternative during an OS deployment task sequence.



11.1 Introducing Application Migration

Application Migration intelligently automates the migration of applications during a Configuration Manager OS deployment. Using migration rules (defined by an administrator), previously installed applications can be reinstalled, upgraded or replaced with an alternative during an OS deployment task sequence.

These rules can include usage criteria, allowing you to choose to only install previously installed applications if they were being used, or perhaps replace a rarely used application with a less costly alternative. This functionality enables applications to be actively rationalized during an OS migration exercise, standardizing on products and versions and reclaiming unused software.

Application Migration uses a custom Configuration Manager task sequence step. Tachyon provides inventory data from Configuration Manager, normalized through the 1E Catalog, that it uses to determine the applications installed and used on each computer.

The **1E Application Migration** task sequence step is added to an existing OS Deployment Task Sequence. This step calls the Application Migration API on the Tachyon Server to return a list of Configuration Manager Applications and Packages that need to be installed, based on the source computer's inventory and applicable Application Migration rules. The Applications and Packages are installed using the standard Configuration Manager **Install Application** and **Install Package** steps, each configured to install based on dynamic variables defined in the **1E Application Migration** step. For details, please refer to Using Application Migration in a task sequence.

11.2 Implementing Application Migration

Information for preparing, installing and upgrading Application Migration.

11.2.1 Design Considerations

Information that will help you design and plan the implementation of Application Migration in your organization.

11.2.1.1 Options for using Application Migration

To install migrated applications and packages in the Refresh and Replace OS Deployment scenarios, Application Migration provides a custom action that must be added to your task sequences to supplement the **Install Application** and **Install Package** actions.

You can use these actions in your own task sequences, as described in Using Application Migration in a task sequence, and deploy them using Software Center or other means.

You can further simplify your processes and end-user experience by using 1E Shopping self-service features, where users use the Shopping web portal to start their own OS upgrades and migrations. The Wizards allow users to see a list of applications that are currently installed and the corresponding applications that will be installed as a result of applying the defined Application Migration rules.

In each case:

Shopping OSD Wizard (Applications to reinstall page).

Shopping WSA Wizard (Applications page).

For users requesting a self-service OS migration from the Shopping Web:

they cannot choose the applications to reinstall during a self-service OS migration.

if you previously used the AppMapping feature and have migrated to Application Mapping, users will see a list of their previously shopped for apps in My Software.

For administrators shopping on behalf of others:

on the Reinstall tab, the option to choose specific application to be reinstalled on machines is not available.

on the Select New Apps tab, only applications that come with the new OS are listed and the option to select additional applications as part of this deployment is not available.

OSD mapping rules and OSD machine mapping details are not available.

Note

Shopping documentation is now available on our new site .

11.2.1.2 Preparing Tachyon platform 8.1

Application Migration 8.1 requires Tachyon platform 8.1.

Current status	Option
Tachyon platform is *not* installed.	Use Tachyon setup to install Tachyon platform. We recommend installing Application Migration at the same time, but you can install it later. Please refer to: Planning for Tachyon and Installing Tachyon for details on preparing for and installing the platform. Installation includes an extract from Tachyon setup for installing Application Migration.
You have an older version of Tachyon platform and Application Migration already installed.	Use Tachyon setup to install Tachyon platform 8.1. You must choose to install Application Migration 8.1 at the same time. Please refer to: Planning for Tachyon and Upgrading Tachyon Platform for details on preparing for and upgrading to Tachyon platform. Installation includes an extract from Tachyon setup for installing Application Migration.
If you are using Application Migration 2.5 on SLA Platform 3.3 and now want to upgrade to Application Migration 8.1.	Upgrade your existing SLA Platform 3.3 to Tachyon platform 5.2 first, then upgrade to Tachyon platform. Upgrading Tachyon Platform When you perform each upgrade, ensure you also install Application Migration at the same time, using Tachyon setup. If you are using Nomad, then you must also review Upgrading Nomad, before upgrading Tachyon platform. This is because Tachyon platform 5.2 and later replaces ActiveEfficiency with Content Distribution. When upgrading, you will need to consider the following choice to ensure your existing Application Migration Task Sequence steps and Shopping integration settings will continue to work after the upgrade. Either modify your existing Task Sequences (TS).

Current status	Option
	Ensure the Tachyon Platform (Master Stack) website provides the same binding(s) used by existing TS. The choice depends on which DNS Names you want to use. Please refer to DNS Names. When Using Application Migration in a task sequence, your Application Migration TS step includes **Web Server Base URL**, which uses a server or DNS Name, and either HTTP or HTTPS. Tachyon platform 5.2 and later, allows you to specify an additional (alternate) HTTPS binding during setup. Please refer to Website configuration. By default, Tachyon setup creates the following bindings:

Reference	Default binding	What you can do during Setup
HTTP	HTTP - platform server name (eg. ACME-TCN01.ACME.LOCAL) - Port 80	You can change the port. For example change it to 8080 to match the default HTTP port used by SLA Platform 3.3. If for any reason you want to keep HTTP port 80 for other purposes, you can manually add an HTTP binding to the website after installation. If your TS uses a different host header, then you can specify this during setup.
Main HTTPS	HTTPS - DNS Name (included in the web server certificate) - port 443	You can change the DNS Name and port, for example to 8443 to match the default HTTPS port used by SLA Platform 3.3. We recommend you do not change this binding just for the benefit of Application Migration. This is because this binding is typically used by administrators to connect to the platform

Current status	Option	
		website, and also for platform clients if the server has Response Stack components (Switch and Background Channel). If you do not wish to edit your TS then we recommend you use the Alternate HTTP binding during Setup, or manually create an additional HTTPS binding after installation.
Alternate HTTPS	Optional HTTPS - DNS Name (included in the web server certificate) - port 443	You can optionally configure the Alternate HTTPS binding during Setup, for the TS to connect to. This is the recommended choice if you do not wish to edit your existing TS. If you need to use the Alternate HTTPS binding for other purposes, then you can manually create an additional HTTPS binding after installation.

If SLA Platform was configured to use HTTPS it is likely that you will need to generate a new Web Server certificate for Tachyon platform that meets the additional requirements of the platform, please refer to Web Server certificate for more information.

> **Note**
>
> Tachyon setup 8.1 includes 1E Catalog 8.1, and expects Catalog to be installed on the Tachyon platform server. If your existing SLA Platform system has a remote Catalog server, then you will need to consider relocating it. Relocation probably means changing your firewall and whitelist settings. Please refer to Requirements: Whitelisting connections to 1E Cloud.

AI Powered Auto-curation

This feature was introduced in Tachyon 5.x. Using the AI Powered Auto-curation feature, you'll be able to increase the total amount of normalized software in your Inventory repositories. This is done using AI that integrates with the inventory consolidation

process. By using AI, your organization will benefit from significant numbers of normalized software and a reduced manual effort needed to normalize software.

For details of additional hardware requirements, please refer to AI Powered Auto-curation.

Note

The Web Service used by Application Migration is provided by the Platform web application of the Tachyon website. This is configured by default to use Windows Authentication and its clients do not need to provide client certificates.

11.2.2 Requirements

Application Migration is implemented as an application that runs on the Tachyon platform, which includes SLA and 1E Catalog components. Please refer to Installing Tachyon for more details. Application Migration is licensed through the platform. You will require a license file including Application Migration. Refer to License requirements for more information.

11.2.2.1 Accounts needed to install Application Migration

11.2.2.1.1 Installing Application Migration on Tachyon platform

The user installing Application Migration on the platform needs the following permissions:

Have local admin rights on your Tachyon server.

Be an existing platform user with the **Full Administrator** role.

Note

For a new installation of Tachyon, the only account that exists in Tachyon will be the **installation account**, which by default is assigned to the Tachyon role listed above. You will need to add users and assign roles to them.

When upgrading from SLA Platform, SLA users are migrated to Tachyon, but are not assigned to any roles. You will need to assign users to appropriate roles in Tachyon.

For steps on viewing existing users and adding a new user in Tachyon Platform 8.1, please refer to the Users and Groups page.

Warning

When installing Tachyon or upgrading from SLA Platform, do not install Tachyon using an **installation account** that you also intend for using and administrating Tachyon and Application Migration. The Tachyon **installation account** is purposefully given limited capabilities, which can't be easily edited later.

A recommended workaround for this is to add the **installation account** to an AD security group, and then assign the security group to appropriate roles in Tachyon, for example Full Administrator.

11.2.2.1.2 Installing 1E Task Sequence Tools

The 1E Task Sequence tools are installed on the Configuration Manager site server, SMS provider and any devices on which the Configuration Manager console is installed.

The user installing **1E Task Sequence Tools** needs the following permissions:

Have **local admin rights** on the device you are installing on.

Be a **Full Administrative user** in Configuration Manager.

11.2.2.1.3 Service Accounts

Details of platform service accounts are included in Service accounts.

The SQL Login that is used by the Tachyon server web applications and services depends on whether the SQL Server is remote from the Tachyon server or is local, as described in the following table.

Installation scenario	Service account SQL Login
Server is remote from SQL.	The computer account of the remote server. For example **ACME\ACME-TCN01$**
Server and SQL are local.	The local network service account, **NT AUTHORITY\NETWORK SERVICE**

> **Note**
>
> Before upgrading Tachyon, or installing or upgrading Consumer applications like Application Migration or AppClarity, the SQL Login must be granted the following rights to support Database Snapshot of the 1E Catalog and SLA databases, to restore them if an error occurs:

dbcreator rights on the SQL database instance hosting the 1E Catalog database.

dbcreator rights on the SQL database instance hosting the SLA databases.

During installation, setup will always:

Attempt to create the SQL Login.

Grant it **db_owner** permission on each of the Tachyon databases.

Remove the **db_owner** permissions when installation is completed.

11.2.2.2 Accounts needed to use Application Migration

Tachyon platform uses Role-based Access Control to associate users with the tasks that they are required to perform. The **Application Migration Administrator** role is the only role associated with Application Migration. Other platform roles are required in order to complete some post-installation setup and ongoing management of the platform necessary for Application Migration to

function, but not considered part of the day-to-day operation of an Application Migration administrator.

> **Note**
>
> The user that installed Tachyon (the Tachyon Installation Account) is assigned the Permissions Administrator role so can be used to add other users and assign roles to them, but you cannot add or change the roles assigned to the original Tachyon Installation Account. It is therefore important to install Tachyon with an account that will NOT be using Application Migration (or any other platform applications for that matter) after installation.

> **Note**
>
> If you upgraded SLA Platform 3.3 to Tachyon platform 8.1, all previously defined users will be present in the platform, but will not be assigned any security roles. You will need to assign the appropriate roles after upgrading the platform.

There are three types of users that are involved in the setup and operation of Application Migration.

11.2.2.2.1 Platform administrator roles

These are users who can manage users, connectors, management groups and other common components in the platform. These users are typically set up after installing the platform and can be added at any time by other platform administrators (specifically users with the **Full Administrator** or **Group Administrator** role).

Application Migration is a platform application and has a dependency on certain platform components, such as Users, Connectors and optionally Management Groups, Tasks associated with these components would typically be performed by a platform administrator (a user with the **Full Administrator** role). In smaller organizations, or organizations only using the platform for Application Migration, it is likely that the same one or two people will be responsible for managing all aspects of the platform as well as managing Application Migration. In this scenario, it is likely that those users would be assigned the **Full Administrator** role in the platform. Other organizations may be using several platform applications and may want to restrict the number of users that have the **Full Administrator** role.

Refer to Users and Groups page for details on how to add users and assign security roles in the platform.

11.2.2.2.2 Application Migration Administrators role

These are platform users who can use the Application Migration application for day-to-day operation.

In order to use Application Migration, users must be added and assigned the **Application Migration Administrator** role in the platform. This role is added to the platform when Application Migration is installed, so you will need to install Application Migration first, then add users and assign them to the **Application Migration Administrator** role as required.

Alternatively, you can create your own custom role, which must have the following permissions assigned as a minimum.

Name	Type	Permissions
Connector	Connector	Execute.
Process log	Process log	Read.
Repository: Inventory	Repository: Inventory	Read, Write, EvaluateManagementGroups, Populate.
Inventory	Inventory	Read.
Inventory: Association	Inventory: Association	Read, Write, Delete.
Repository: Application migration	Repository: Application migration	Read, Write, Delete, Archive, Populate.
ProviderConfiguration	ProviderConfiguration	Read.
ProviderOperationLog	ProviderOperationLog	Read.

11.2.2.2.3 Task Sequence step user

This is the account specified in the Application Migration Task Sequence step used to connect to the Application Migration API (one of the SLA Provider API). It must be a platform user, but it does not require any specific roles to be assigned.

It can be either a dedicated user account or the Configuration Manager Network Access Account.

11.2.2.3 Supported Platforms

11.2.2.3.1 Tachyon server components

Note

Application Migration requires Tachyon platform. Only the Tachyon Master Stack is required, a Response Stack is not required unless you also want to use the platform's real-time features. Because Application Migration is an application on the platform, the list of Supported Platforms for Application Migration is identical to Tachyon platform.

For full details, refer to Tachyon Platform 8.1 - Supported Platforms

11.2.2.3.2 System Center Configuration Manager connector

The list below shows the versions of Configuration Manager supported by Tachyon Platform 8.1, please refer to System Center Configuration Manager connector for detailed prerequisites and configuration.

SCCM CB 2203

SCCM CB 2111

SCCM CB 2107

SCCM CB 2103

SCCM CB 2010

11.2.2.3.3 1E Client

Note

This version of Application Migration requires 1E Client 8.x with the Shopping client enabled. Shopping client provides WSA features.

Refer to Supported Platforms for details about:

Windows clients

macOS clients

Linux clients

Solaris clients.

11.2.2.3.4 PowerShell

PowerShell 4.0 or later, is required by the Application Migration Task Sequence step. The step executes in a Configuration Manager OS deployment task sequence after the new OS is installed.

11.2.2.4 1E Companion Products

Supported versions of 1E companion products that Application Migration features depend on.

Products and features that Application Migration depends on	Supported versions of companion products	
Tachyon platform	Required by all Application Migration features. The platform Master Stack installation is required with the System Center Configuration Manager connector enabled. The Tachyon Response Stack is only required if you will be using additional platform real-time features outside of Application Migration.	Tachyon Platform 9.0 and later
1E Client	1E Client, with Shopping client enabled, needs to be deployed to devices if using Application Migration with	1E Client 24.5 Long-Term

Products and features that Application Migration depends on	Supported versions of companion products	
	1E Shopping and Windows Self-service Assistant (WSA). 1E Client, with platform client enabled, does not need to be deployed to devices unless platform real-time features are required by other 1E applications.	Service Branch (LTSB) if using platform v9.1 1E Client 9.0

Supported versions of 1E companion products with features that depend on Application Migration.

Products and features that depend on Application Migration	Supported versions of companion products	
Shopping	Self-service OS deployment integrated with Application Migration. Optional feature.	Shopping 6.1 Shopping 6.0 (with hotfixes)

11.2.2.5 Networking

11.2.2.5.1 Firewall

Port	Traffic	Notes	Configurable
TCP 80 (HTTP)	Inbound/Outbound	Used by the website hosting the SLA Operations Provider API for HTTP traffic.	Yes, during installation.
TCP 443 (HTTPS)	Inbound/Outbound	Used by the website hosting the SLA Operations Provider API for all HTTPS traffic. A web server certificate is required.	Yes, during installation.

Note

Previous versions of the SLA Platform used port 8080 by default for HTTP communication. If you are upgrading from SLA Platform 3.3 to platform 8.1 or later, you should retain the port settings currently used by SLA Platform by defining the port on the Web Site Configuration page of platform setup.

For full details of communications, please refer to Communication Ports.

11.2.3 Installation

11.2.3.1 Installing Application Migration

Application Migration is installed through Tachyon platform setup. The **Select Configuration** section of platform setup allows you to choose whether to install AppClarity. Refer to Tachyon Setup.

11.2.3.2 Relicensing Application Migration

Licensing of Application Migration and later is handled through the platform. You will no longer need to license Application Migration using the installer. Refer to the Tachyon Setup for details about license requirements.

11.2.3.3 Installing the 1E Task Sequence tools

The 1E Task Sequence Tools installer extends the Configuration Manager Task Sequence Editor, adding the Application Migration step that can be added to OS deployment task sequences. This step executes during the OS deployment, calling an Application Migration API that returns a list of Configuration Manager Applications and Programs to be installed on the computer being deployed.

Install the 1E Task Sequence Tools on the following systems:

The Configuration Manager Primary Site server. In a multi-site hierarchy, install it on the CAS and each primary site.

If any site has one or more remote SMS Providers, install it on each remote SMS Provider server.

Any remote Configuration Manager console systems that are used to edit task sequences.

Version 2.5.300 of the 1E Task Sequence tools installer is included in the Windows Serving Suite 4.1 download zip, and in its own download zip, which can be downloaded from the 1E Support Portal.

To install the 1E Task Sequence Tools:

Start a command prompt with elevated rights and run the following command-line from the location the installer was downloaded:

```
msiexec /i 1ETaskSequenceTools.msi /l*v C:\Temp\TSTools-Install.log
```

On the **Welcome screen**, click **Next**.

On the **License Agreement screen**, accept the terms of the agreement and click **Next**.

On the **Ready to Install screen**, click **Next**.

On the **Completion screen**, click **Finish**.

11.2.3.3.1 Reviewing 1E Task Sequence Tools installation

To review your Task Sequence Tools installation:

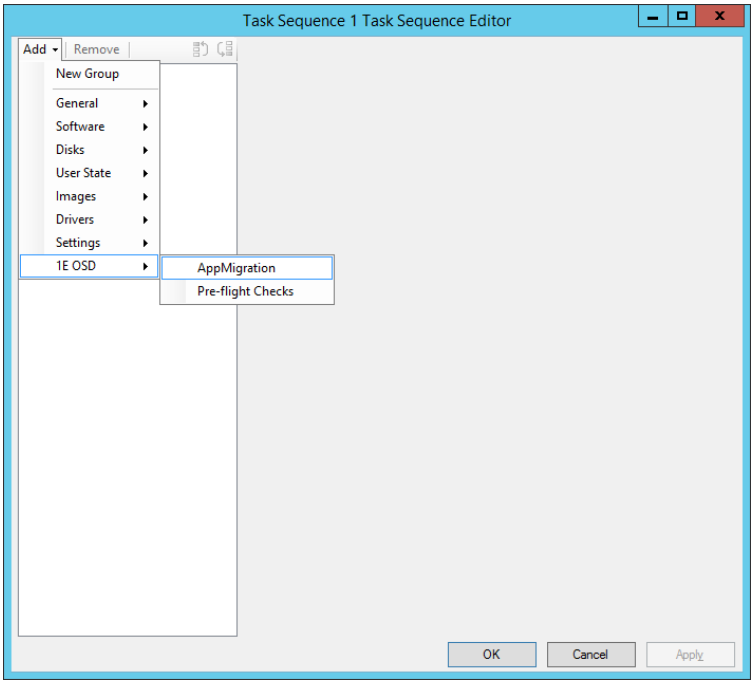
From your **Configuration Manager console**, choose the **Software Library workspace**.

Expand the **Operating Systems folder** and select **Task Sequences**.

Right-click any task sequence and from the context menu, choose **Edit**.

In the **Task Sequence Editor** dialog, click **Add** (located top left in the dialog) and ensure that the **1E OSD** group appears and it contains the **AppMigration** Task Sequence step, as shown in the picture opposite.

Exit the **Task Sequence Editor** without making any change by clicking **Cancel** .



11.2.4 Post-install configuration

Steps to configure Tachyon platform after installation of Application Migration.

11.2.4.1 Application Migration roles

Assign users to roles as described in Requirements: Accounts needed to install Application Migration.

The **Application Migration Administrators** role does not exist in the platform until Application Migration is installed. Add this role to all users that need to configure and operate Application Migration.

Platform administrator roles are required to perform the tasks described on this page.

11.2.4.2 Enable Auto Install for Configuration Manager Applications and Packages

Application Migration uses the **Install Application** and **Install Package** steps in a Task Sequence to install migrated applications and packages. These Task Sequence steps are dependent on the relevant checkbox (auto install flag) being enabled for *each* application and package:

Allow this application to be installed from the Install Application task sequence action without being deploye d

Allow this program to be installed from the Install Package task sequence action without being deployed.

If a checkbox is not enabled, the software installation will fail for that application or package. An administrator can enable this checkbox for each application and package by using either of the following methods:

in Configuration Manager during or after creating each application and package.

using the **Auto Install** feature in Application Migration when creating application associations, rules or Role Based Application sets.

For information about where to manually enable the checkbox for applications and packages in Configuration Manager, please refer to Using Application Migration in a Task Sequence: Auto Install for Configuration Manager Applications and Packages.

11.2.4.2.1 Auto install configuration

To use the **Auto Install** feature, you'll first need to configure the following providers in the **Settings** application of Tachyon platform:

Set Auto-Install option in SCCM

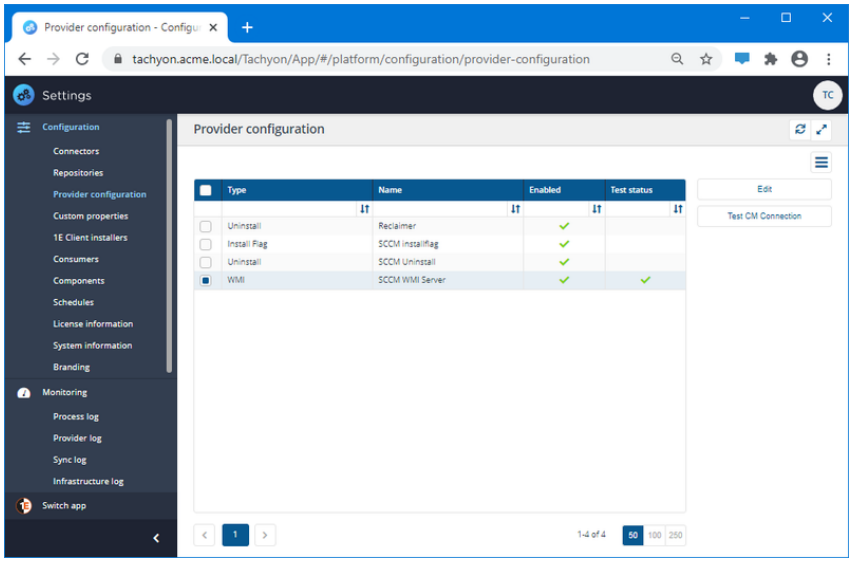
SCCM WMI Server

First grant the user account you want to use to configure provider related details with the role **Provider Configuration Administrators**. This role allows you to Update, delete and view provider configurations.

Once you have granted the **Provider Configuration Administrators** role, login to Tachyon platform with the user account and enable the providers.

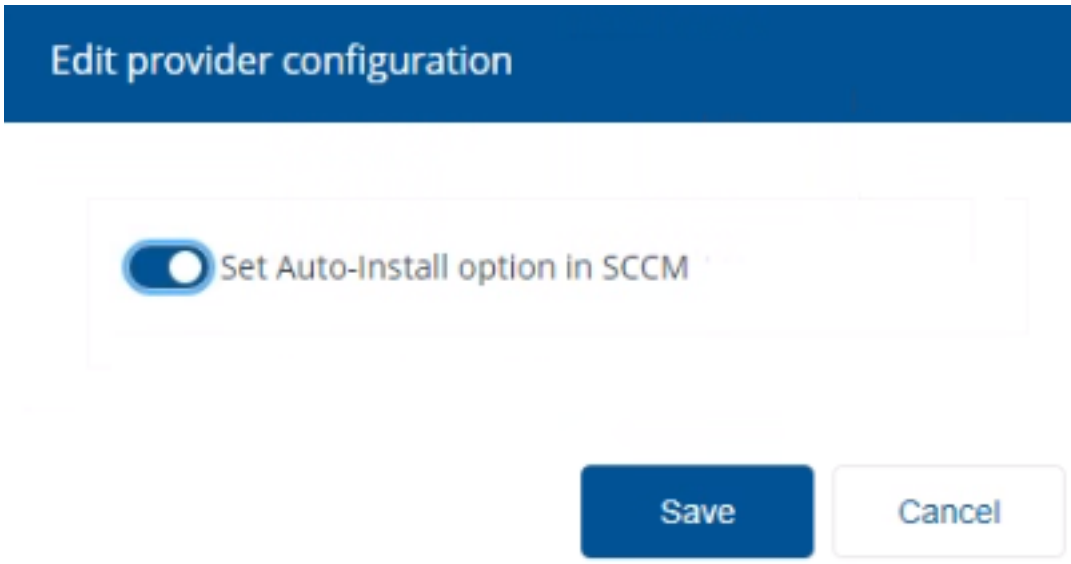
> **Note**
>
> Before you can enable the provider configuration, make sure you have configured a System Center Configuration Manager connector. If you do not have a System Center Configuration Manager connector the SCCM providers will not be visible. Refer to System Center Configuration Manager connector.

> **Warning**
>
> If these providers are not configured correctly, the **Auto Install** status icon in the Migration Rules page may remain spinning, if the appliaction or program has not had its auto install flag already enabled manually outside of Application Migration.



11.2.4.2.2 The Set Auto-Install option in SCCM provider

The **Set Auto-Install option in SCCM** provider is used by the **Auto Install** feature, and must be enabled to allow Application Migration to enable relevant checkboxes (flags) in Configuration Manager applications or packages.



To set the provider configuration:

Navigate to **Settings→Provider configuration**.

Select the provider with the name **Set Auto-Install option in SCCM** and click **Edit**.

In the **Edit provider configuration** popup, toggle this control to on (to the right) to enable **Set Auto-Install option in SCCM**.

Click **Save**.

11.2.4.2.3 Enabling SCCM WMI Server

The WMI provider holds the connection details of the Configuration Manager server.

To set the provider configuration:

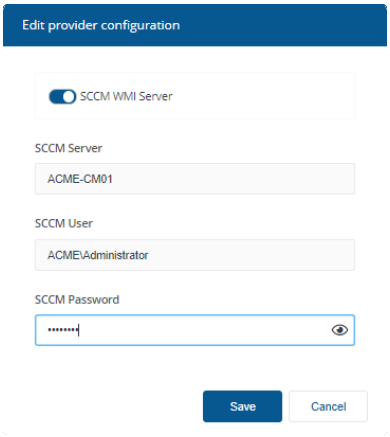
Navigate to **Settings→Provider configuration**.

Select **SCCM WMI Server** and click **Edit**.

In the **Edit provider configuration** popup, slide the **SCCM WMI Server** toggle to on and complete the displayed form using the following information as guidance:

Field	Description
SCCM WMI Server	Toggle this control to on (to the right) to enable the **SCCM WMI Server**.
SCCM Server	Enter the name of the Configuration Manager server. In our example this is **ACME-CM01**. In a Microsoft Endpoint Configuration Manager hierarchy, this would be the CAS.
SCCM User	The credentials for provider **SCCM WMI Server** may differ from those used for your System Center Configuration Manager (SCCM) connector. Make sure the credentials used here have SCCM administrator rights. SCCM Uninstall must be run under an account that's a member of the **dbcreator** server role on the database server where the SCCM database is hosted, in our example this would be **CM_CM1** on **ACME-SQL01**. The **SCCM User** account in our example is **ACME\Administrator**.
SCCM Password	The password for the **SCCM User** account.

When you have entered the correct information, click **Save**.



11.2.4.2.4

11.2.4.2.4.1 Testing SCCM WMI Server

As the SCCM WMI Server provider defines how all the SCCM providers access Configuration Manager - you should test the details and credentials you have entered as soon as the provider has been saved.

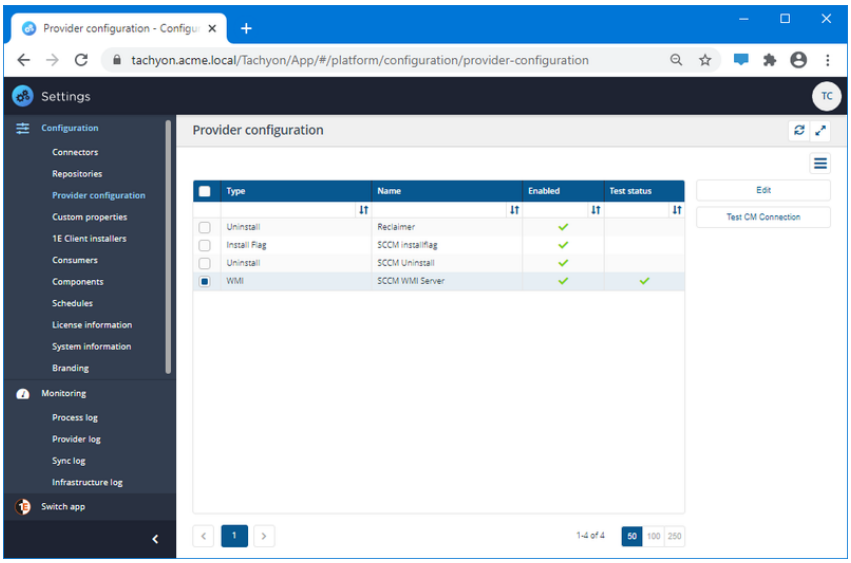
Navigate to **Settings→Provider configuration**.

Select the provider with the name **SCCM WMI Server.**

Click on the **Test CM Connection** button, this button is enabled when only the **SCCM WMI Server** provider has been selected.

A test will be scheduled to run. When the test has completed successfully a green checkmark appears in the **Test status** column for the **SCCM WMI Server** row in the table, as shown in the picture opposite.

If the test fails you will need to recheck the details and credentials you have provided, making sure that the selected account has necessary permissions as described in Enabling SCCM WMI Server.



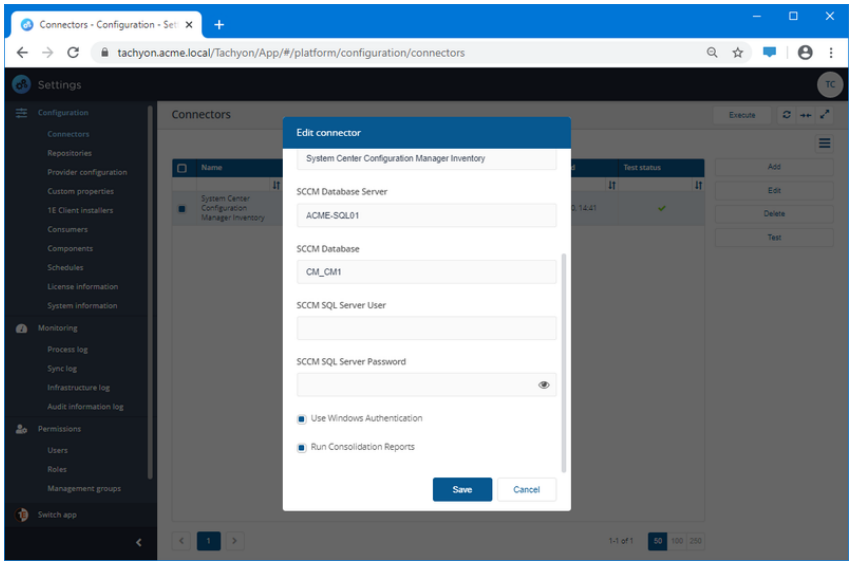
11.2.4.3 Configure a System Center Configuration Manager inventory connector

Application Migration requires software inventory and application configuration data from Configuration Manager. To get this data, Application Migration uses the Tachyon platform **System Center Configuration Manager Connector** to populate an Inventory repository. By default, Application Migration uses the **Default Inventory** repository.

To perform this task you will need to be logged into the platform as a user with the Connector Administrator role. Connectors are configured from the **Settings** app. Refer to System Center Configuration Manager connector.

> **Note**
>
> The platform can collect inventory data from other data sources using different connectors. However, Application Migration requires the Configuration Manager connector to be used as this connector also collects details of Configuration Manager Applications, Packages and Programs that are used to install migrated applications when the Configuration Manager Task Sequence is executed.

When setting up the connector you should check the **Run Consolidation Reports** option in the **Edit connector** popup. Doing this ensures that every report needed to display data in Application Migration will be run when the inventory connector is executed. If you do not do this, you can always run the consolidation actions independently of the connectors, as described in Executing the consolidation actions independently.



11.2.4.3.1 Execute the System Center Configuration Manager inventory connector

Once the System Center Configuration Manager inventory connector has been added it needs to be executed to synchronize the data from Configuration Manager into Application Migration. To do this you'll need to be logged into Tachyon platform as a user with the Application Migration Administrator role, or any other role that includes permission to execute a connector.

Note

Connectors can be executed in the **Settings** app from either the **Configuration**→Connectors page or the **Monitoring**→Process Log page. The steps below use the **Process Log** page as Application Migration Administrators have access to this page but not the Connectors page.

To execute the connector:

From the **Settings** app, go to the **Monitoring**→Process Log page.

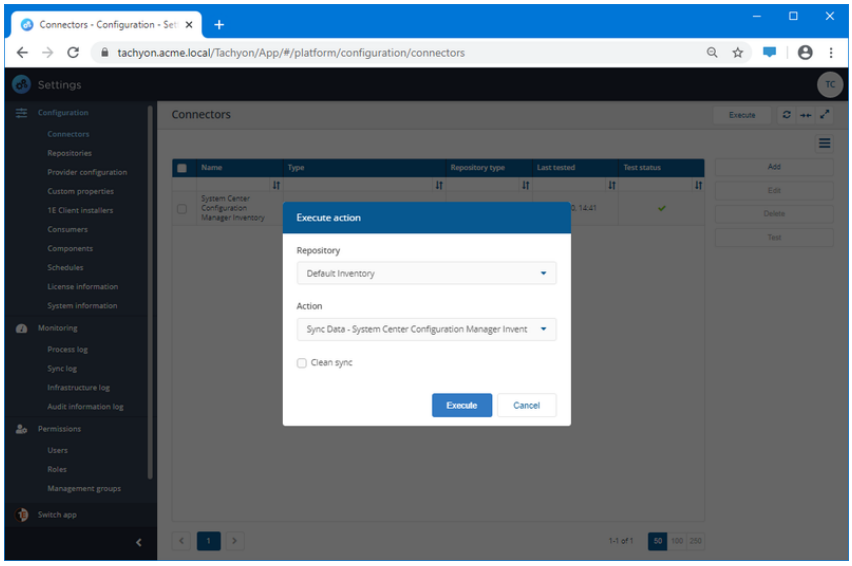
Click on the **Execute** button on the top right of the page.

Select the inventory repository in the **Execute action** popup. Typically, this will be the **Default Inventory** repository, unless other Inventory repositories have been created specifically for use by Application Migration.

Select the **Sync Data** action for the System Center Configuration Manager connector.

Click on the **Execute** button in the **Execute action** popup.

The picture shows the **Execute action** popup with the **Default Inventory** selected and the **Sync Data - System Center Configuration Manager Inventory** action selected.



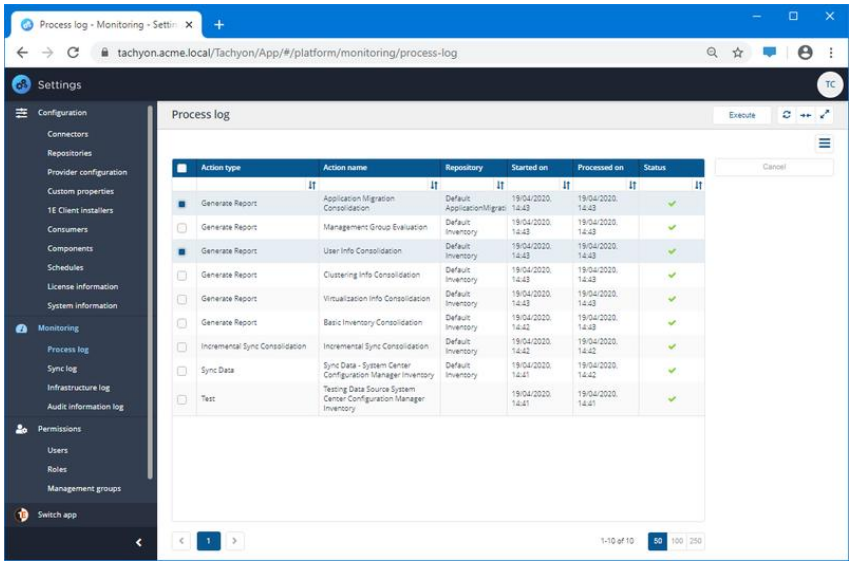
11.2.4.3.2 View the Process log

When the connector is executed, the progress of the synchronization can be checked in the **Settings** app from the **Monitoring→Process log** page. To perform this task you will need to be logged into the platform as a user with the **Application Migration Administrator** role, or any other role that includes permission to view the **Process Log**.

The picture shows the **Monitoring**→**Process log** page where the data sync using the System Center Configuration Manager Inventory connector was executed.

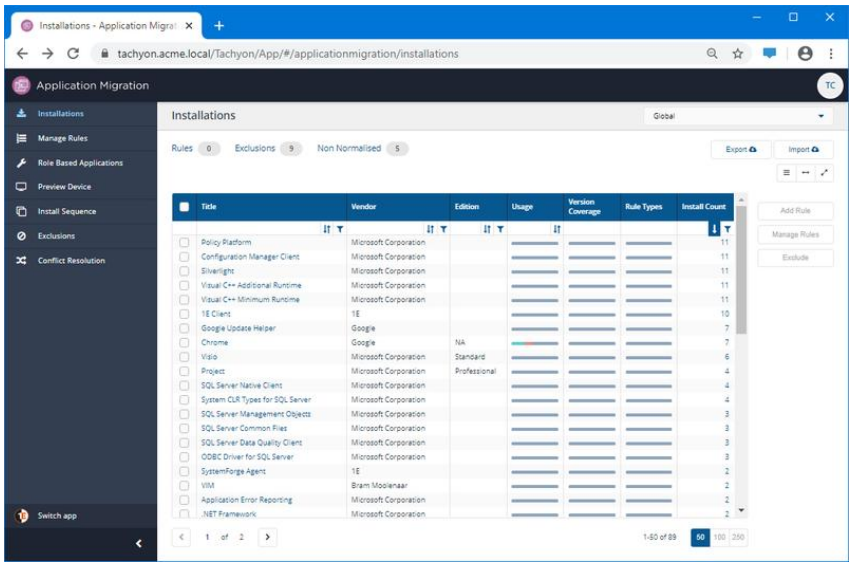
Note

A number of other steps follow the initial sync, including the **Basic Inventory Consolidation** report and the **Application Migration Consolidation** report, as highlighted. These reports were run automatically after the data sync as the option to Run Consolidation Reports was checked when the connector was added. The Application Migration Consolidation report is the last step in getting the data ready for Application Migration.



11.2.4.3.3 View data on the Application Migration Installations page

Once the reports have been run you will be able to see data in the Application Migration app on the **Installations** page, as shown.



11.2.4.3.4 Scheduling the connector to keep data synchronized

The process above executes a single, on-demand synchronization of data from Configuration Manager into Application Migration. You should schedule the connector to execute regularly to

keep the data in Application Migration up to date, ensuring new devices, new software installations and software removals are correctly reported.

To perform this task you will need to be logged into Tachyon platform as a user with the **Schedule Administrator** role. The **Application Migration Administrator** role does not have the required permissions to schedule connectors. Refer to Schedules page.

11.2.4.4 Executing the consolidation actions independently

There are scenarios where you would want to execute the consolidation reports separately from an inventory synchronization, for example you may have a number of inventory connectors connecting into different data sources. In this case you would want to perform all the synchronizations before executing the consolidation actions.

There are two consolidation actions you need to execute for Application Migration:

Basic Inventory Consolidation.

Application Migration Consolidation.

11.2.4.4.1 Executing the Basic Inventory Consolidation action

The **Basic Inventory Consolidation** report can be run independently of the **Settings** app:

Clicking the **Execute** button in either the **Configuration**→**Connectors** or **Monitoring**→**Process log** pages.

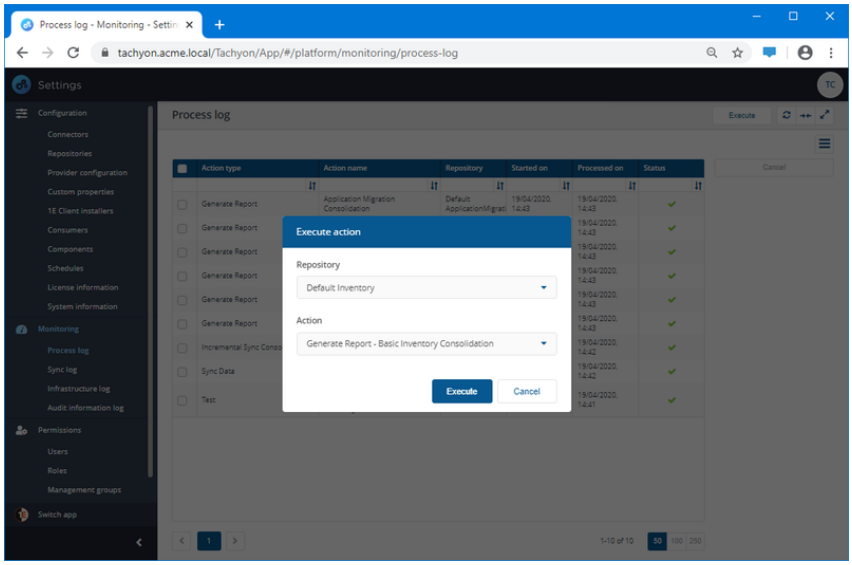
> **Note**
>
> Users assigned the **Application Migration Administrator** role will only be able to run the Basic Inventory Consolidation report from the **Process Log** page.

Selecting an Inventory repository.

Selecting the **Generate Report - Basic Inventory Consolidation** action.

Clicking the **Execute** button in the **Execute action** popup.

> **Note**
>
> Running the Basic Inventory Consolidation report will also run the Application Migration Consolidation report.



11.2.4.4.2 Executing the Application Migration Consolidation action

You may want to run the Application Migration Consolidation report independently after deleting a Management Group or fixing an orphaned Application Migration rule to update the data in the Application Migration UI.

The **Application Migration Consolidation** report can be run independently of the **Settings** app:

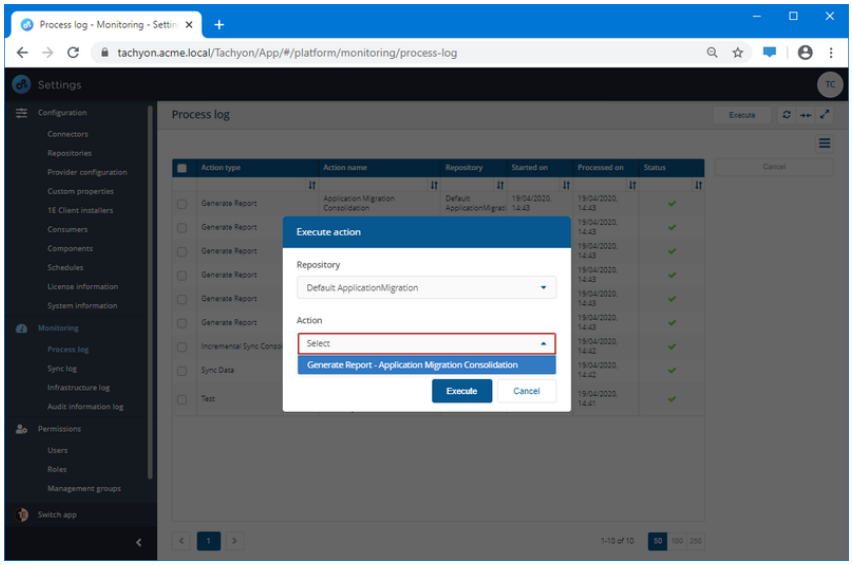
Clicking the **Execute** button in either the **Configuration→Connectors** or **Monitoring→Process log** pages.

> **Note**
>
> Users assigned the **Application Migration Administrator** role will only be able to run the Basic Inventory Consolidation report from the **Process Log** page.

Selecting an Application Migration repository.

Selecting the **Generate Report - Application Migration Consolidation** action.

Clicking the **Execute** button in the **Execute action** popup.



11.2.5 Upgrading Application Migration

How to upgrade Application Migration and Task Sequence tools in various scenarios.

11.2.5.1 Upgrading to Application Migration 8.1

Application Migration is installed through Tachyon setup. Refer to Tachyon Setup.

Web site configuration in Tachyon setup

If upgrading SLA Platform 3.3 to Tachyon platform 8.1, you must first upgrade to Tachyon platform 5.2 first.

When configuring **Website Configuration** in Tachyon setup, you should specify the current SLA Platform configuration (host header and HTTP / HTTPS ports) settings. For example, if SLA Platform 3.3 was installed with the default settings (HTTP on port 8080 and HTTPS on 8443), you should set the HTTP Port to 8080 and HTTPS Port to 8443 in the Website Configuration page of the setup wizard.

If a Host Header was used for SLA Platform, ensure the same host header is used for Tachyon platform. This will ensure your existing Application Migration Task Sequence steps and Shopping integration settings will continue to work after the upgrade, will prevent integration errors with the existing Catalog website (refer to Known issues) and will also ensure other websites installed in the Default Website will continue to be accessible using the server FQDN in the URL.

If SLA Platform was configured to use HTTPS, it is likely that you will need to generate a new Web Server certificate for Tachyon platform that meets the additional requirements of the platform. Refer to Web Server Certificate.

11.2.5.1.1 Upgrading Tachyon Platform

If you are currently running Application Migration on Tachyon Platform, you will need to upgrade to Tachyon Platform 8.1 and include Application Migration. Please refer to Upgrading Tachyon Platform for details.

11.2.5.2 Managing platform users

Tachyon setup will migrate users defined in SLA Platform 3.3 during the upgrade. However, these users will not be granted any permissions in the platform. After upgrading from SLA Platform 3.3, you should add at least one user to the **Global Administrators** role (this should have been done if you followed the platform post-installation steps). This can be a user which was present in SLA Platform v3.3 or it can be an altogether new user. After this initial upgrade and configuration, either the installation user or the Global Administrator can add/remove users.

If you were previously using Application Migration 2.5 on platform versions 4.1, or 3.0 on 5.0, the existing user permissions that you defined in the platform to enable users to use Application Migration will remain.

Whatever upgrade path was taken, after upgrading to platform v5.2 you will need to assign the **Application Migration Administrators** role to users that will be working with Application Migration to ensure they have the necessary permissions to complete all tasks associated with the day-to-day operation of Application Migration.

In some cases, the same users may need to perform tasks in the platform, such as configuring connectors or creating Management Groups and using them to synchronize data from Configuration Manager, running various consolidation reports and managing Management Groups. Refer to Requirements: Accounts needed to use Application Migration.

> **Note**
>
> The user account defined in the Application Migration Task Sequence step to connect to Application Migration during Task Sequence execution only needs to be defined as a User in Tachyon platform. This user will be migrated / retained when upgrading, so no further action is required. This account does not require the Application Migration Administrator security role, or any other security role.

11.2.5.3 Upgrading 1E Task Sequence Tools

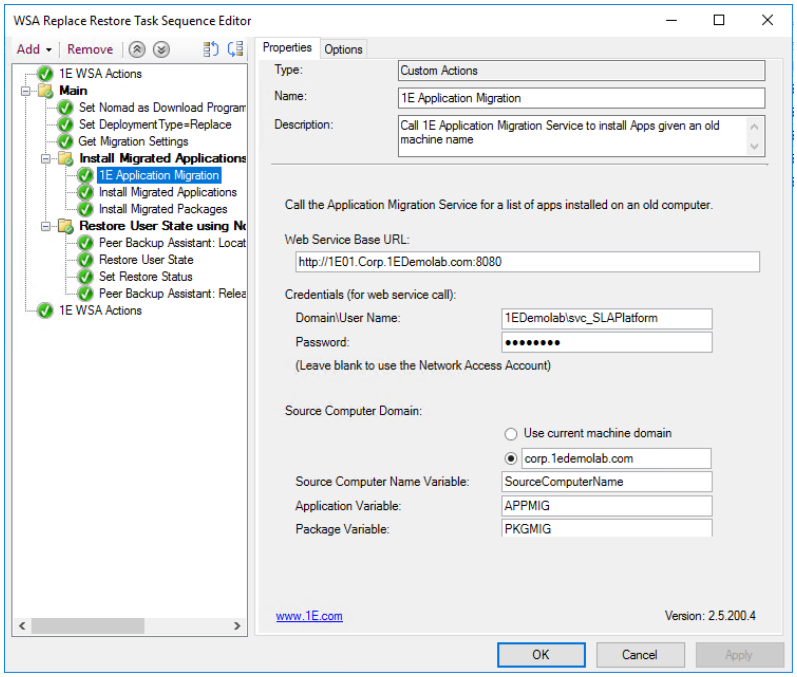
If you have a version of 1E Task Sequence Tools older than 2.5.300 installed, you should upgrade to the version for your platform release. To upgrade the 1E Task Sequence Tools, follow the instructions under the Installation: Installing the 1E Task Sequence tools heading using the latest version of *1ETaskSequenceTools.msi*.

After the upgrade, existing task sequences that included the Application Migration step will continue to work, provided you have not changed the Base URL of the SLA Platform or Tachyon platform server.

The **Properties** page for the step will reflect the layout for the version of the **1E Task Sequence Tools** in which the step was originally added to the Task Sequence.

> **Note**
>
> You should replace the Application Migration step in existing Task Sequence in due course by removing the existing Application Migration step and adding a new one in its

place. If you do not do that, you will not benefit from the fixes and improvements introduced in the latest version.



11.3 Using Application Migration

You can use the Application Migration pages to manage the migration of applications from one system, or one version of a system to another.

11.3.1 Getting started with Application Migration

An outline of the steps you need to take after installing Application Migration to get you migrating applications through your OS Deployment Task Sequences.

11.3.1.1 Introduction

Migrating applications with Application Migration involves working with Application Migration and Configuration Manager.

Application Migration is used to identify the applications that are installed in your environment and to create migration rules that define how each application should be migrated. It is also used to define sets of applications required by specific roles (Role-based application sets) and to preview the results of a migration on a specific device.

Configuration Manager automates the installation of the required applications (based on migration rules and role-based application sets) in a Task Sequence. The **Application Migration** Task Sequence step returns a list of Configuration Manager Applications and Packages that need to be installed, which are then installed through the **Install Application** and **Install Package** Task Sequence steps.

Note

Application Migration can only upgrade or migrate an application if the target application and version (the one you want to upgrade *to*) is packaged for deployment in Configuration Manager. This guide assumes you already have the applications you need packaged in Configuration Manager.

11.3.1.2 The Application Migration navigation panel

The Application Migration navigation panel has a number of items that let you perform different functions related to configuring and running Application Migration.

Menu item	Description
Installations	On the Installations page you can view installed applications in your environment, see how frequently they're used, and whether migration rules exist. You can also create and modify migration rules and exclude applications you're not interested in. Refer to Using the Installations page.
Manage Rules	Migration rules are used to define what happens to previously installed applications during an OS deployment. These rules can include usage criteria, allowing you to choose to only install previously installed applications if they were being used, or perhaps replace a rarely used application with a less costly alternative. Refer to Managing migration rules.
Role Based Applications	A Role Based Application Set defines a set of applications that should be installed on a computer for a user performing a particular role, or perhaps working at a particular location. Refer to Role Based Application Sets.
Preview Device	Before deploying the OS Deployment Task Sequence, you can preview the effect that Application Migration will have on the software installed on a device. This can be for existing or new build devices. This is done from **Preview Device**, where you can see the following menu items: **Existing Device**: Post-migration application status for existing computers undergoing an in-place upgrade or a computer refresh. **New Device**: Applications to be installed on new-build computers by Management Groups or device attributes. Refer to Previewing post-OS migration application states.
Install Sequence	In some cases, when some applications are installed together, they need to be installed in a certain order. You can do this in Application Migration by adding applications that have specific installation order constraints to the Install Sequence. Refer to Setting the Install Sequence for applications.

Menu item	Description
Exclusions	Products can be excluded from consideration by Application Migration, helping you to focus on the important products and minimizing effort during the Application Migration workflow. Refer to Managing product exclusions.
Conflict Resolution	Conflicts arising from having more than one migration rule for a computer belonging to more than one management group can be easily resolved before the migration takes place. Refer to Viewing and resolving migration rule conflicts.

11.3.1.3 Getting started with Application Migration

The recommended approach to get started with Application Migration is:

Configure Tachyon Providers to support the Auto Install feature. Refer to Post-install configuration.

Set up Tachyon platform to synchronize inventory data and Application/Package information from Configuration Manager. The inventory data is automatically normalized by the 1E Catalog into consistent Vendor, Title, Version and Edition (VTVE) identifiers and is used to show what applications are installed in your environment. Application and Package information imported from Configuration Manager is used to define the 'target' application in a migration rule to be installed by Configuration Manager. Refer to Post-install configuration.

Set up users and assign the appropriate roles in the Tachyon platform. All users that will be working with Application Migration must be added to the Tachyon platform and assigned the Application Migration Administrator role. Refer to Requirements: Accounts needed to use Application Migration.

Normalize the imported Configuration Manager Applications and Packages by associating them with a Vendor, Title, Version and Edition from the 1E Catalog. This makes it easier later on when defining migration rules, although the association for a particular application can also be defined when you create the migration rule. Refer to Manage associations.

Work through the installations in your environment from the Installations page and define migration rules. As you review each application, you can:

Exclude it if it is not an application you want to migrate (e.g. it is an application that is included in your base build, or is a runtime library or other component that is always installed through another application installation).

Create a migration rule to define how the application should be migrated (e.g. upgraded, replaced or retained).

> **Note**
>
> There will typically be thousands of software titles in your environment. The Installations page in Application Migration will display the most commonly installed applications at the top, so you can focus on these as you work your way down the list. You can also filter the list by title or vendor if you want to start by defining rules for a few specific applications.
>
> Refer to Using the Installations page.

Update your Configuration Manager OS Deployment Task Sequences to include the Application Migration step. Application migration occurs on a device when a Task Sequence is executed that has the 1E Application Migration step included. Refer to Using Application Migration in a task sequence for details.

Preview the expected results of Application Migration on a device. Before deploying an Application Migration Task Sequence to a device, you can see what effect Application Migration will have on the applications currently installed on a given device by Previewing post-OS migration application states.

Deploy the Application Migration Task Sequence to devices. Deploy your updated Task Sequences as required to upgrade or reinstall Windows, or to transfer the data and applications from an old device to a new one.

Once you are familiar with the above process, you can start to investigate the following features of Application Migration.

Creating exceptions for specific departments or locations. In some cases, you may have a migration rule for an application that you want to apply to most devices but require a different rule for the same application on a specific group of devices (e.g. a department or location. For example, you may want to upgrade AutoCAD 2018 to AutoCAD 2019 everywhere except in the Seattle office, where they need to retain AutoCAD 2018 as they are working with a client on the older version. You can do this in Application Migration by

Creating Management Groups in the Tachyon platform that correspond to the departments or locations for which exceptions are required. Refer to the Management Groups - tutorial.

Creating a Global migration rule in Application Migration. By default, migration rules are Global unless a specific Management Group is selected when the rule is created.

Creating the exceptional migration rule for the appropriate Management Group. Selecting the Management Group from the drop-down on the **Installations** page will filter the list of installations to show only the software installed on the devices in the selected Management Group. It also means that any rules that are added from that view apply only to the selected Management Group. Refer to Using the Installations page for more information on creating the migration rules from the Installations page. You can also create rules limited to specific Management Groups from the Manage Rules page (refer to Managing migration rules for more information). However, it is easier to create a migration rule from the Installations page as the selected application's Vendor, Title, Edition, and Version are pre-populated in the Edit Rule form.

Installing sets of Applications based on the user's department or location. In addition to migrating applications that were previously installed on a device, Application Migration can be used to install pre-defined application sets onto a device based on the department or location that the device is in, You can do this in Application Migration using the Role-based Application Sets feature by:

Creating Management Groups in the Tachyon platform that correspond to the departments or locations for which application sets are to be required. Refer to the Management Groups - tutorial.

Creating one or more Role-based Application sets and adding them to the appropriate Management Group. Refer to Role Based Application Sets.

Installing applications in a specific order. Application Migration normally installs applications in the Task Sequence in no particular order. In some cases, when some applications are installed together they need to be installed in a certain order. You can do this in Application Migration by adding the applications that have specific installation order constraints to the Application installation sequence. Refer to Setting the Install Sequence for applications.

11.3.2 Using the Installations page

On the Installations page you can view installed applications in your environment, see how frequently they're used, and whether migration rules exist. You can also create and modify migration rules and exclude applications you're not interested in.

11.3.2.1 Using the Installations page

You use the Installations page to view applications installed in your estate and create migration rules for them. The page lists Applications by Title, Vendor and Edition, ordered by **Install Count** in descending order, with the most commonly installed applications are at the top of the page. Typically, you'll work your way down the list of applications, either adding a migration rule to define how that application should be migrated or excluding the application. Alternatively, you can use the column filters to search for specific applications you want to migrate and apply rules to the filtered list.

From the Installations page you can create a migration rule for all versions of a selected application, or you can drill down by clicking the application title to see all versions of the application and create more granular rules for specific versions.

Refer to Managing migration rules for more information on creating and managing migration rules.

11.3.2.1.1 Page elements

The following items are displayed on the Installations page:

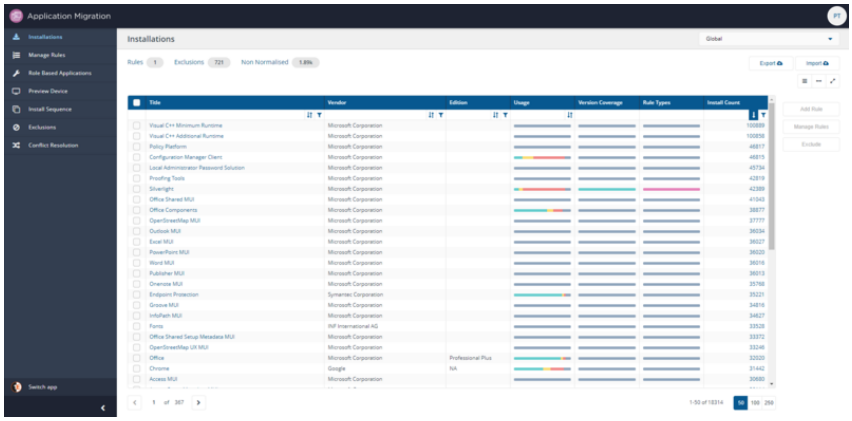
Option	Description
Management Group	By default, the Installations page shows the global view of software installations across your entire estate. If you've defined one or more Management Groups, selecting a Management Group from the drop-down displayed in the top-right of the page will filter the view to show software installed on devices in that Management Group. If you add migration rules from the Installations page with a specific Management Group selected, the rule will only apply to installations in that Management Group and will not affect installations outside that Management Group. **Note** Management Groups are containers used to group devices and the software installed on those devices. Management Groups are defined using configurable rules that look at various properties of the devices and their installed software, these are then evaluated to determine the group membership. This means that Management Group membership adapts to changes to the devices and software in your environment.

Option	Description
Title controls	The title area includes information on your current rules, exclusions and non-normalised products. It also includes buttons to export and import rules to and from a spreadsheet.

Control	Description
Rules	Displays the number of existing rules associated with a particular Management Group. Follow the link to Add, Edit or Delete existing rules. For more details, please refer to: Managing migration rules: Adding Migration Rules Managing migration rules: Modifying an existing rule Managing migration rules: Deleting an existing rule.
Exclusions	Displays excluded items. Excluded items are not associated with any Management Group. Follow the link to view the exclusions. Please refer to Managing product exclusions for more details.
Non-Normalized	Displays the number of items which have not yet been normalized against the Catalog. Follow the link to resolve the unmatched items.
Export	Creates and downloads a spreadsheet in **.xlsm** format that has all your installed applications to enable you to create new rules to associate with them without having to be online.
Import	When you have created the new rules for your applications, import the file, which may be in **.xlsx** or **.xlsm** format, so that Application Migration can implement the new rules.

Add Rule	Allows you to add a new migration rule for the selected application.

Option	Description
Manage Rules	Allows you to manage existing migration rules for the selected application.
Exclude	Allows you to exclude the selected application if you're not interested in it for application migration purposes. For example, runtime libraries, drivers, and applications included in your core OS build, or components that are installed by another application that will be migrated.



11.3.2.1.2 Installations table

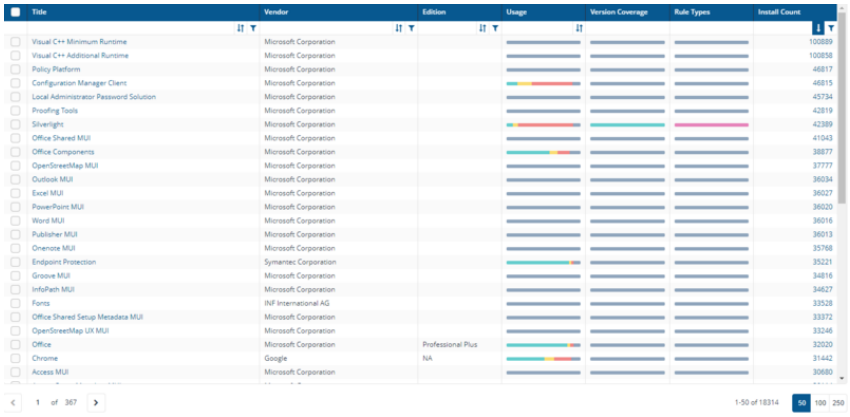
The Installations table lists the applications installed in your estate. All versions of a given **Title**, **Vendor** and **Edition** are consolidated into a single row. Clicking on the **Title** displays a popup with version-specific data.

By default, the list is ordered in descending order by the **Install Count** , so the most prolific applications are displayed at the top. Each application has indicators showing how frequently the application is used and whether there are any migration rules to cover it. This allows you to focus on the most commonly installed and used applications which do not have migration rules.

The following table describes each column.

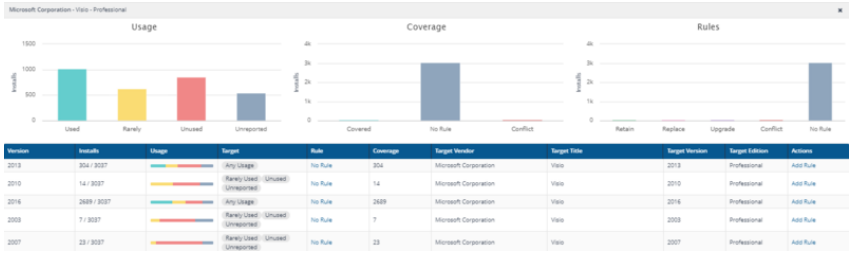
Colum name	Description
Title	Product title.
Vendor	Product vendor.
Edition	Product edition.
Usage	A usage summary for that product. Hover your mouse over the bar to view the installation count in each usage state.

Colum name	Description
Version Coverage	A summary of installations of the product that are covered by one or more migration rules. Hover your mouse over the bar to see what is **Covered** , has **No Rule** os is in **Conflict** . If the bar is completely grey there are no migration rules defined for the application.
Rule Types	A summary of the migration rule types defined for that product. Hover your mouse over the bar to see the count of each type. If the bar is completely grey there are no migration rules defined for that application.
Install Count	The total number of installations for that product across your estate.



11.3.2.1.3 Viewing Installation details

You can click on a specific title to see clearer representations of **Usage**, **Coverage**, **Rules**, and details for each application version. In this view you can create a version-specific migration rule by clicking the **Add Rule** link in the **Actions** column. In our example, we've chosen Visio Professional.



The table below describes the three charts in the top panel.

Panel	Description
Usage	Hover your mouse over the column to see the number of **Used**, **Rarely**, **Unused** and **Unreported** installations.

Panel	Description
Coverage	Hover your mouse over the column to see the number of installations that are **Covered** by a rule, have **No Rule** coverage, or have a rule **Conflict**.
Rules	Hover your mouse over the column to see the number of installations that Application Migration will **Retain**, **Replace** or **Upgrade**, or installations for which there is a rule **Conflict** or **No Rule**.

The detail table below the charts shows the following information for each version:

Column name	Description
Version	Version of the product.
Installs	The number of installations of that version out of the total of all installed versions, for example, 304/3017.
Usage	A usage summary for that version. Hover your mouse over the bar to see the count of installations in each usage state.
Target	Indicates the usage states that apply to that version as defined in the rule in the same row. If there are different rules for different usage states of the same software version, these would be shown as separate rows, each indicating the usage states defined in the rule in the same row.
Rule	Indicates the type of migration rule applying to that version. Clicking on the link in this column reveals the Management Groups including installations of the version.
Coverage	Indicates how many installations of that version covered by the rule indicated in the Rule column.
Target Vendor	Indicates the vendor of the application that this version will be migrated to by the rule indicated in the same row.
Target Title	Indicates the title of the application this version will be migrated to by the rule shown in the same row.
Target Version	Indicates the version of the application this version will be migrated to by the rule shown in the same row.

Column name	Description
Target Edition	Indicates the edition of the application this version will be migrated to by the rule shown in the same row.
Actions	**Add Rule** allows you to create a rule for this specific version. When you click the **Add Rule** link in this column, you'll be taken to the **Add Rule** page in **Manage Rules**. The source **Vendor**, **Title**, **Version** and **Edition** will be pre-populated with the version of the application in the same row.

11.3.2.2 Filtering results

You can filter the results of the **Installations** table by **Title**, **Vendor**, **Edition**, **Usage** or **Install Count** columns. For example, to narrow the results of the installed applications to show only Microsoft Visio Professional:

Click on the filter icon

just beneath the header row in the **Title** column.

From the dropdown menu choose **contains** and type Visio.

Click **Apply**.

Repeat for the **Edition** column, choosing **contains** and typing professional.

Click **Apply**.

This will restrict the list of displayed applications to Visio Professional.

11.3.3 Managing migration rules

11.3.3.1 Introduction to migration rules

Migration rules are used to define what happens to previously installed applications during an OS deployment. These rules can include usage criteria, allowing you to choose to only install previously installed applications if they were being used, or perhaps replace a rarely used application with a less costly alternative.

A migration rule comprises the following elements.

Migration rule element	Description
Rule type	Defines whether the rule will retain, upgrade or replace an application. An application will be removed during an OS wipe-and-load or device replacement if there is no rule defined.
Source Application	Defines the application, identified by Vendor, Title, Version and Edition, that is to be migrated.
Target Application	Defines the application, identified by Vendor, Title, Version and Edition, that will be installed in place of the source application. For retain rules, the Target Application is the same as the Source Application. For upgrade rules, the Target Application is a different version of the Source Application.
Usage	Defines whether the source application will be migrated if it is used, rarely used, unused or any combination of these states. You can create multiple rules for the same Source Application with different usage settings. For example, you may want to retain an application if it is being used, but replace it with a cheaper alternative if it is not being used.
Association	Defines the Configuration Manager Application or Package and Program that will install the Target Application. The association of a Configuration Manager Application or Package and Program with a Vendor, Title, Version and Edition can be made ahead of creating migration rules through Manage associations in Inventory, or while defining the rule.

About Vendor, Title, Version and Edition

Application Migration identifies each application by Vendor, Title, Version and Edition as defined in the 1E Catalog. Some publishers use a 'colloquial version', such as 'Office 2019' or 'Acrobat Reader DC', to identify a broad major release, in addition to the full version that changes with each update. Where the 1E Catalog has a colloquial version defined for a given application, the Source Application and Target Application definitions in a migration rule will use the colloquial version. In some cases an application may have a mix of full versions and colloquial versions (typically when the adoption of colloquial versions came later in the product life cycle). Application Migration also includes the concept of a 'readable version', which is simply the full version truncated to the first two parts of the full version number (e.g. 16.0) to make managing rules easier.

When defining an Upgrade or Replace rules, the Source Application can be defined using a colloquial version (if available), readable version or full version. These rule types can also use a wild card (e.g. * or 16.*), which is useful for creating a single rule that will upgrade *any* version of an application to another version, or replace *any* version of an application with a different application.

If the selected Vendor, Title and Edition has already been associated with an Application or Package and Program in Configuration Manager, those associated versions will appear in bold at the top of the Version drop-down list when defining the target of any Migration rule or application in a Role-based Application set.

11.3.3.2 Understanding behavior of migration rules in different OS deployment scenarios

Migration rules will behave differently depending on the type of OS deployment being performed, If the existing OS is being reinstalled ('wipe-and-load'), or a new OS is being installed on a replacement device and you are using Application Migration to migrate applications from an old device, all migration rules will be applied. Any previously installed applications for which no migration rule has been defined will not be migrated (effectively these applications will be 'removed', although technically they are simply not reinstalled in the new OS. Replace rules will install the replacement (target) application in the new OS and the original (source) application will not be installed, so the application is effectively replaced in the new OS.

An In-place upgrade behaves differently, as the disk is not wiped during an in-place upgrade, so the previously installed applications remain installed after the upgrade. For this reason, any rules defined to retain an existing application are ignored by Application Migration during an in-place upgrade as the application will be retained anyway. Upgrade rules will be applied, and in most cases the installation of the later version will simply upgrade the previously installed application. However, in some cases, installing a later version of an application on a device that has an older version installed may result in both versions being installed 'side-by-side' - this all depends on how the vendor has implemented their installer.

Rules defined to replace an application will result in both the original (source) application and the replacement (target) application being installed during an in-place upgrade. This is because Application Migration does not actually remove the source applications when replacing an application. However, you can use Application Supersedence in Configuration Manager (refer to https://docs.microsoft.com/en-us/mem/configmgr/apps/deploy-use/revise-and-supersede-applications for details on how to configure Application Supersedence to have Configuration Manager uninstall the replaced (source) application when the replacement (target) application is installed.

11.3.3.3 Migration Rules and Management Groups

By default, migration rules are Global - they apply to all devices in your organization. In some cases you may want to define different migration rules for an application on different devices. For example, you may want to upgrade AutoCAD 2018 to AutoCAD 2019 everywhere except in the Seattle office, where they need to retain AutoCAD 2018 as they are working with a client on the older version. If you have Management Groups defined in the platform, you can create rules that apply globally or to a specific Management Group. Management Group migration rules take precedence over Global migration rules, so in our example, you would create a Global rule to upgrade AutoCAD to 2019 and a Management Group rule for the Seattle Management Group to retain the 2018 version. Devices in the Seattle Management Group will apply the Management Group rule, not the Global rule,

It is possible for a device to exist in multiple Management Groups, so it is also possible for conflicts to arise, where a device is in multiple Management Groups, each with different rules defined. If this occurs, the rule will be shown as a Conflict on the Installations page that must e resolved in order for any rule to apply during OS deployment. Refer to Viewing and resolving migration rule conflicts.

11.3.3.4 Adding Migration Rules

Migration rules can be added from the Installations page or the Manage Rules page.

11.3.3.4.1 Adding rules for installed applications

Typically, you will work from the Installations page to identify an installed application that you want to migrate, selecting it and clicking the **Add Rule** button. This will take you to the Add Rule page, but will pre-populate the Source Application Vendor, Title and Edition according to the application you selected in the Installations page. If you want to create a rule for a specific version of an application, from the Installations page click on the application title to view the installed versions and click the **Add rule** link in the **Action** column for the version you want to migrate. Again, this will take you to the Add Rule page, but with the Source Application Version pre-populated along with the Vendor, Title and Edition.

> **Note**
>
> You will not be able to add a rule for a specific version if that version and usage combination is already covered by another rule, for example a wild-card upgrade rule.

The following pages provide step-by-step instructions for adding different types of rules from the Installations page.

Retain - Adding a rule to retain an application

Upgrade - Adding a rule to upgrade an application

Replace - Adding a rule to replace an application.

11.3.3.4.2 Auto Install for Migration Rules

Application Migration uses the **Install Application** and **Install Package** steps in a Task Sequence to install migrated applications and packages. These Task Sequence steps are dependent on the relevant checkbox (auto install flag) being enabled for *each* application and package:

Allow this application to be installed from the Install Application task sequence action without being deployed.

Allow this program to be installed from the Install Package task sequence action without being deployed.

If a checkbox is not enabled, the software installation will fail for that application or package. An administrator can enable this checkbox for each application and package by using either of the following methods:

in Configuration Manager during or after creating each application and package.

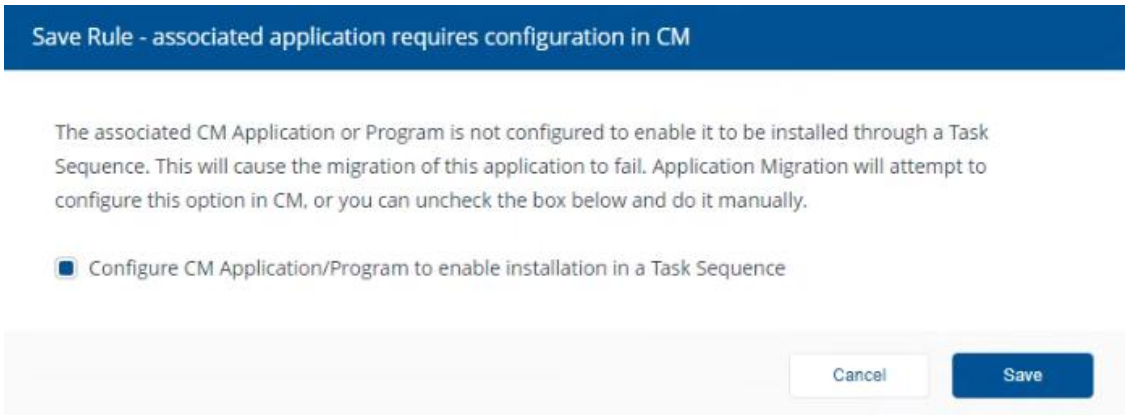
using the **Auto Install** feature in Application Migration when creating application associations, rules or Role Based Application sets.

For information about manually enabling these checkboxes for Configuration Manager applications and packages. Refer to Using Application Migration in a Task Sequence: Auto Install for Configuration Manager Applications and Packages.

> **Note**

Application Migration's **Auto Install** feature is able to read the checkbox (auto install flag) for applications and programs, but in order for Application Migration to enable them for you, you'll need to configure related providers in the Settings application of the platform. These should already be configured as a post-installation step. Refer to Post-install configuration.

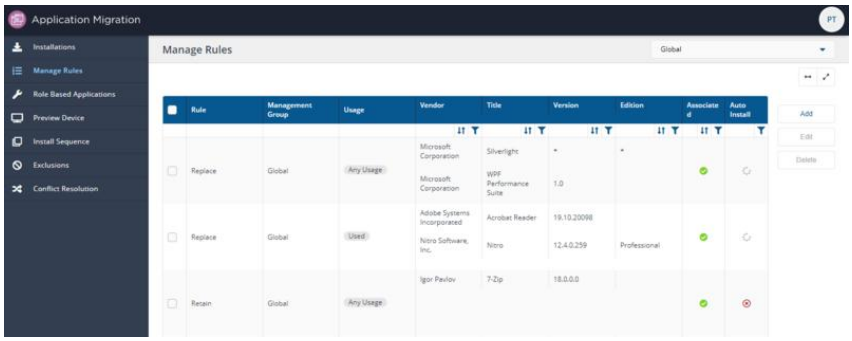
When you save the migration rule, and the Auto Install flag is not already enabled for the associated Application or Program, then you will see the popup shown opposite. You should enable **Configure CM Application/Program to enable installation in a Task Sequence** and click **Save**. The Auto Install status will then change from red to green. Status values are described in the table below.



On the **Manage Rules** page, the **Auto Install** column displays a status for each migration rule. Our example shows two different types of status, **In-Progress** and **Not Checked**.

Auto Install status	Description
Checked	Green tick. Auto install flag for Configuration Manager application or package program is set.
Not Checked	Red cross. Auto install flag for Configuration Manager application or package program is not set.
In-Progress	Spinning. Application Migration has triggered an operation which attempts to set the auto install flag of Configuration Manager application or package program. If the status permanently spins then it is likely that your administrator has not configured the providers in **Settings**. Once they have been configured, the setting will be applied and the icon will change from spinning to green.

Auto Install status	Description
Failed	Red warning triangle. Application Migration triggered an operation which failed while trying to set the auto install flag of Configuration Manager application or package program.
Not Applicable	A rule has broken association and the application migration report is not run.



Note

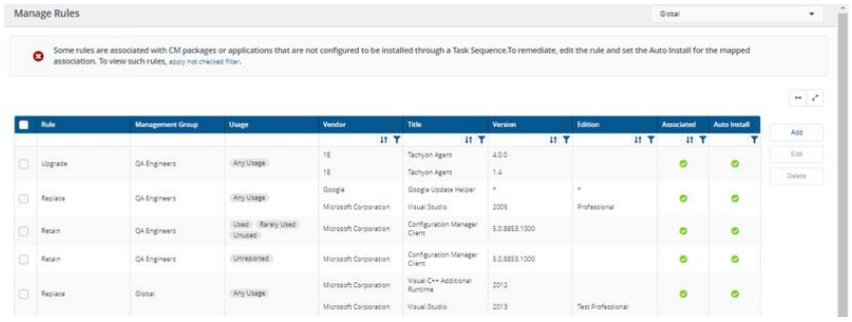
If a rule has **Auto Install** unchecked, you will be prompted to edit that rule and set **Auto Install** to enabled. You can view this type of rule by filtering the **Auto Install** column by **Not Checked**.

You will also see a similar message on the following Application Migration pages and a prompt to take action if the Auto Install is unchecked:

Installation

Preview Device→Existing Device

Preview Device→New Device.



11.3.3.4.3 Adding rules for applications that are not reported as installed

The Installations page can be used to add migration rules for applications that are already installed in your estate. If you want to add a migration rule for an application that is not yet reported as installed on any devices in your estate, you will need to use the Manage Rules page.

From the Application Migration navigation menu on the left, select **Manage Rules.**

In the Manage Rules page, click **Add** (top right).

In the New Migration page screen, choose the rule type (**Upgrade application**, **Replace application** or **Retain application as is**) for the new rule.

If you choose to upgrade the application:

In **Source A**pplication , choose the **Vendor**, **Title**, **Version** and **Edition**.

Choose a **Usage** category (**Any Usage**, **Used**, **Rarely Used**, **Unused or Unreported)** the application must meet in order to be upgraded during the migration. If the application does not meet the criteria, it will not be installed.

In **Target Application,** choose the **Version** and **Edition** to upgrade to.

If you choose to replace the application:

In **Source A**pplication , choose the **Vendor**, **Title**, **Version** and **Edition**.

Choose a **Usage** category (**Any Usage**, **Used**, **Rarely Used**, **Unused or Unreported)** the application must meet in order to be upgraded during the migration. If the application does not meet the criteria, it will not be installed.

In **Target Application,** choose the **Vendor, Title**, **Version** and **Edition** in this order and choose the attributes for the replacement product.

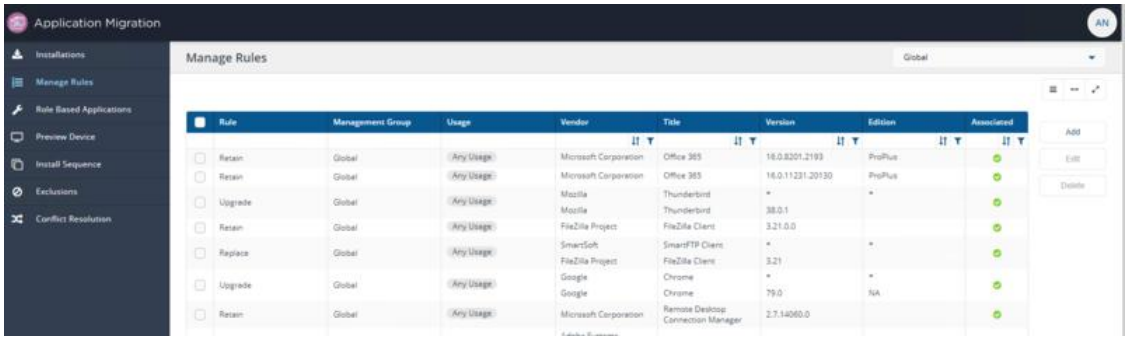
If you choose to retain the application as is:

In **Source A**pplication , choose the **Vendor**, **Title**, **Version** and **Edition**.

Choose a **Usage** category (**Any Usage**, **Used**, **Rarely Used**, **Unused or Unreported)** the application must meet in order for it to be retained during the migration. If it does not meet the usage criteria, it will not be installed.

Associate the target with a Configuration Manager package or application.

Click **Save** and close.



11.3.3.5 Modifying an existing rule

Migration rules are modified from the Manage Rules page. For convenience, you can access the Manage Rules page from the Installations page by selecting an application then clicking the Manage Rules button. This will take you to the Manage Rules page, filtered to show the rule(s) for the selected application, Alternatively you can go to the Manage Rules page to view all migration rules and manually select the rule you want to modify, In either case, from the Manager Rules page select the rule and click the Edit button.

In this example, we are going to modify the existing retain Acrobat Reader migration rule by:

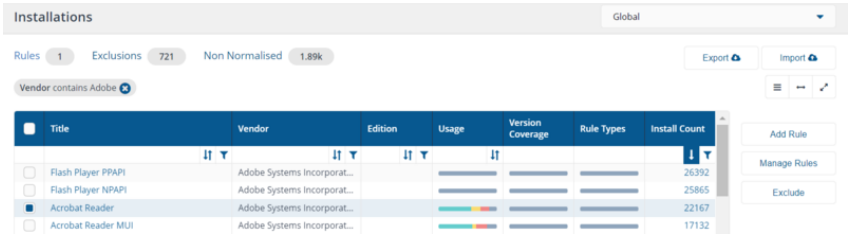
Changing its behavior from retain to replace.

Replacing all instances of Acrobat Reader with Nitro Reader.

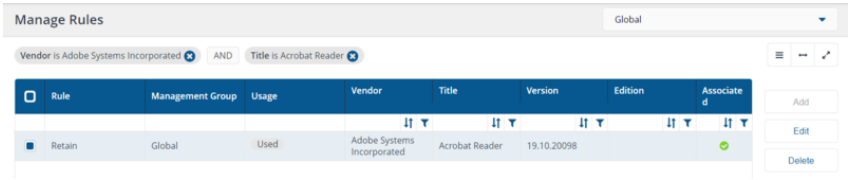
To modify the existing retain rule for Acrobat Reader:

On the Installations page, on the Vendor column click the filter icon

and narrow the results down with the criteria: **Vendor contains Adobe**.

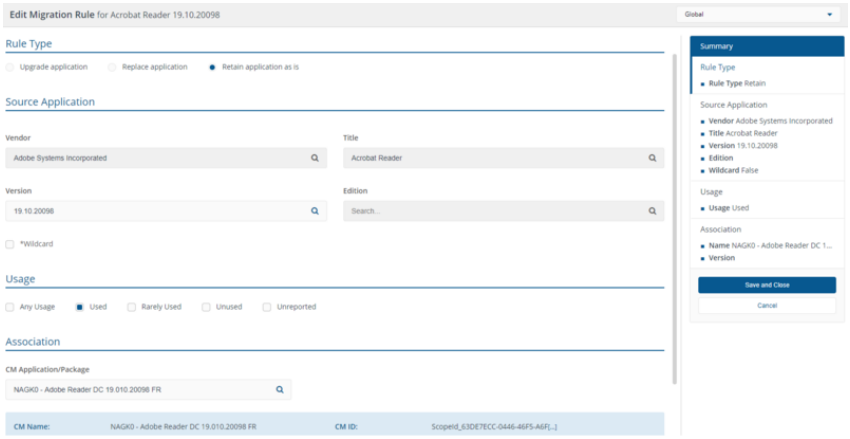


In the table, locate and select Acrobat Reader, then click the **Manage rules** button.



On the Manage Rules screen, select the rule and click **Edit**.

In the Edit Migration Rule screen, the original rule configuration is displayed.



Click **Replace application** to change its behavior and under this, choose the attributes for the replacement application by clicking:

Vendor and from the list, select **Nitro Software, Inc.**

Title and from the list, choose **Nitro.**

Version and from the list choose **12.4.0.259.**

Associate the target with an existing Configuration Manager Application/Package.

Click **Save** and close.

On the Application Migration page, the migration rule for Adobe Acrobat is updated from **Retain** to **Replace.**

11.3.3.6 Deleting an existing rule

Migration Rules are deleted from the Manage Rules page. For convenience, you can access the Manage Rules page from the Installations page by selecting an application then clicking the Manage Rules button. This will take you to the Manage Rules page, filtered to show the rule(s) for the selected application, Alternatively you can go to the Manage Rules page to view all migration rules and manually select the rule you want to delete, In either case, from the Manager Rules page select the rule and click the Delete button.

In our example, we are going to delete an existing rule for Acrobat Reader.

To delete an existing rule for Acrobat Reader:

On the Installations page, on the Vendor column click the filter icon

and narrow the results down with the criteria: **Vendor contains Adobe**.

In the table, locate and select Acrobat Reader then click the **Manage rules** button.

On the Manage Rules screen, select the rule to be deleted and click **Delete**.

You will be prompted to confirm your actions.

Click **Delete** to remove the rule.

11.3.3.7 Exporting and importing migration rules

You can export your installed applications to an Excel format file that can be worked on offline, with template columns that let you define new migration rules. Once you've finished defining the rules you can then import them back into Application Migration.

Refer to Working offline on migration rules for more information.

11.3.3.8 Adding a rule to retain an application

A retain migration rule reinstalls exactly the same version of the application during the migration.

In this tutorial, we'll create a rule that retains 7-Zip 18.

To do this:

On the **Installations** page in the **Title** column click the filter icon

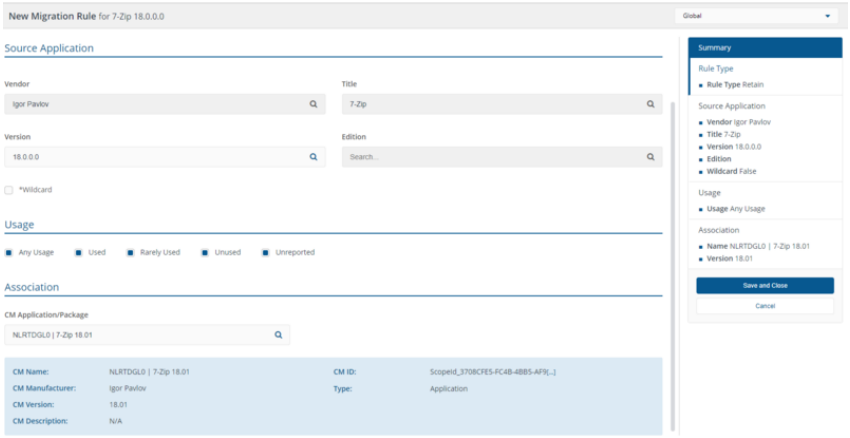
and narrow the results down with the criteria: **Title contains 7-Zip**.

Click the title to expand the list of installed versions. Click the **Add rule** link in the Action column in the row of the version you want to retain.

Note

As Retain rules typically apply to a specific version, adding the rule from the specific version in the UI in this manner will pre-populate the version in the migration rule.

On the **New Migration Rule** page, choose **Retain application as is** for the behavior of the rule.



As we want to retain all instances of 7-Zip regardless of usage, in **Usage** check **Any Usage**.

Because this version of 7-Zip is not already associated with a Configuration Manager package or application, you must add the association. In the **Association** section, choose the 7-Zip 18.0.0.0 **CM Application/Package** from the search field.

Click **Save** and **Close.**

On the **Manage Rules** page In **Title,** search for 7-Zip to view a summary of the rule you just created.

11.3.3.9 Adding a rule to replace an application

A replace migration rule replaces an application with an alternative. This is useful for standardizing on common tools such as file compression applications.

In this tutorial, we are going to create a rule that replaces any version of WinZip with 7-Zip (specifically 16.14).

To do this:

On the **Installations** page, on the **Vendor** column click the filter icon

and narrow the results down with the criteria: **Vendor contains WinZip**.

Check the checkbox in the left-hand column for WinZip and click **Add rule**.

On the **New Migration Rule** page, choose **Replace application** for the behavior of the rule.

In **Source Application**, the attributes for WinZip are already populated and the wildcard box is automatically checked.

As we want to replace all instances of WinZip, in **Usage** check **Any Usage**.

In **Target Application** click field (in bold) and then choose the following values:

Vendor - Igor Pavlov.

Title - 7-Zip.

Version - 16.14.

As this 7-ZIP is not already associated with a Configuration Manager package or application, you must make the association for it to be installed.

In the **Association** section, choose the 7-Zip 16.14 **CM Application/Package** from the search field.

Click **Save** and **Close.**

On the **Manage Rules** page In **Title,** search for 7-Zip to view a summary of the rule you just created.

11.3.3.10 Adding a rule to upgrade an application

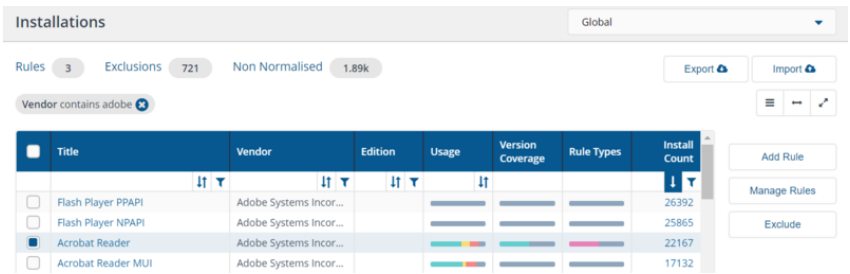
An upgrade migration rule upgrades an existing application to a newer version.

11.3.3.10.1 Adding upgrade rules

To do this:

On the **Installations** page, on the **Vendor** column click the filter icon

and narrow the results down with the criteria contains **Adobe**.



Click the checkbox in the left-hand column for Acrobat Reader and click **Add rule**.

On the **New Migration Rule** page, choose **Upgrade application** for the behavior of the rule.

In **Source Application**, the attributes for Acrobat Reader are already populated and the wildcard box is automatically checked.

As we want to upgrade all instances of Adobe Acrobat 9 to Adobe Acrobat DC, in **Usage** check **Any Usage**.

In **Target Application** click **Version** and choose the following value DC.

As this version of Adobe Acrobat DC Reader is not already associated with a Configuration Manager package or application, you must make the association for it to be installed.

In **Association**, **CM Application/Package**from the list of applications, choose Adobe Acrobat Reader DC.

Click **Save** and **Close.**

On the **Manage Rules** page In **Title,** search for Adobe Acrobat Reader DC to view a summary of the rule you just created.

11.3.3.10.1.1 What happens in upgrade scenarios where the currently installed version of the application is later than the target application?

In upgrade rules where the source version is specified as a wild card, it is possible that versions of the source application in the upgrade rule, that are already installed on the client devices, actually have a later version than the target specified in the upgrade rule.

In versions prior to Application Migration 3.1, the upgrade rule would try to replace the source application already installed on the client device with an earlier target application version, which would result in one of the following possibilities:

the application would be downgraded

the application would remain at the later version and the Application Migration rule would fail

the application in the upgrade rule would be installed in parallel with the existing later version.

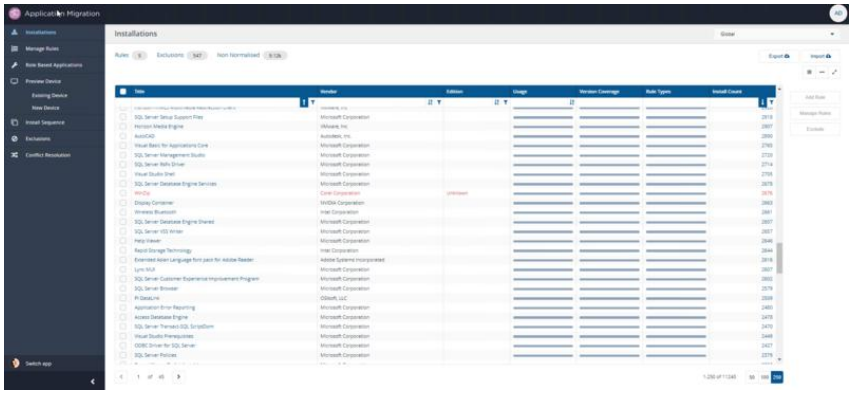
To remedy these unpredictable and unwanted results, in Application Migration 3.1, if an upgrade rule tries to downgrade an application then it will be ignored.

11.3.3.11 Viewing and resolving migration rule conflicts

Conflicts arising from having more than one migration rule for a computer belonging to more than one management group can be easily resolved before the migration takes place.

It's likely that you'll encounter conflicts where two or more migration rules exist for a computer that belongs to more than one Management group, refer to Management Groups page. Under these circumstances, the migration will fail to take place unless you resolve the conflict.

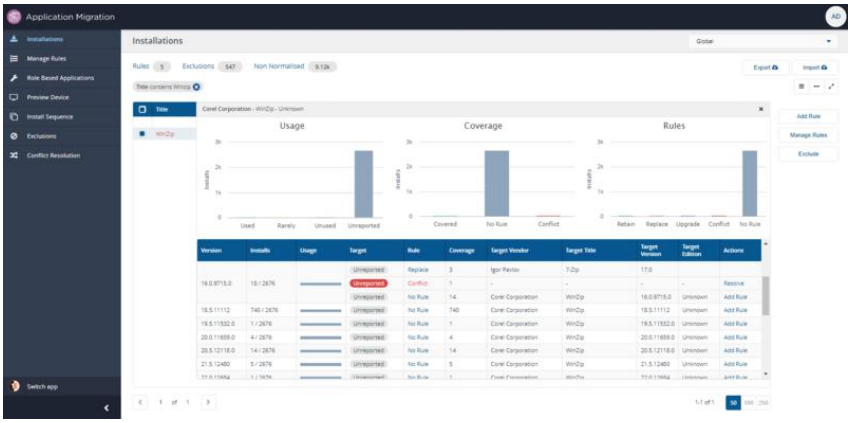
Conflicts are highlighted in red on the **Installations** screen. In our example, there's a conflict for WinZip.



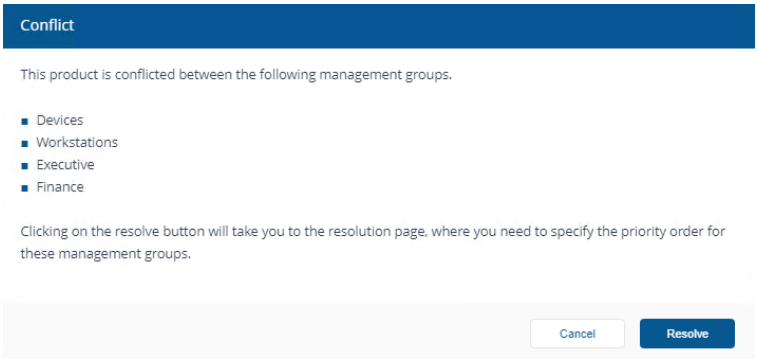
11.3.3.11.1 Viewing a migration rule conflict

To view the migration rule conflict:

Click on the link in the **Title** column to show the drawer view for the software.



Click on **Resolve** in the **Actions** column to display a **Conflict** popup screen showing the Management Groups the computer is a member of that are causing the conflict. In our example these groups are:



Clicking on **Resolve** takes you to the **Conflict Resolution** page, where you can specify the priority order for these Management groups and resolve a migration rule conflict. The next section Resolving a migration rule conflict explains how you can do this.

11.3.3.11.2 Resolving a migration rule conflict

Clicking on **Resolve** in a **Conflict** popup takes you to the **Conflict Resolution** page where you can add and prioritize Management groups to avoid migration rule conflicts.

The priority list for management groups decide which rules apply in a conflict. A common example of this would be when a device happens to be in more than one management group. In this case, management groups higher up in the priority list will have their rules applied first to such devices. To do this:

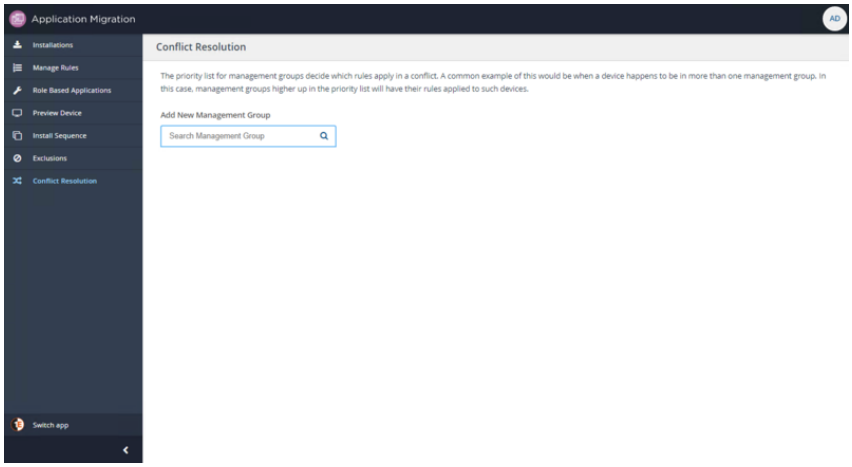
Use the **Add New Management Group** to search for and add the Management groups you want to prioritize, in our example these groups are:

Devices

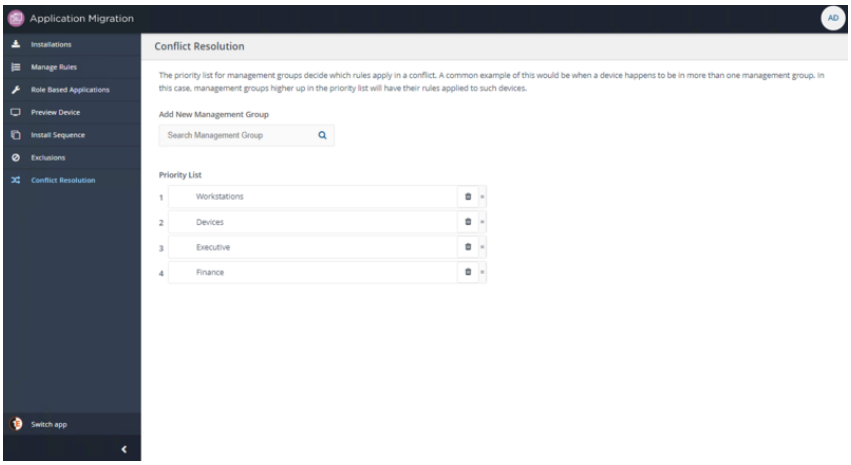
Workstations

Executive

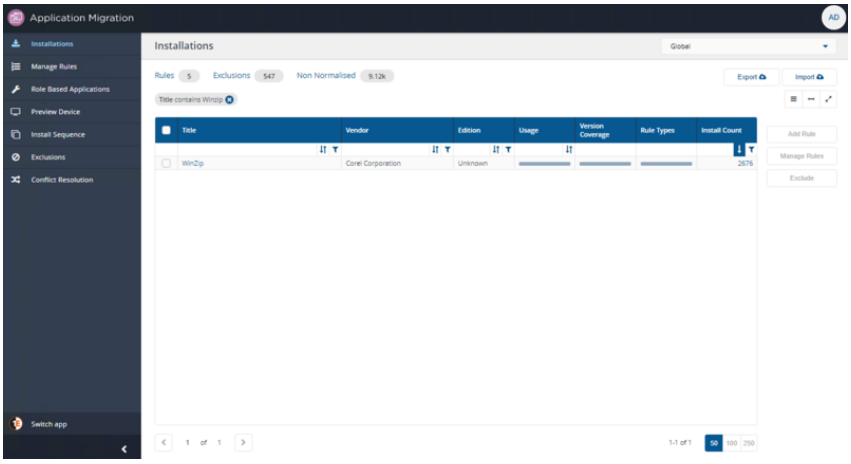
Finance.



In the **Priority List**, arrange the Management groups using drag and drop based on your order of precedence.



Check the **Installations** screen to confirm the conflict is now resolved. In our example, by setting an order of priority for our Management groups, WinZip now shows without the conflict warning.

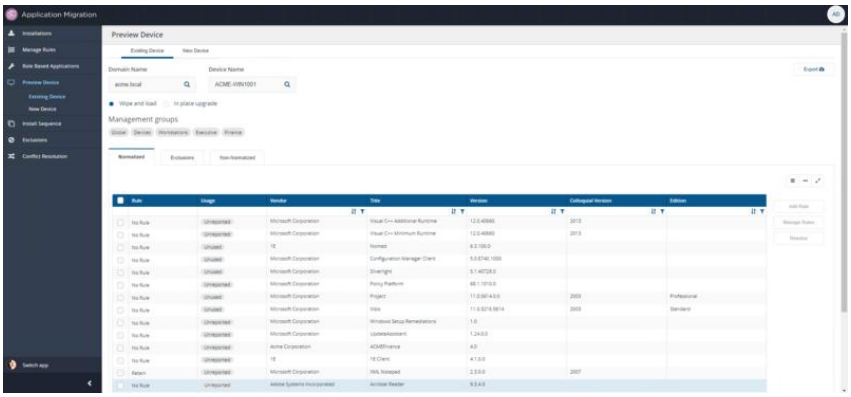


By following this process Application Migration decides which of your **Vendor, Title, Version, Edition (VTVE)** rules should take priority if there's a migration rules conflict.

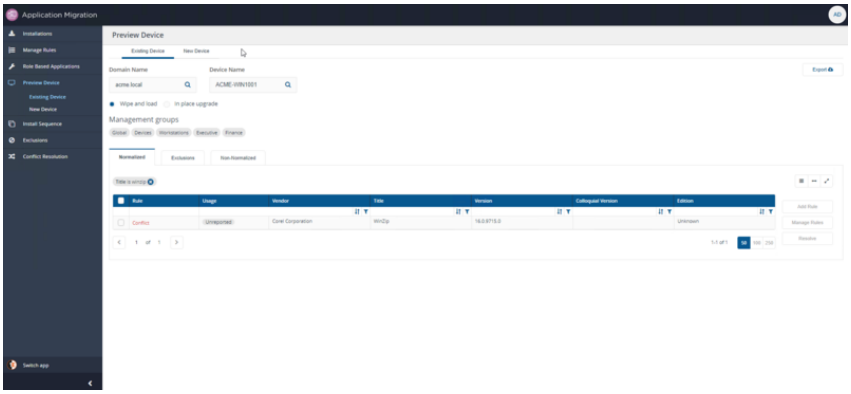
11.3.3.11.3 Using Preview Device to resolve conflicts

In addition to viewing and resolving Migration Rule conflicts from the **Installation** screen, you can also view and resolve conflicts from the **Preview Device** screen by searching for individual computers.

Click on **Preview Device** and then **Existing Device** screen.



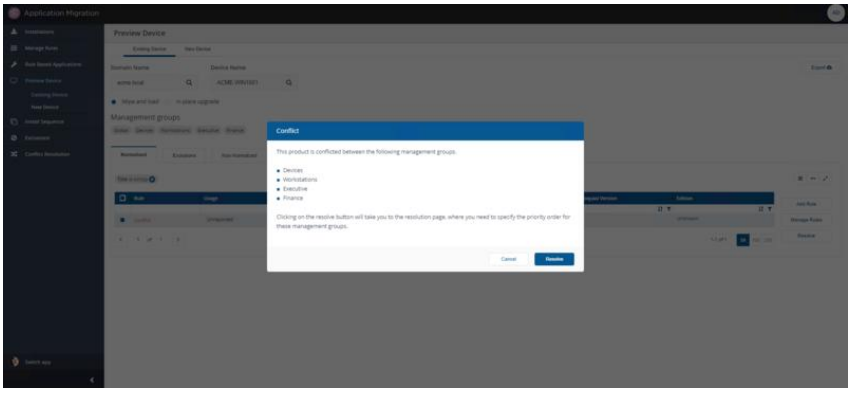
In the **Domain Name** field start typing the name of the Domain where the computer is located, in our example this is **ACME.LOCAL**.



In the **Device Name** filed start typing the name of the computer you want to check, in our example we selected **ACME-WIN1001**.

All the Management groups this computer is a member of are displayed, as are the rules that apply to software installed on that computer. In this example we know there's a conflict related to WinZip, so we have filtered the view to just show this Title.

To resolve the conflict, select the title and click **Resolve**.



Clicking **Resolve** takes you to the **Conflict Resolution** page where you can add and prioritize Management groups to avoid migration rule conflicts as described in Resolving a Migration Rule Conflict.

11.3.3.12 Working offline on migration rules

You can export your installed applications to an Excel format file that can be worked on offline, with template columns that let you define new migration rules. Once you've finished defining the rules you can then import them back into Application Migration.

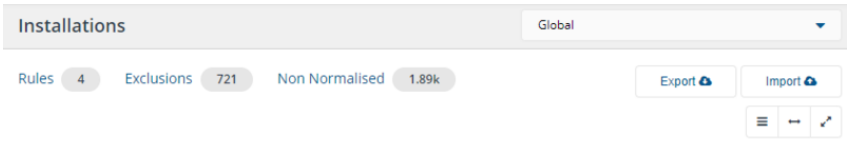
11.3.3.12.1 Exporting your installed applications

To simplify the process for creating new application migration rules, use the export feature – it creates a spreadsheet that has all your installed applications to enable you to create new rules to associate with them without having to be online. Existing rules cannot be modified with this process.

When you have added new rules to the spreadsheet, simply import it back to Application Migration and have your new migration rules implemented.

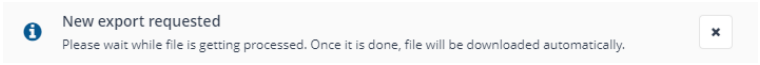
To get an export of your installed applications:

Under the **Applications Migration** menu, click **Installations**.



On the **Installations** page, click **Export** on the top right of the page.

A prompt is displayed while the export takes place. The default download location is the local computer downloads folder.



When the export is complete, you can retrieve the file (*`Application Migration.xlsm`*) from the **Downloads** folder.

11.3.3.12.1.1 What you get with the export

> **Note**
>
> The export includes all inventoried applications from the current view, but will not include any existing rules. To use this feature effectively, filter the display page to include vendors or applications for which you have not already defined rules for, then export it so you can define rules for these installations.

The properties of the exported Application Migration spreadsheet are:

Column	Optionality	Default value	Notes
RuleType	Mandatory		Pick-list to identify the type of migration rule. You must have a value for this column or it results in an error when we pre-flight the input during the import. Values are: Replace Upgrade Retain.
CurrentVendor		Pre-populated	Vendor of the product to be migrated. Pick-list of vendors from the 1E Catalog.

Column	Optionality	Default value	Notes
CurrentTitle		Pre-populated	Title of the product to be migrated. Pick-list of titles available from that vendor.
CurrentVersion		Pre-polulated	Version of the product to be migrated. An asterisk (*) denotes all versions – dot (.) format or colloquial versions.
CurrentEdition		Pre-populated	Edition of the product to be migrated.
ManagementGroup	Mandatory	Global	The Management group the product is associated with. You must have a value for the column or it results in an error when we pre-flight the input during the import.
Usage	Mandatory	Any Usage	Usage category for the product to be migrated. You must have a value for this column or it results in an error when we pre-flight the input during the import. Values are: Any Usage Used Rarely Used Unused Unreported Used | Rarely Used Used | Unused Used | Unreported Rarely Used | Unused Rarely Used | Unreported Unused | Unreported

Column	Optionality	Default value	Notes
			Used | Rarely Used | Unused Used | Rarely Used | Unreported Used | Unreported | Unused Rarely Used | Unused | Unreported.
TargetVendor			Vendor of the product for the migration rule. Pick-list of vendors from the 1E Catalog.
TargetTitle			Title of the product for the migration rule. Pick-list of titles available from the TargetVendor.
TargetVersion			Version of the product for the migration rule. Can be in a dot format or colloquial versions.
TargetEdition			Edition of the product for the migration rule.
ApplicationType	Mandatory		Configuration Manager package/application associated with the target product. You must have a value for this column or it results in an error when we pre-flight the input during the import. Values are: Application Package.
Application/PackageName			Application name of the Configuration Manager package/application associated with the target application.
Application/PackageId			Application ID of the Configuration Manager package/application associated with the target application. Displayed as:

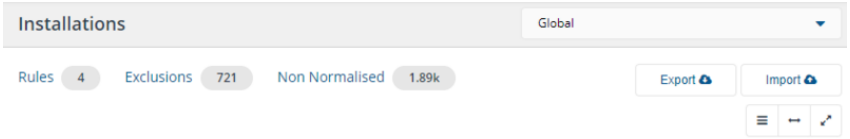
Column	Optionality	Default value	Notes
			Plain text field for Application application type Pick-list for Package application type. There may be multiple packages with the same name and if you choose one of these, you will also choose the PackageId to identify it.
ProgramName			Program name of the Configuration Manager package associated with the target application. Relevant only if ApplicationType = Package
ImportResult			Post-import, for each row, it will display Added, Failed or Skipped.
ImportLog			Post-import, for each row, it will display the reason why the record could not be processed if ImportResult was Failed or Skipped.

11.3.3.12.2 Importing your application rules file

When you have created the new rules for your applications, import the file so that Application Migration can implement your new rules. Ensure you have met the mandatory requirements (refer to the What you get with the export table on this page) before you import your file to avoid non-critical errors being reported.

To import the file:

Under the **Application Migration** menu, click **Installations**.



On the **Installations** screen, click **Import**.

On the **Upload migration rules screen**, click **Choose** file.

Locate your updated import file and click **Open**.

You'll see a prompt as the upload takes place.

When the upload completes, the results are displayed and an import file is automatically downloaded to the **Downloads** folder on your local computer. Refer to the table below for the In-flight validation used.

Click **Close** and locate the file to address any reported issues.

11.3.3.12.2.1 In-flight validation

When you import your migration rules, we run an in-flight validation on your spreadsheet and only create the migration rules when they pass our tests.

Validation on	Checks	Import result	Error message	Remedial action
Rule types	RuleType is mandatory and must must be one of: Replace Upgrade Retain.	Failed	Rule type must be valid.	Provide a valid rule type.
If the rule type is Retain, SourceVersion and SourceEditions cannot	Failed	Rules of Retain type cannot have wildcard rules.	Do not use wildcard characters in source version or source edition.	

Validation on	Checks	Import result	Error message	Remedial action
contain wildcard characters.				
Two duplicate rules must not be present in import file.	Skipped	Another rule for this application, usage and management group already exists in the import file.	Delete one of the rules.	
Rules must be unique for source product, usage and management group. Creating a duplicate rule will throw an error.	Skipped	Another rule for this application, usage and management group already exists in the database.	Delete the rule from the import file as it already exists. If you want to update the rule, please visit the website.	
Rules cannot override an existing Configuration Manager association for a target product.	Failed	The target product in this row is already associated with another CM Application/Package. CM associations cannot be overridden through the import file feature. Please overwrite the CM association through the product user interface."	Assign the same association to the target product as it exists in the database. If you want to update the SCCM association, please visit the website.	

Validation on	Checks	Import result	Error message	Remedial action
Vendor	SourceVendor must not be empty.	Failed	Source Vendor must not be empty.	Provide a valid source vendor.
Title	SourceTitle must not be empty. It is required for a replace rule.	Failed	Source Title must not be empty.	Provide a valid source title.
Version	SourceVersion must not be empty. It must have the minimum value of a.b and must be in one of these formats: a.b, a.b., a.b.c.d, a.*, a.b.*,a.b.c.*, * You cannot use the wildcard character as part of a version, for example a.*.b, a.b.*.c, *.a	Failed	Source Version must not be empty.	Provide a valid source version.
If the rule type is Retain, SourceVersion and cannotcontain wildcard characters.	Failed	Rules of Retain type cannot have wildcard rules.	Do not use wildcard characters in source version.	
TargetVersion must not be empty. It must have the minimum value of a.b and must be in one of these	Failed	Target Vendor, Title or Version is missing.	Provide a valid target version.	

Validation on	Checks	Import result	Error message	Remedial action
formats:a.b, a.b., a.b.c.d.				
Edition	If the rule type is Retain, SourceEditions cannotcontain wildcard characters.		Rules of Retain type cannot have wildcard rules.	Do not use wildcard characters in source edition.
Combination of Vendor, Title, Version and Edition	The combination of SourceVendor, SourceTitle,SourceVersion and SourceTitle must have an equivalent item in the 1E Catalog.	Failed	Source Vendor, Title, Version and Edition has not matching entry in the 1E Catalog.	Select a valid source product.
Combination of Vendor, Title, Version	The combination of TargetVendor, TargetTitle and TargetVersion must not be empty and must have an equivalent item in the 1E Catalog.	Failed	Target Vendor, Title, Version, Edition has no matching entry in the 1E Catalog.	Select a valid target product.
TargetVendor, Target Title and Target Version must not be empty as these values are required for a Replace rule type.	Failed	Target Vendor, Title or Version is missing.	Provide valid target vendor, target title and target vendor for the Replace rule type.	
TargetVersion must not be empty as it is required for	Failed	Target Vendor, Title or Version is missing.	Provide a valid target version for the Upgrade rule type.	

Validation on	Checks	Import result	Error message	Remedial action
an Upgrade rule type.				
Management group	Management group must not be empty. By default, the Global management group is always present.	Failed	Management group name is not valid.	Select a valid Managemen t group.
Usage	Usage is mandatory and must be one of: Unreported Unused Rarely Used Used Any Usage.	Failed	Selected usage is not valid.	Select a valid usage.
Application types	ApplicationType must not be empty and must be one of: Package Application.	Failed	ApplicationTyp e is not valid.	Enter a valid application type.
The Package or Application must already exist in Configuration Manager.	Failed	Associated CM Package or Application is invalid.	Enter a valid Configuration Manager Package or Application.	

11.3.3.13 Managing Configuration Manager association alerts

Application Migration users will see alerts on specific pages that identify orphaned applications - when one or more rules or applications in an application set reference Configuration Manager objects that no longer exist, or where the Configuration Manager association has been deleted.

11.3.3.13.1 What are associations?

Applications and Packages in Configuration Manager are identified by a name and optionally publisher and version arbitrarily determined by the Configuration Manager administrator that created them. The platform uses a standard format of Vendor, Title, Version and Edition to identify applications.

The **Manage Associations** section of Inventory enables an administrator to effectively normalize the Applications and Packages imported from Configuration Manager by associating them with a Vendor, Title, Version and Edition defined in the 1E Catalog. These associations are then used to define migration rules in Application Migration, refer to Managing migration rules and reclaim rules in AppClarity.

11.3.3.13.2 What happens if an association is broken?

You will be notified when some rules are associated with Configuration Manager packages or applications that no longer exist on the following pages:

Manage Rules.

Installations.

Role Based Applications.

To manage associations, the Inventory repository used by your application must be populated by a **System Center Configuration Manager** connector that collects details of Applications and Packages defined in Configuration Manager.

There are two reasons why an association could be broken:

Someone has explicitly changed or deleted the association on the Manage associations page.

Someone has explicitly changed or deleted the source package or application the association depended on from Configuration Manager. In this case, the impact will only be seen after the **System Center Configuration Manager** connector sync has run.

Notifications will appear after the **Application Migration Consolidation** action has run.

For how associations and connectors work, refer to Manage associations and System Center Configuration Manager connector.

For managing rules in Application Migration, refer to Managing migration rules.

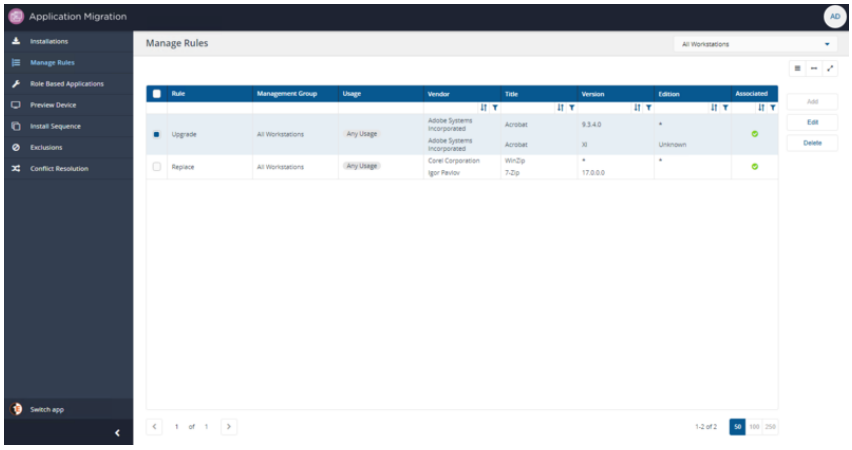
11.3.3.13.3 Managing association alerts

Manage Rules page

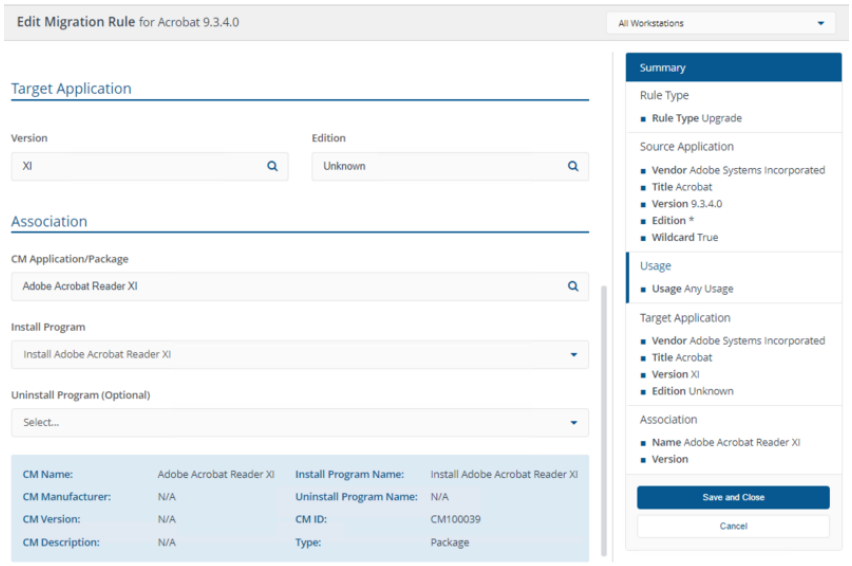
In this example we have a Rule to upgrade computers in the **All Workstations** Management Group from Adobe Acrobat version 9.3.4.0 to Adobe Acrobat XI.

To upgrade Adobe Acrobat version 9.3.4.0, the migration rule has an association with a Configuration Manager package for Adobe Acrobat Reader XI which has a Configuration Manager package ID of **CM ID - CM100039**.

Manage Rules page:



Configuration Manager Association:



Viewing associations between Configuration Manager and products

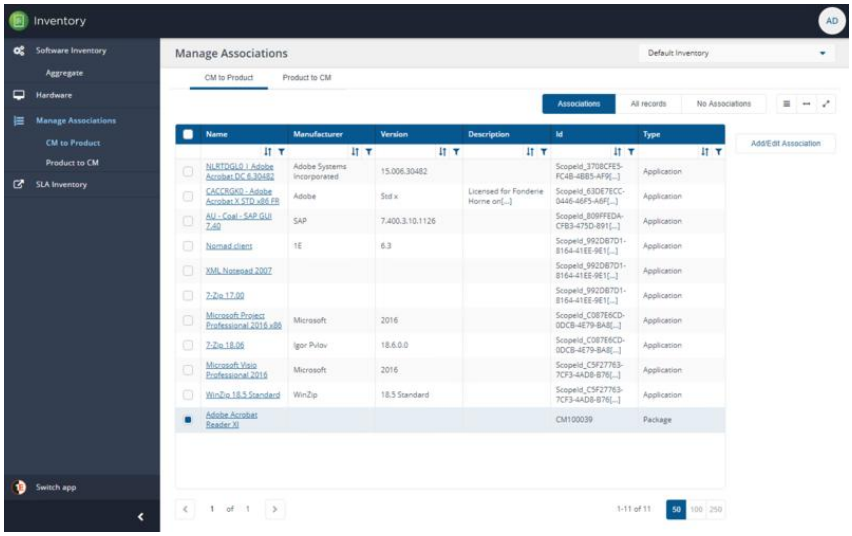
Associations between products and Configuration Manager packages and applications are managed in the Inventory Application.

In our example, we can view the Adobe Acrobat Reader XI associations by switching to the Inventory app and then on the **Manage Associations** page, viewing **CM to Product**, selecting **Adobe Acrobat Reader XI** and clicking **Add/Edit Association**.

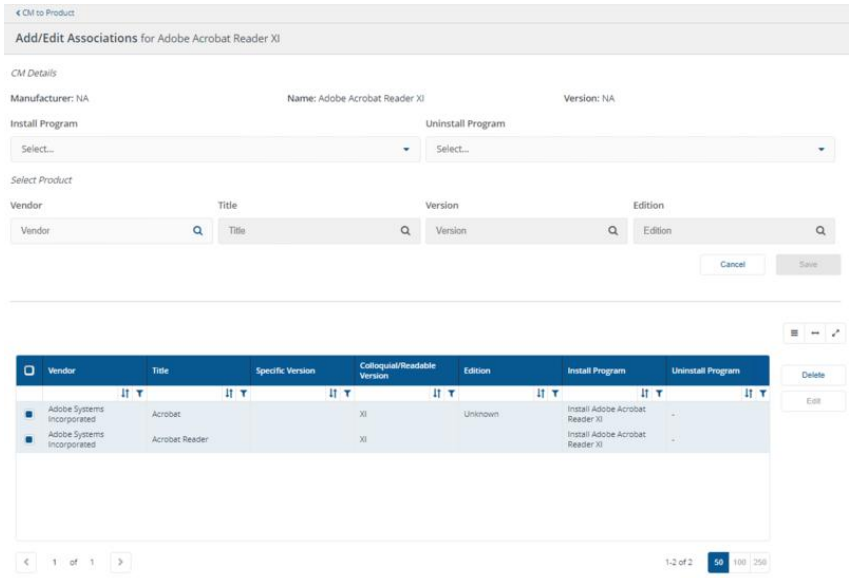
On the **Add/Edit Associations** for **Adobe Acrobat Reader XI** we can see that Adobe Acrobat Reader XI is associated with the correct application in Configuration Manager.

To find out more about how the Inventory Application works, please refer to Introducing Inventory.

Manage Associations page:



Add/Edit Associations for Adobe Acrobat XI:



When an alert is generated

If the Configuration Manager association is no longer present because, for example either the associated Configuration Manager application or package has been deleted from Configuration Manager. Or the Configuration Manager association has been deleted in Application Migration. You will see an alert.

In our example, the Adobe Acrobat XI package gets deleted from Configuration Manager. At the point of deletion Application Migration does not know the package is gone.

It is after the next **Generate Report - Application Migration Consolidation** runs and the **Manage Rules** page gets refreshed, that you will see an alert.

> **Tip**
>
> It's good practice to schedule the regular synchronization of data from Configuration Manager into Application Migration using the System Center Configuration Manager inventory connector.

You should schedule the connector to execute regularly to keep the data in Application Migration up to date, ensuring new devices, new software installations, and software removals are correctly reported.

To perform this task you will need to be logged into the Tachyon portal as a user with the Schedule Administrator role. The Application Migration Administrator role does not have the required permissions to schedule connectors.

Refer to the Schedules page for details on how to schedule a connector.

Note

To fully understand how to:

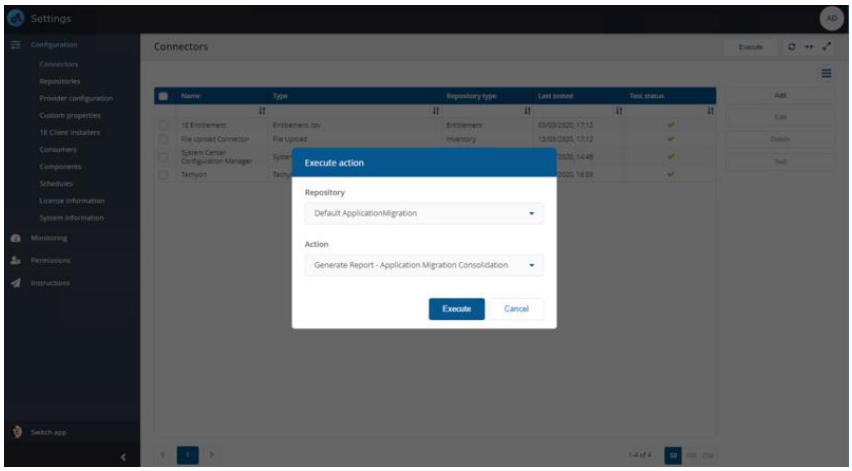
Get data into Application Migration from Configuration Manager.

Keep data synchronized between Application Migration and Configuration Manager.

Execute consolidation actions independently.

Please refer to Post-install configuration.

Generate Report - Application Migration Consolidation:



What the alerts look like

You will see an alert displayed in a banner at the head of the page indicating there are one or more rules associated with Configuration Manager packages or applications that no longer exist. In the **Associated** column there will be a warning symbol indicating which specific rule has a missing association.

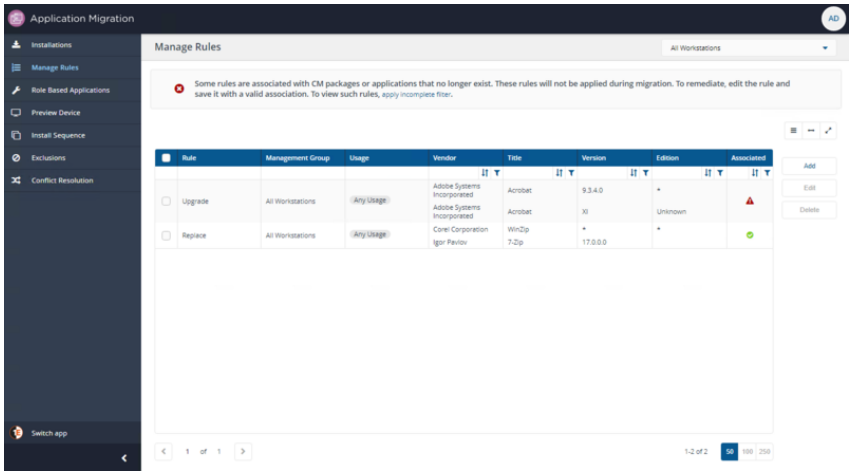
Using the **apply incomplete filter** link in the warning banner you can apply a filter to display incomplete rules and then remediate them by investigating and fixing the missing associations.

For example, if a package has been removed from Configuration Manager, you would need to either recreate or re-import this package in Configuration Manager. You could also adopt your migration rule to include a package that is still present in Configuration Manager.

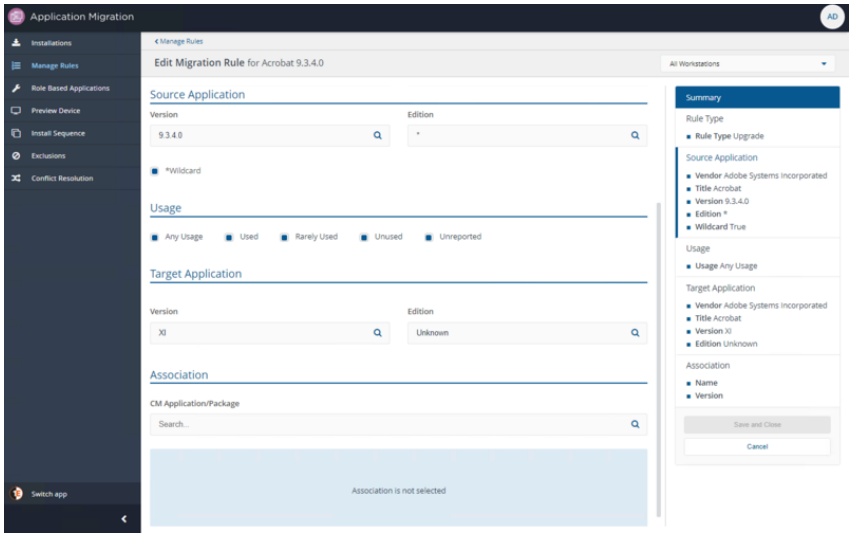
Or, if the package is present in Configuration Manager and only the association was removed, then you will need to recreate the appropriate associations for your rule to work correctly.

For more details about adding, modifying and deleting migration rules in Application Migration please refer to Managing migration rules.

Refreshed Manage Rules page:



Configuration Manager associations are no longer present:



11.3.4 Managing product exclusions

Products can be excluded from consideration by Application Migration, helping you to focus on the important products and minimizing effort during the Application Migration workflow.

11.3.4.1 What are exclusions?

The list of products in 1E Catalog is quite substantial and contains items such as security updates, service packs, hotfixes, drivers, etc which are not useful if you are compiling application migration rules. There may also be applications that you do not use in your organization, for example Cisco Jabber has no value to you if you are committed to Skype for Business as your instant messenger.

You most likely will not want to create migration rules for these types of applications and the Exclusions feature helps reduce the level of noise you have to navigate. Excluded applications are based on vendor, title and edition and fall into two categories.

11.3.4.1.1 System driven exclusions

These exclusions (typically service packs, hotfixes, security updates, etc.) are automatically managed by Application Migration – they are filtered out when you run the Application Migration consolidation report or when its next synchronization event takes place. The algorithm looks for these sub strings to build an exclusions list:

security update for

update for

visual c++ redistributable

Multi-Targeting Pack

service pack

language pack

integration pack

targeting pack

developer pack

boosterpack

codec pack

clipartpack

compatibility pack

hotfix for

integration package

visual j# redistributable

mui pack

Windows Server

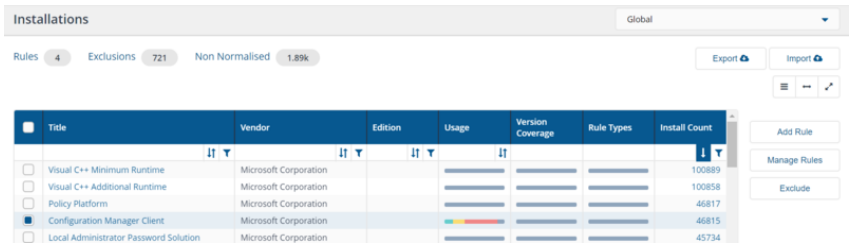
Windows.

11.3.4.1.2 User driven exclusions

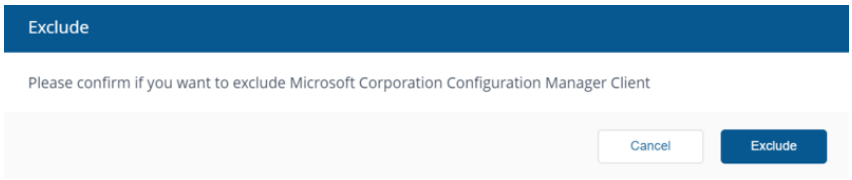
User driven exclusions (typically those that have no relevance to your organization) are those you specifically choose to exclude. For example, if you choose to exclude Microsoft SQL Server Compact edition, all versions for that product will be excluded, however other SQL Server editions will be unaffected.

11.3.4.2 Adding to the list of exclusions

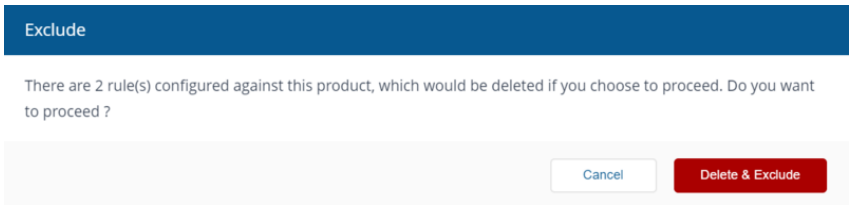
To exclude an application, on the **Installations** page, locate the application you want and click **Exclude**. Click the filter icon to narrow down the list if necessary.



You can exclude applications irrespective of whether they have migrations rules associated with them or not. You will be prompted to confirm your actions. If there are rules associated with the application, the prompt will notify you of the number of rules associated with it and to confirm your intentions to exclude the application.



In this case the popup button text will be changed to be **Delete & Exclude** and the color will change to red indicating that there are consequences for the action. The associated rules are deleted if you proceed.



Multiple applications can be selected and excluded at the same time.

There are now four scenarios for excluding applications:

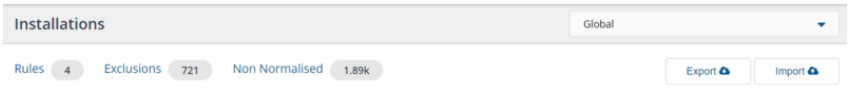
Scenario	Behavior
Excluding a single application with no associated rules.	An **Exclude** popup is displayed that shows the name of the application.
Excluding a single application with associated rules.	An **Exclude** popup that shows the name of the application and a count of the associated rules.
Excluding multiple applications with no associated rules.	An **Exclude** popup is displayed that shows the number of applications being excluded.

Scenario	Behavior
Excluding multiple applications with associated rules.	An **Exclude** popup is displayed that shows the number of applications being excluded an a count of all the associated rules for all of those applications.

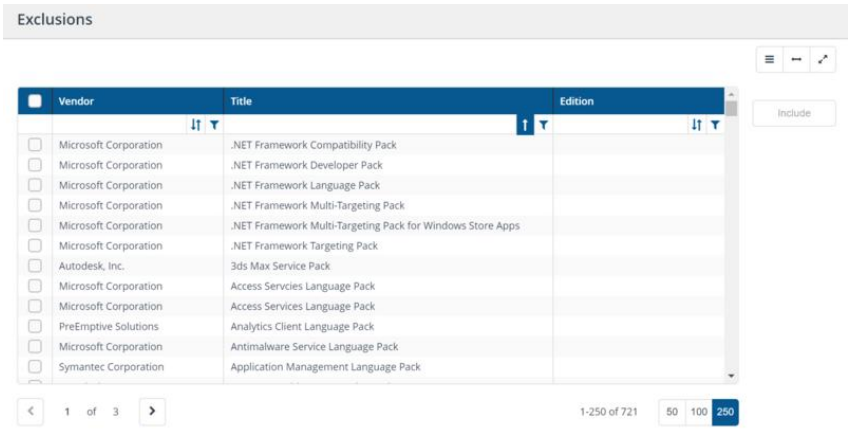
11.3.4.3 Reviewing your exclusions

To view a list of your exclusions:

On the **Installations** page (the number after the exclusions link indicates the total number of excluded products). Clicking the Exclusions link takes you to the Exclusions page.



The list of exclusions on the Exclusions screen are sorted by **Vendor**, **Title** and **Edition**.



To include an excluded application so that it can be part of your application migration strategy, locate the application and check the checkbox to select it, click **Include**. Click the filter icon

to narrow down the displayed list if necessary. Follow-up by adding a migration rule to this included application, for more information refer to Managing your rules.

11.3.5 Previewing post-OS migration application states

Before deploying the OS Deployment Task Sequence, you can preview the effect that Application Migration will have on the software installed on a device. This can be for existing or new build devices. This is done from **Preview Device**, where you can see the following menu items:

Menu item	Description
Existing Device	Post-migration application status for existing computers undergoing an in-place upgrade or a computer refresh.
New Device	Applications to be installed on new-build computers by Management Groups or device attributes.

Applications not subject to migration rules behave differently depending on the type of OS deployment, as follows:

Computer refresh also known as **wipe and load** - applications for which no migration rule exists will be removed, that is not reinstalled when the new OS is installed)

In-place upgrade - applications for which no migration rule exists are retained, as in-place upgrade does not remove any applications

Computer replacement - if the device is being replaced and either a Computer Association defined in Configuration Manager or the 1E Windows Self-service Assistant is being used for the replacement, applications for which no migration rule exists will not be installed on the new device. To preview the results of a replacement, select the old device and the Wipe-and-load option.

New devices - for completely new computers you can use the Preview Device feature to see which Role-based Applications will be installed on a new device. As the new device does not exist, you need to either select the specific Management Group that the computer *will* exist in once it is built, or define the attributes (name, AD Site or OU, or any combination of these) that the computer *will* have when it is built.

11.3.5.1 Previewing applications installed on existing devices post-migration

When you preview a computer, you'll be able to see the following information:

Management groups associated with the computer

Products installed on the computer along with their usage statistics

Migration rule statuses:

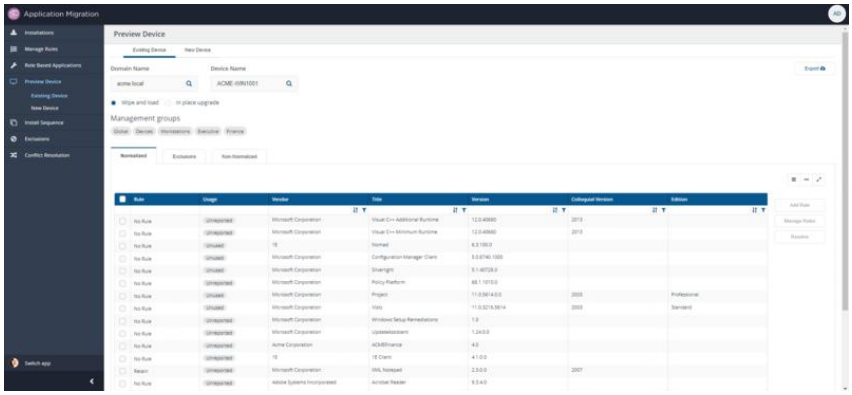
No rule – if a rule has not been set up

Retain, Replace, Upgrade rules – if they are set up

Conflict – if there are conflicting rules for that particular product.

Excluded applications on the computer

Applications on the computer which have not been normalized.

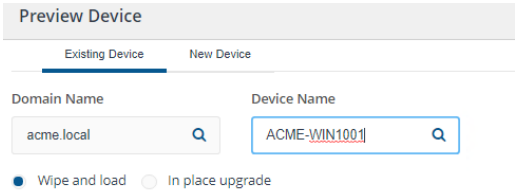


To get a post-migration preview of an existing computer:

Under the **Preview** Device menu click **Existing** Device .

Choose the type of deployment you want - **Wipe and Load** or **In-place upgrade**.

In both **Domain Name** and **Device Name** fields, start typing a name and a list matching your string is dynamically displayed for you to choose from.



11.3.5.1.1 Behavior of the post-migration preview screen and table

In our example, we are going to preview the **Wipe and load** post-migration application state for **ACME-WIN1001** which is in the **ACME.local** domain.

When we selected ACME-WIN1001 as **Device Name**, the Global, Devices, Workstations, Executive and Finance Management Groups are identified. ACME-WIN1001 is member of all these Management groups. If a computer is a member of more than one Management Group, they will be identified under the **Management groups** heading. Below this heading, is the details table which is made up of three tabs:

Normalized

Exclusions

Non-Normalized.

11.3.5.1.2 Normalized

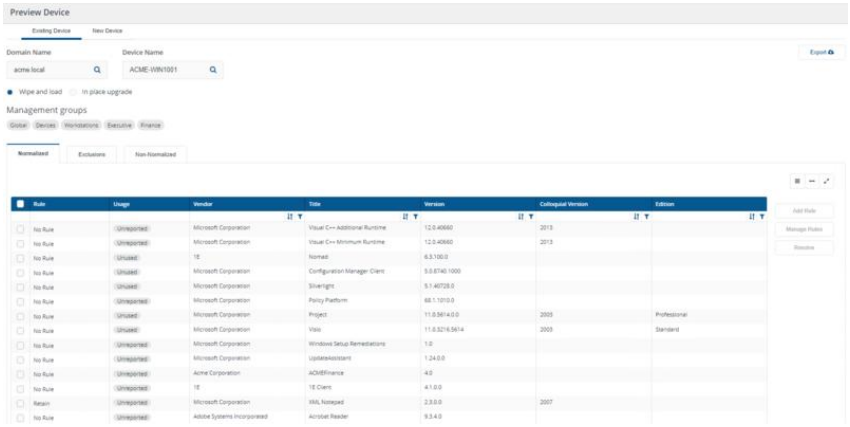
The Normalized tab displays a list of applications installed on ACME-WIN1001 which have a corresponding item in the 1E Catalog. The table in this tab displays a preview of the post-OS application migration state for a **Wipe and load** deployment. For each application in the table, you will be able to identify:

Rules associated with it under the **Rules column.**

Usage statistics

Details about the application in the **Vendor**, **Title**, **Version**, **Colloquial Version** and **Edition** columns

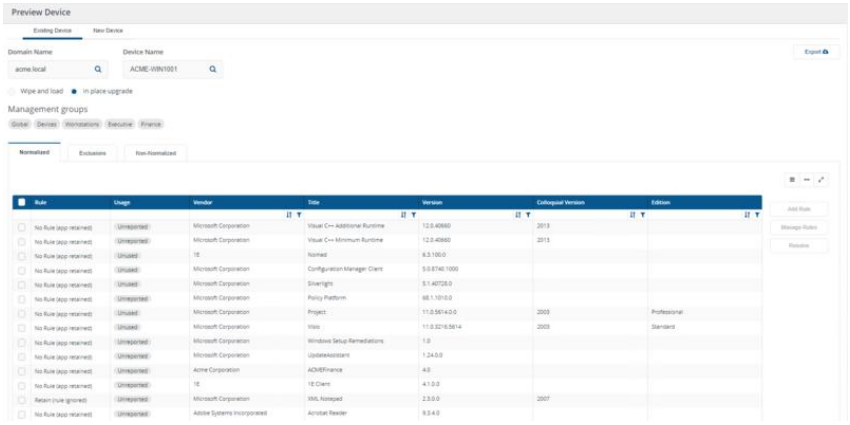
Options to **Add Rule**, **Manage Rules** or **Resolve** conflicts.



If we had chosen to preview the **In-place upgrade** post-migration application state forACME-WIN1001 notice the following changes where an application is:

Subject to a **Retain** rule for the **Wipe and load deployment**, (In the example shown this is XML Notepad, the second row from the bottom) the rule is ignored and the **application is not installed** for the **In-place upgrade** as all installed applications are retained anyway during an in-place upgrade.

Not subject to a rule (**No rule**) for the **Wipe and load** deployment, it is **retained** (last row) for the **In-place deployment** as all installed applications are retained anyway during an in-place upgrade.

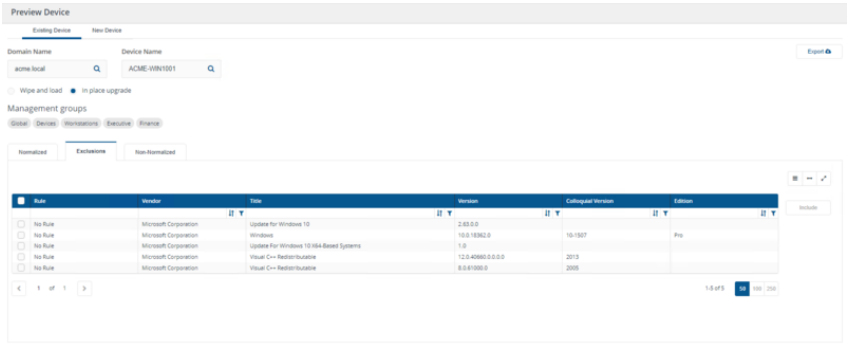


11.3.5.1.3 Exclusions

The Exclusions tab displays all excluded products for the computer ACME-WIN1001.

The list of products in 1E Catalog is quite substantial and contains items such as security updates, service packs, hotfixes, drivers, etc which are not useful if you are compiling application migration rules. There may also be applications that you do not use in your organization, for example Cisco Jabber has no value to you if you are committed to Skype for Business as your instant messenger.

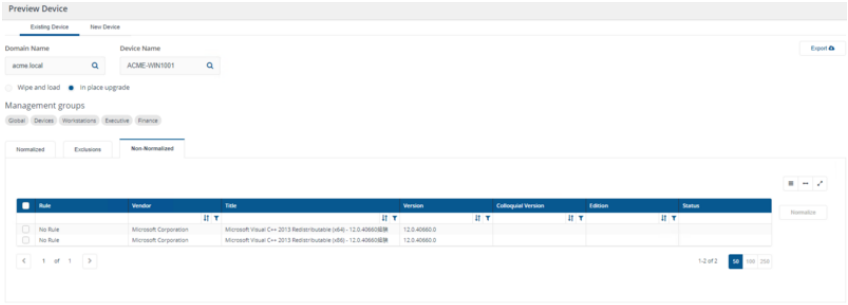
Please refer to Managing product exclusions for more details.



11.3.5.1.4 Non-normalized

The Non–normalized tab displays all unmatched source applications for ACME-WIN1001. You can add an item from this list to the Catalog by selecting it and clicking **Normalize**.

Normalization is a Platform function that refers to the process of finding (or not finding) a match rule in 1E Catalog, then deduplicating and rationalizing the information using Platform logic, and publishing the information on the 1E Catalog UI. Partial Matching for example does not have a match rule in 1E Catalog but it's still normalized and published on the UI using Platform logic.



11.3.5.2 Previewing applications to be installed on new devices

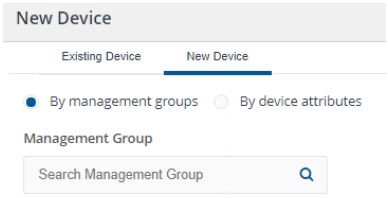
As well as previewing the post-migration status for existing computers that are subject to an in-place upgrade or a computer refresh, you can preview applications that will be installed on new devices. This allows you to modify application rules or applications associated with Role Based Applications Sets before carrying out your production builds.

This feature works by evaluating the combination of rules assigned to a particular Management Group and the rule-based application sets you create and associate with those Management Groups.

To preview applications to be installed on new-build computers:

Under the **Preview** Device menuclick **New** Device .

Click **New Device**.



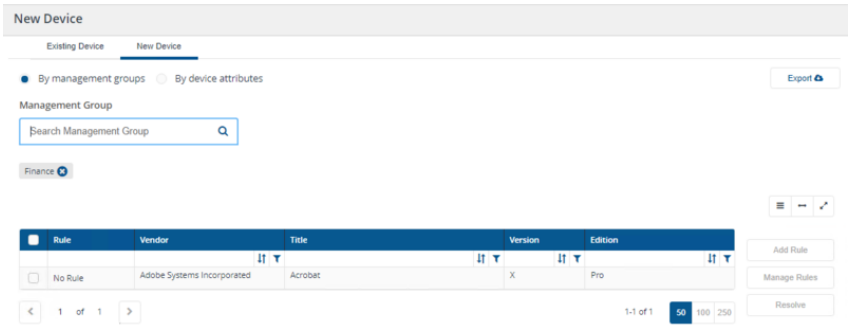
You can view the new computer two ways:

By management groups

By device attributes.

11.3.5.2.1 By management groups

On the **New Device** screen, select **By management groups.**



In **Management Group** start typing the name of a Management Group. A list matching your search string is displayed for you to choose from.

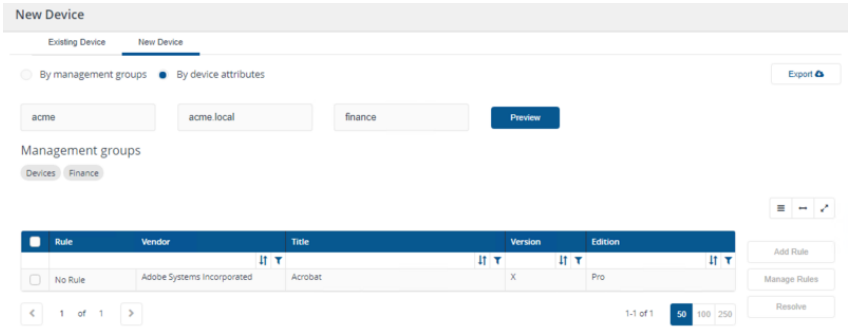
The table shows applications that will be installed on new builds complying with the rules assigned to that Management Group and the Role-based Application Sets you create and associate with it.

You can choose more than one Management Group to preview. If the list of applications is incorrect, you can update the Role-Based Application Set you created and run the preview again.

You can also add and manage Application Migration rules from this view for any of the listed applications by clicking **Add Rule.**

11.3.5.2.2 By device attributes

On the **New Device** screen select **By device attributes.**



You only need to know the details of any one of the three attributes to retrieve the list of applications for installation on new builds:

Device Name

Active Directory Site

Organizational Unit.

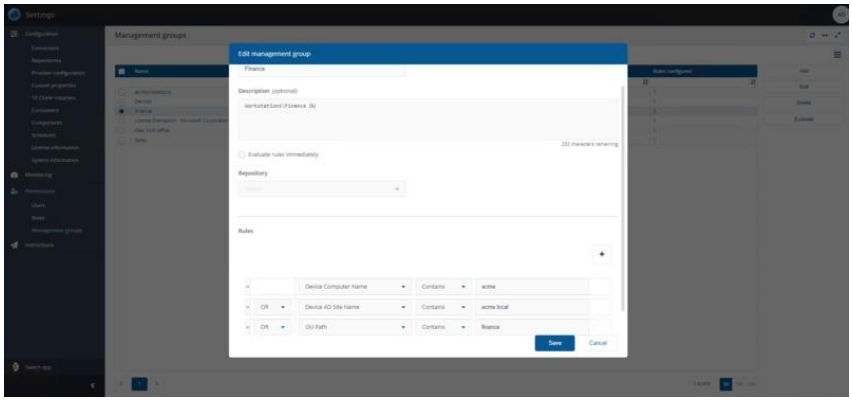
For example:

We created the **Finance** Management group with the following rules:

Device name contains **acme**

Active Directory Site name is **acme.local**

Organizational Unit is **finance**.



On the **Preview Machine screen**, we start typing the name of a computer, the AD site or the OU. In our illustration, we have populated the computer attribute fields with the values from the rule we created for the **Finance** Management group.

The table shows applications that will be installed on new builds complying with the rules assigned to that Management Group and the Role-based Application Sets you create and associate with it.

For more information about Management groups and how to use them, please refer to Management Groups page.

11.3.5.3 Exporting device preview information

You can export the device preview information to an Excel spreadsheet using the **Export** button at the top-right of the interface. This information can be presented to end-users to give them some indication of the software that will be present on their device post-OS migration.

The information in the exported file is described in the following tables for **Existing Devices** and **New Devices**:

11.3.5.3.1 Existing Devices

The information in the exported file, **ExistingDeviceWipeAndLoad.xlsx** is described in the following tables for **Existing Devices** (one per sheet in the Excel file):

The Normalized sheet

Column	Description
Rule	List to identify the type of migration rule. Values are: Replace Upgrade Retain No Rule.
Usage	Usage category for the product to be migrated. Values are: Any Usage Used Rarely Used Unused Unreported Used | Rarely Used Used | Unused Used | Unreported Rarely Used | Unused Rarely Used | Unreported Unused | Unreported

Column	Description
	Used | Rarely Used | Unused Used | Rarely Used | Unreported Used | Unreported | Unused Rarely Used | Unused | Unreported.
Source Vendor	Vendor of the product to be migrated.
Source Title	Title of the product to be migrated.
Source Version	Version of the product to be migrated. An asterisk (*) denotes all versions – dot (.) format.
Source Colloquial Version	Version of the product to be migrated, colloquial version.
Source Edition	Edition of the product to be migrated.
Target Vendor	Vendor of the product for the migration rule.
Target Title	Title of the product for the migration rule.
Target Version	Version of the product for the migration rule. Can be in a dot format or colloquial versions.
Target Edition	Edition of the product for the migration rule.

The Exclusions sheet

Column	Description
Rule	List to identify the type of migration rule. Values are: Replace Upgrade Retain No Rule.

Column	Description
Vendor	Vendor of the product to be excluded.
Title	Title of the product to be excluded.
Version	Version of the product to be excluded. An asterisk (*) denotes all versions – dot (.) format.
Colloquial Version	Version of the product to be excluded, colloquial version.
Edition	Edition of the product to be excluded .

The Non-Normalized sheet

Column	Description
Rule	List to identify the type of migration rule. Values are: Replace Upgrade Retain No Rule.
Vendor	Vendor of the product to be migrated.
Title	Title of the product to be migrated.
Version	Version of the product to be migrated. An asterisk (*) denotes all versions – dot (.) format.
Colloquial Version	Version of the product to be migrated, colloquial version.
Edition	Edition of the product to be migrated.

11.3.5.3.2 New Devices

The information in the exported file, **NewDeviceByDeviceAttributes.xlsx** is described in the following table for **New Devices** :

Sheet1

Column	Description
Rule	List to identify the type of migration rule. Values are: Replace Upgrade Retain No Rule.
Source Vendor	Vendor of the product to be migrated.
Source Title	Title of the product to be migrated.
Source Version	Version of the product to be migrated. An asterisk (*) denotes all versions – dot (.) format or colloquial versions.
Source Edition	Edition of the product to be migrated.
Target Vendor	Vendor of the product for the migration rule.
Target Title	Title of the product for the migration rule.
Target Version	Version of the product for the migration rule. Can be in a dot format or colloquial versions.
Target Edition	Edition of the product for the migration rule.

11.3.6 Role Based Application Sets

A Role Based Application Set defines a set of applications that should be installed on a computer for a user performing a particular role, or perhaps working at a particular location.

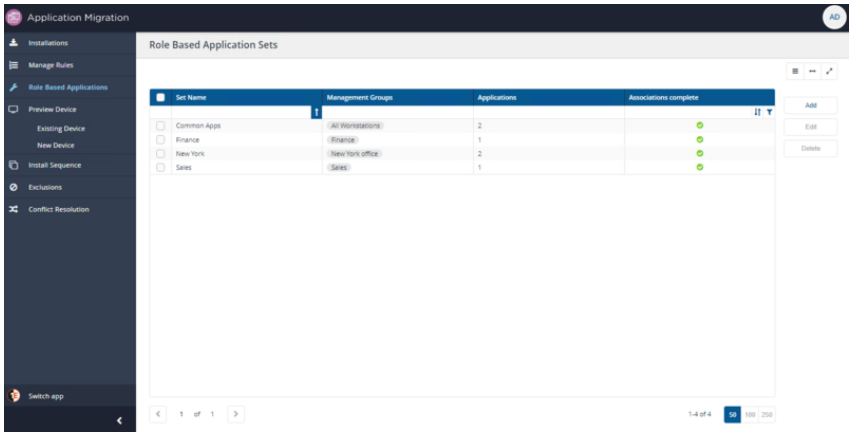
Role Based Application Sets are primarily designed to be used when building a new computer, where there are no applications to be migrated but there is a base set of applications the new user needs. They can also be applied when rebuilding, upgrading or replacing a computer, so the user gets the applications defined for their role plus any applications migrated as a result of migration rules.

11.3.6.1 How Role Based Application Sets work

Before defining Role Based Application Sets, you will need to create Management groups in Tachyon platform corresponding to the roles or locations that your Application Sets will apply to. Management groups can be defined using AD Site, OU or Computer Name. You can use partial matching of computer name in a Management group definition if your computer naming convention includes identifiers for location or department.

Role-based Application Sets are built by defining the name of the set and the Management groups the set is associated with, you then add applications to the set. You can preview the results of Role-based Application Sets on a computer from the Preview Device page in Application Migration. At deployment time, the Application Migration step in the Task Sequence returns the list of applications that need to be installed based on matching of the computer name, Organizational Unit (OU) and Active Directory (AD) site of the computer being deployed.

If a computer meets the criteria of multiple Management groups, the combination of all applicable application sets applies. If two or more applicable application sets include different versions or editions of the same application (vendor and title), Application Migration will attempt to install all versions / editions. The end result on the computer will depend on the behavior of the vendor's installers - for example, if they support side-by-side installation of multiple versions - and may be affected by Application Supersedence rules in Configuration Manager.



To read more about:

Management groups, refer to Management Groups page

How to create and manage Role-based Application Sets, refer to Managing Role-based Application Sets.

> **Note**
>
> Migration rules are applied to Role Based Application Sets before the results are returned.
>
> For example, if your application set includes Visio 2013 but there is a rule applicable to the computer being deployed that upgrades Visio 2013 to Visio 2016, Application Migration will return Visio 2016 in the list of applications to be installed.

11.3.6.2 Working with Role Based Application Sets

The following examples show the behavior of Role-based Application Sets, based on the following Management groups:

Management group name	Included applications	Membership criteria	Members
All Workstations	Adobe Acrobat DC Standard 7-Zip 17.0.0.0	Workstations OU	ACME-WIN1001, ACME-WIN1002, ACME-WIN701, ACME-WIN702, ACME-WIN802
Sales	Microsoft Project Professional 2016	Workstations\Sales OU	ACME-WIN702
Finance	SAP GUI 7.4.0	Workstations\Finance OU	ACME-WIN802
New York office	WinZip 18.5.0 Standard XML Notepad 2007	New York AD site	ACME-WIN1003

11.3.6.2.1 Simple implementation of a Role Based Application Sets

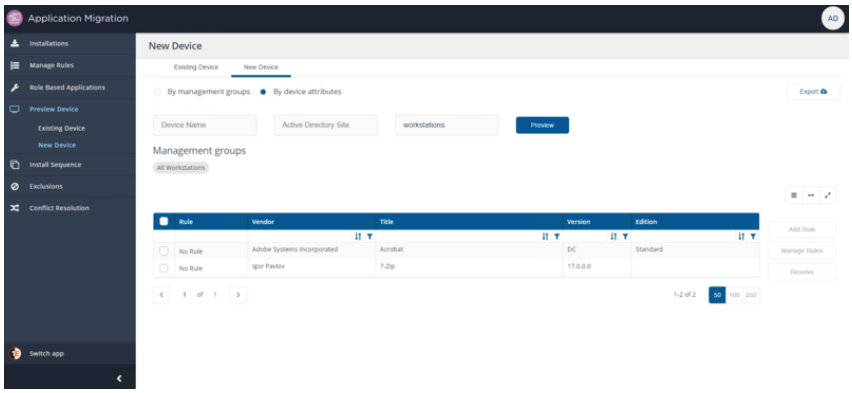
In the following example, a Role Based Application Set named Common Apps has been created for the **All Workstations** Management group.

The set includes Adobe Acrobat DC Standard and 7-Zip 17.0.0.0. Because the **All Workstations** Management group includes all computers in the Workstations OU, any new computer that's added to the Workstations OU in the Task Sequence will have Adobe Acrobat DC and 7-Zip 17.0.0.0 installed.

You can use the preview **New Device** view to determine what applications will be installed when a new computer is built. Application Migration can determine which Management groups it will belong to based on how it will be configured during the OS deployment.

On **Preview Device**, the administrator selects **New Device** then selects **By device attributes**. The admin knows the new computer will be added to the Workstations OU, so enters Workstations in the OU field to find the corresponding Management group which is All Workstations.

The results show the Management groups the computer will belong to based on the attributes entered. This defines the applications that will be installed on that computer, in this case Adobe Acrobat DC Standard and 7-Zip 17.0.0.0 from the Common Apps set.



Please refer to Previewing post-OS migration application states for details about what the applications on a device will look like after OS migration.

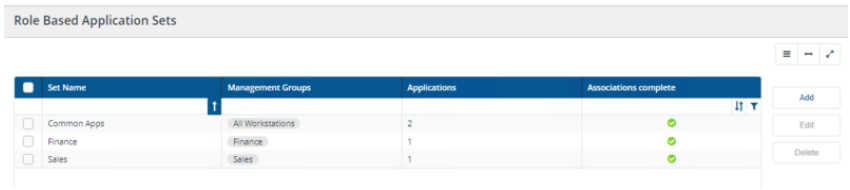
> **Note**
>
> It's possible to associate a Role Based Application Set with multiple Management groups. For example, we could have used the Sales and Finance Management Groups instead of All Workstations.

Applying multiple Role-based Application Sets

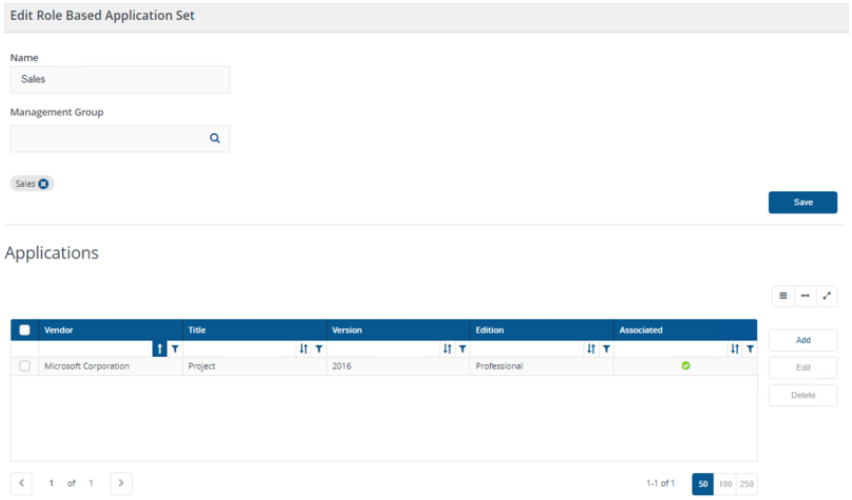
It's possible for a computer to exist in multiple Management Groups and have multiple Role-based Application Sets applied to it.

For example, the Sales Management group includes computers in the Sales OU and the All Workstations Management group includes computers in the Workstations OU.

Because the Sales OU is a child of the Workstations OU, a computer in the Sales OU will also be in the Workstations OU. A computer built in the Sales OU will be included in both All Workstations and Sales Management groups and have the Common Apps and Sales applications installed.

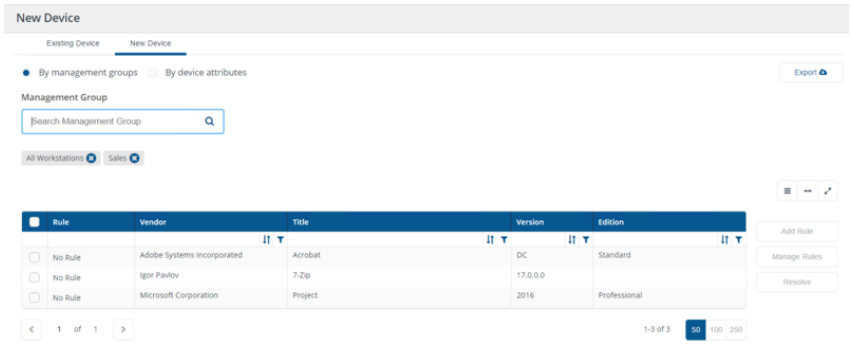


The Sales applications set includes just Microsoft Project Professional 2016



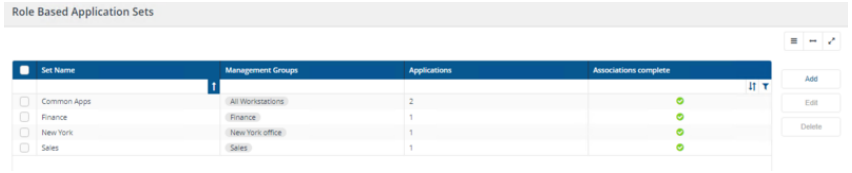
The Preview page does not allow you to select multiple OUs when viewing results **by device attributes**. Instead, you can view **By management groups** and select multiple management groups, as shown in the example.

Using the **By management groups** view, you can see that a computer built in the Workstations\Sales OU will get Adobe Acrobat Standard, 7-Zip 17.0.0.0 and Project Professional 2016.

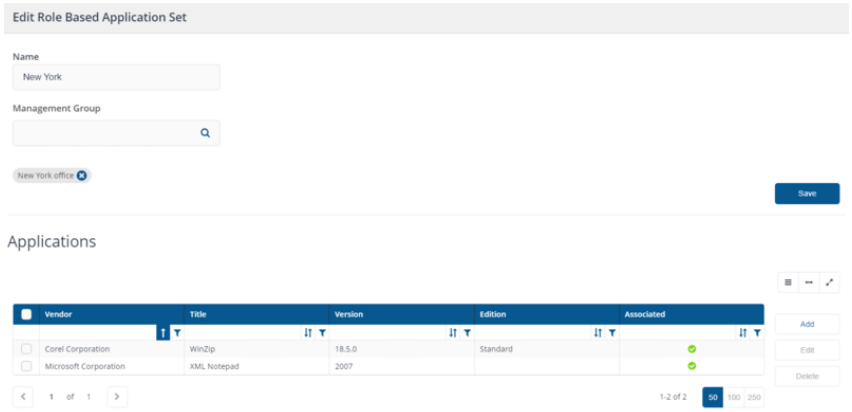


11.3.6.2.2 How Migration Rules modify applications installed using Role-based Application Sets

The following example shows how migration rules can change applications defined in a Role-based Application Set. In this example, we'll add a Role Based Application Set for the New York office Management group.



The New York office application set includes WinZip 18.5.0 and XML Notepad 2007.



As the New York Management Group is based on the New York AD site, we can use device attributes to preview what applications would be installed on a computer that was built in New York in the Workstations OU.

Although the New York Office application set included WinZip, a migration rule has been defined to replace WinZip with 7-Zip, so a computer build in New York in the Workstations OU (All workstations Management Group) will have these applications installed:

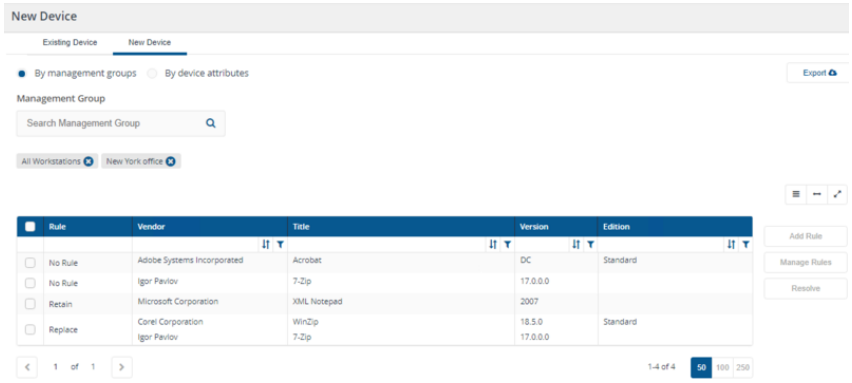
Adobe Acrobat DC Standard

XML Notepad 2007

7-Zip 17.0.0.0.

Role-based Application Sets are likely to be defined in the early stages of Application Migration implementation and may not be updated frequently, whereas migration rules are likely to be updated more frequently as new application versions are released.

The behavior of Role-based Applications ensures the latest rules are applied to Role-based Application Sets. This means you can be sure that new computers are built with the current set of applications even if the Role-based Application Set has not been reviewed for some time.



11.3.6.2.3 Auto Install for Configuration Manager Applications and Packages

Application Migration uses the **Install Application** and **Install Package** steps in a Task Sequence to install migrated applications and packages. These Task Sequence steps are dependent on the relevant checkbox (auto install flag) being enabled for *each* application and package:

Allow this application to be installed from the Install Application task sequence action without being deployed

Allow this program to be installed from the Install Package task sequence action without being deployed.

If a checkbox is not enabled, the software installation will fail for that application or package. An administrator can enable this checkbox for each application and package by using either of the following methods:

in Configuration Manager during or after creating each application and package,

using the **Auto Install** feature in Application Migration when creating application associations, rules or Role Based Application sets.

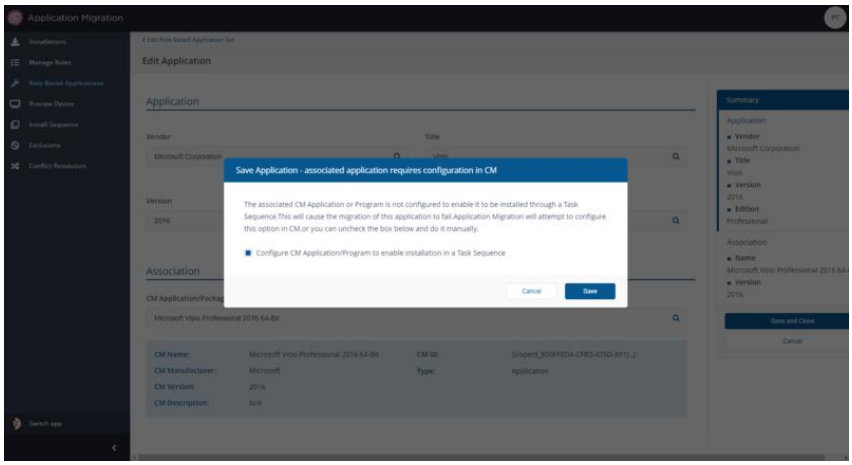
For information about manually enabling these checkboxes for Configuration Manager applications and packages, please refer to Using Application Migration in a Task Sequence: Auto Install for Configuration Manager Applications and Packages.

> **Note**
>
> Application Migration's **Auto Install** feature is able to read the checkbox (auto install flag) for applications and programs, but in order for Application Migration to enable them for you, you'll need to configure related providers in the Settings application of the platform. These should already be configured as a post-installation step. Refer to Post-install configuration.

11.3.6.2.3.1 How Auto Install works with Role Based Application Sets

Once the provider configuration is configured, you can enable the relevant Configuration Manager checkboxes
Allow this application/program to be installed from the Install Application/Package task sequence action without being deployed for Configuration Manager applications/packages associated with a Role Based Application set.

When you create or edit an application or package in a Role Based Application set rule you will be prompted to check **Configure CM Application/Program to enable installation in a Task Sequence** when you click **Save and close**.

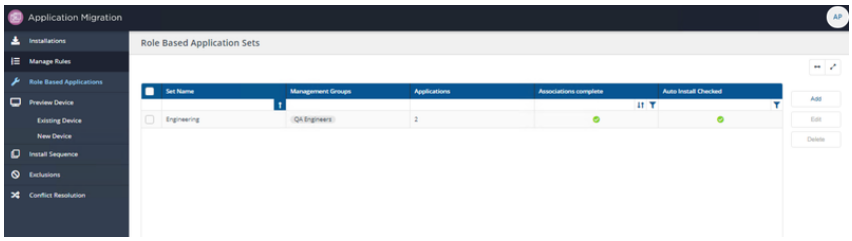


The current state of the Auto Install flag for a Role Based Application set can be seen on the Role Based Application Sets page, as shown in the example.

The **Auto Install Checked** column can have either of the following values:

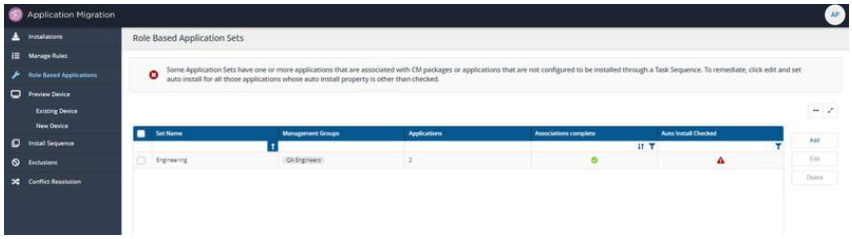
Yes - all applications in the set have auto install value checked

No - at least one of the applications have auto install value other than checked.



Note

If Role Based Application set has an application with the Auto Install unchecked, you will be prompted to edit that rule and set the Auto Install to enabled. You can view this type of rule by filtering the **Auto Install** column by **Not Checked**.

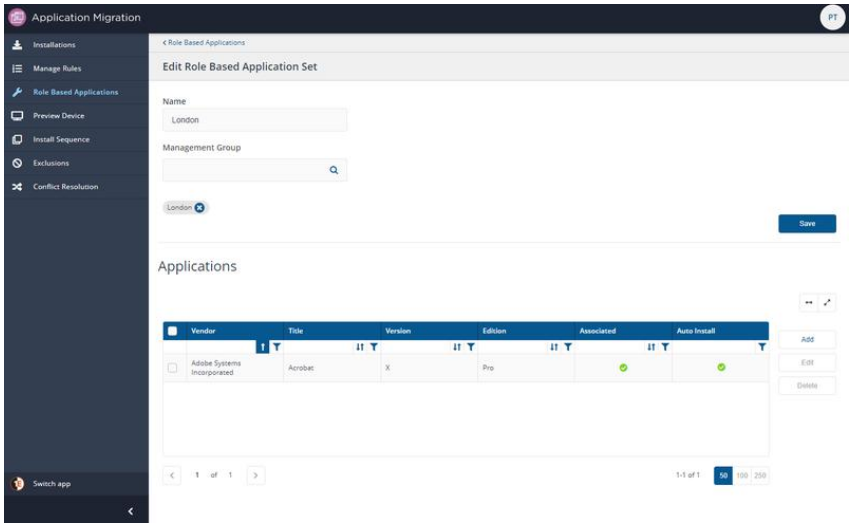


The current state of the Auto Install flag for individual applications of a Role Based Application set can be seen while editing a Role Based Application set as shown opposite.

The **Auto Install** column displays a status for each migration rule. Our example shows two different types of status, **In-Progress** and **Not Checked**.

Auto Install status	Description
Checked	Auto install flag for Configuration Manager application or package program is set.
Not Checked	Auto install flag for Configuration Manager application or package program is not set.
In-Progress	Application Migration has triggered an operation which attempts to set the auto install flag of Configuration Manager application or package program.

Auto Install status	Description
Failed	Application Migration triggered an operation which failed while trying to set the auto install flag of Configuration Manager application or package program.
Not Applicable	A rule has a broken association and the application migration report is not run.



Note

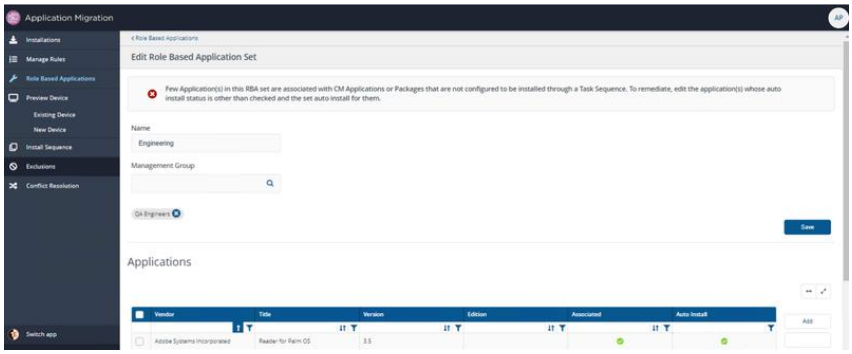
If an application in a Role Based Application set has the Auto Install unchecked, you will be prompted to edit that rule and set the Auto Install to enabled.

You will also see a similar message on the following Application Migration pages and a prompt to take action if the Auto Install is unchecked:

Installation

Preview Device→Existing Device

Preview Device→New Device.



11.3.6.3 Managing Role-based Application Sets

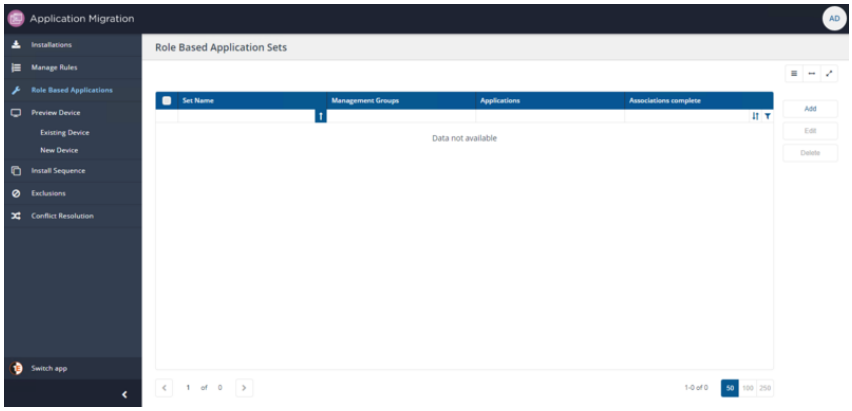
You can add, edit and delete Role-based Applications Sets from the **Role Based Application Sets** page.

11.3.6.3.1 Adding a Role-based Application Set

The process for creating a new Role-based Application Set is:

Create and save the application set.

Associate the applications to this particular application set.



To create a new Role-based Application Set:

Choose **Role Based Applications** from the navigation menu.

Click **Add**.

Under**New Role Based Application Set**:

In**Name**, enter a name for this particular set.

In**Management Group**, start typing the name of the management group you want the set associated with – a list matching your string is dynamically generated for you to choose from.

If there are more management groups you want to associate with this particular set, repeat step b.

Click **Save**.

In the Applications section, click **Add**.

On the **Add Application** screen:

Populate the **Vendor**, **Title**, **Version** and **Edition** fields. As you start typing in the **Vendor** and **Title** fields, a list matching your string is dynamically generated for you to choose from. In our example, we are adding Adobe Acrobat to the application set we just created.

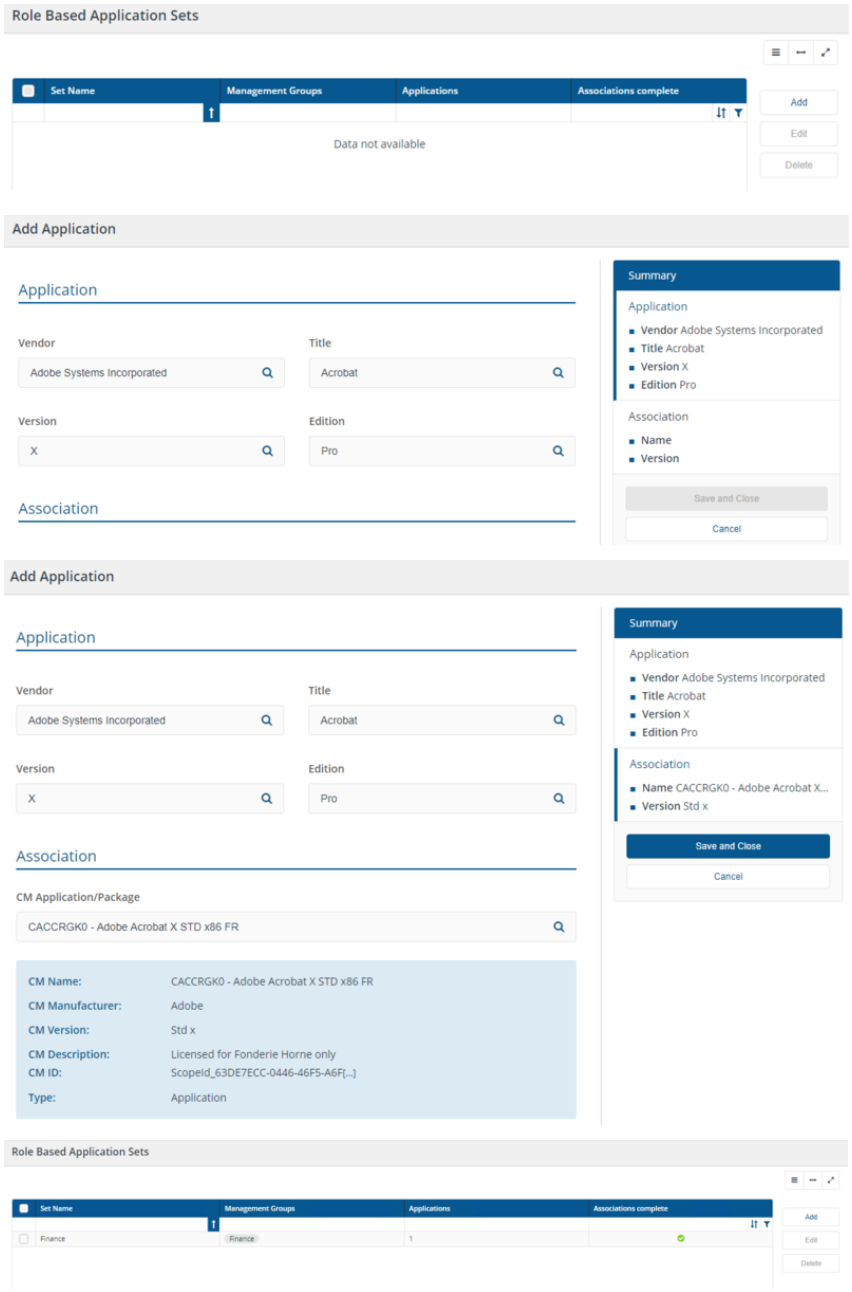
With the **Vendor** and **Title** fields populated, click the **Version** and **Edition** fields respectively for a list to choose from.

In **Association**, click **CM Application/Package**.

In the **CM Application/Package** field, select the application you want from the list.

Click **Save and Close.**

Click **Role Based Applications** in the left-hand menu to view the **Role Based Application Set**.



11.3.6.3.2 Editing an existing Role-based Application Set

To edit an existing Role-based Application Set:

From the **Application Migration** menu, choose **Role Based Applications**.

On the **Summary** screen, locate the set you want from the list, select it and click **Edit**.

On the **Edit set** screen, choose the attributes you want to modify.

To modify the attributes for the application set if you want to:

Update the existing **Name**, place your cursor in the filed and update it

Add a new management group, start typing the name of the management group in **Management Group** – a list matching your string is dynamically generated for you to choose from

Remove an existing management group, click the delete icon next to a management group

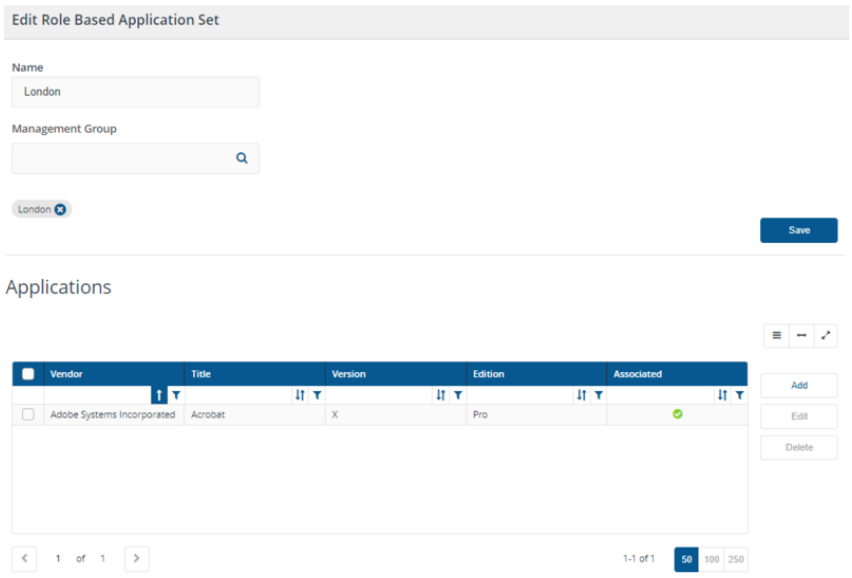
Click **Save** when you have finished.

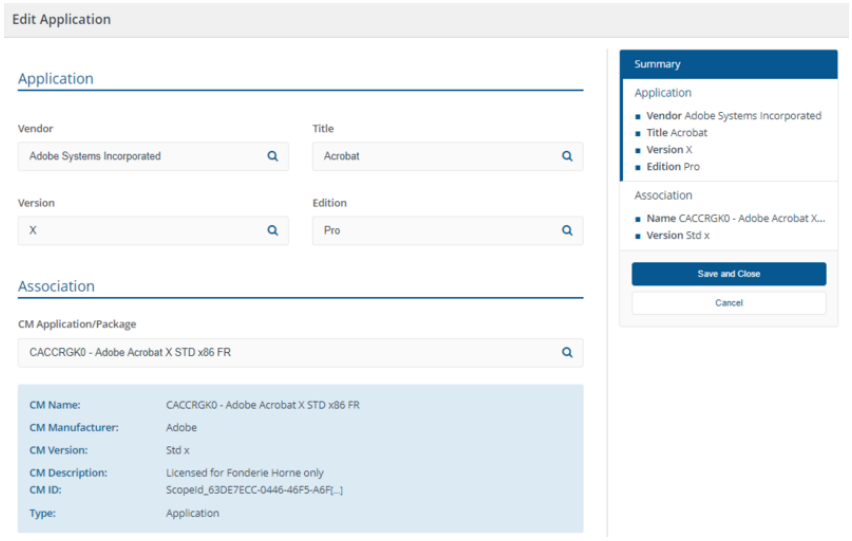
In the Applications section, modify the attributes for the associated applications:

Locate the application you want from the list, select it and click **Edit**

On the **Edit Application** screen, update the details

Click **Save and Close**.





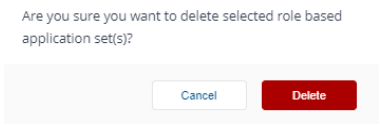
11.3.6.3.3 Deleting an existing application set

To delete an existing application set:

From the **Application Migration** menu, choose **Role Based Applications**.

Locate the set you want from the list, click **Delete**.

Confirm your actions.



11.3.7 Setting the Install Sequence for applications

In some cases, when some applications are installed together, they need to be installed in a certain order. You can do this in Application Migration by adding applications that have specific installation order constraints to the Install Sequence.

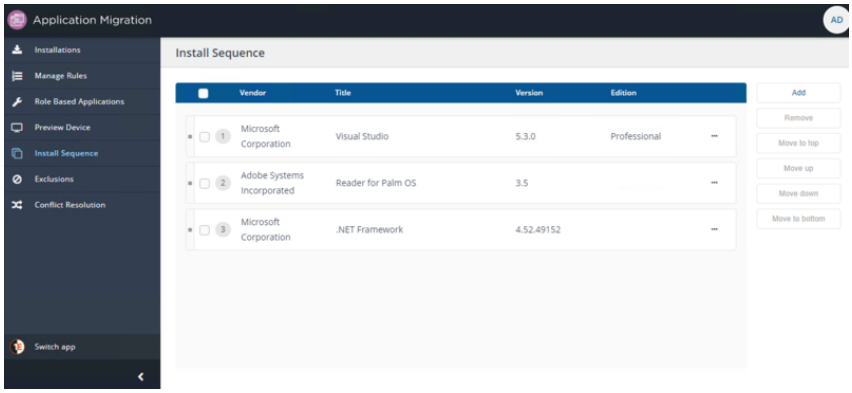
11.3.7.1 Introduction

In previous versions of Application Migration, the order in which applications were installed was not set. In some cases, if certain applications are installed together, they must be installed in a particular order or sequence. This requirement may also apply when multiple versions of the same application are to be installed side-by-side.

In the case where migration rules or role-based applications result in multiple versions of the same application to be installed, Application Migration will automatically install these in order of ascending version. In the case where certain different applications need to be installed in a certain order, users can now define a sequence in which applications should be installed.

For example, a new computer needs setting up with Visual Studio and .Net Framework. In previous versions of Application Migration, if it attempted to install Visual Studio before .Net Framework, the installation would fail.

On the **Install Sequence** page, users can now define that .Net Framework should be installed before Visual Studio.



Note

Install sequence is different from application dependency:

Install sequence - means that *if* applicable migration rules or role-based application sets result in these identified applications being installed together, they will be installed in the defined order or sequence

Application dependency - means that *every time* a certain application is installed, one or more other applications must be installed first. Application dependencies must be defined on the Application or Program in Configuration Manager, independent of Application Migration.

11.3.7.2 Using the Install Sequence page

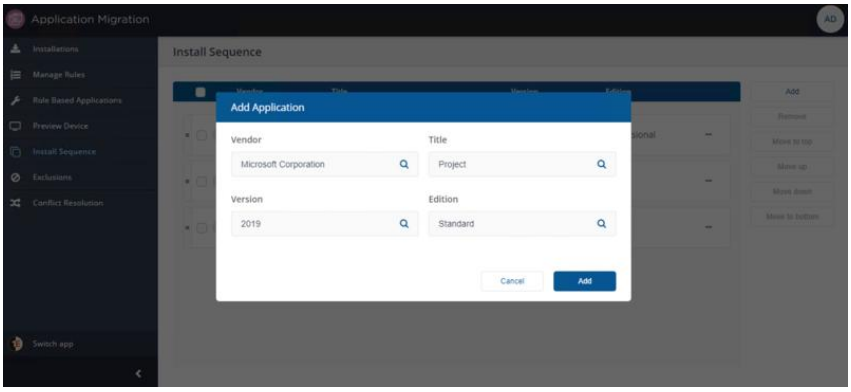
Users can add, remove or reorder applications on the Install Sequence page.

11.3.7.2.1 Adding an application

To add an application:

Click on the **Add** button to open the **Add Application** popup.

On the **Add Application** popup, fill the Vendor, Title, Version and Edition fields then click **Add** to save.



Note

When adding an application for installation sequencing, be sure to define the Vendor, Title, Version and Edition exactly as defined in the migration rule or role-based application set that will install the application. For example, if you add 7-Zip v9.20.0.0 but have a migration rule that will install v9.20 (readable version), the sequencing will not apply to that migration rule and 7-Zip would be installed after all specifically sequenced applications.

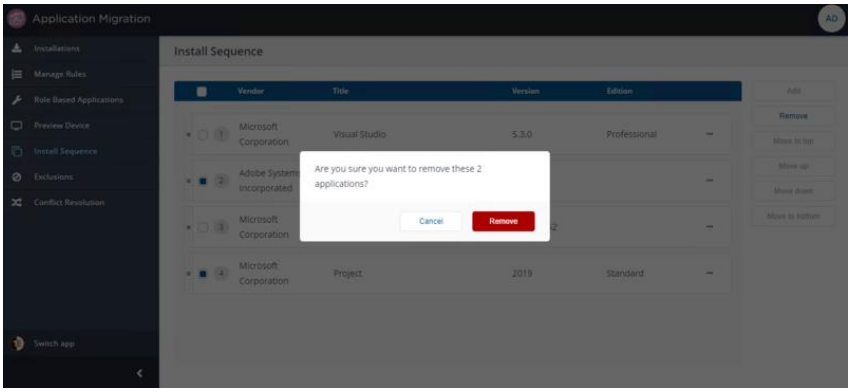
The application is added to the end of the sequence.

11.3.7.2.2 Removing an application

To remove one or more applications:

Select the applications.

Click **Remove**, a popup to confirm the removal will appear.



Click **Remove** to remove the selected applications.

11.3.7.2.3 Move an application to the top

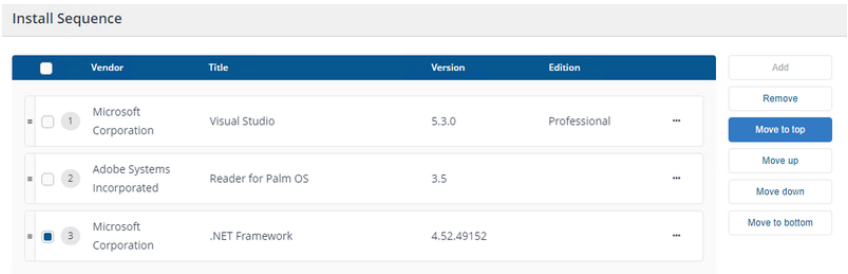
To move an application to the top:

Select the application, for example .NET Framework.

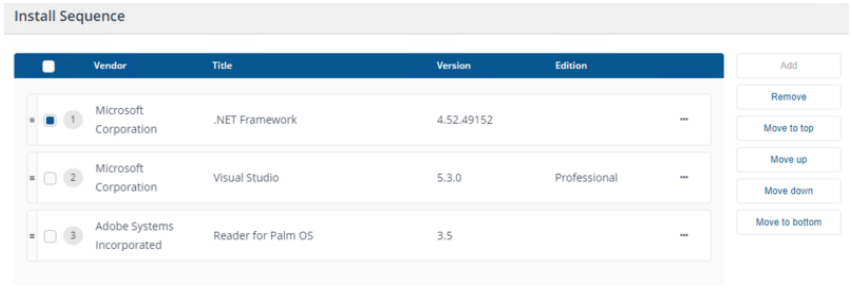
Click the **Move to top** button.

The application will be moved to the top of the sequence.

Before moving the application:



After moving the application:



11.3.7.2.4 Move an application to the bottom

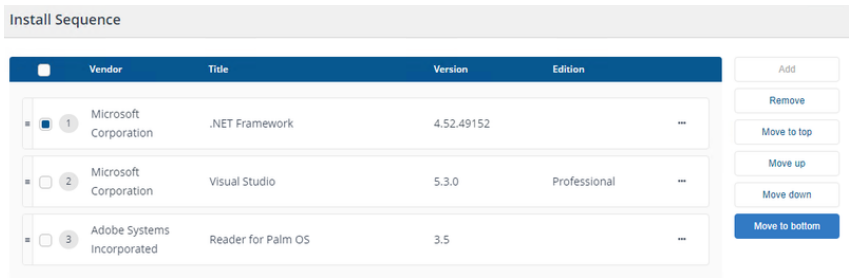
To move an application to the bottom:

Select the application, for example .NET Framework.

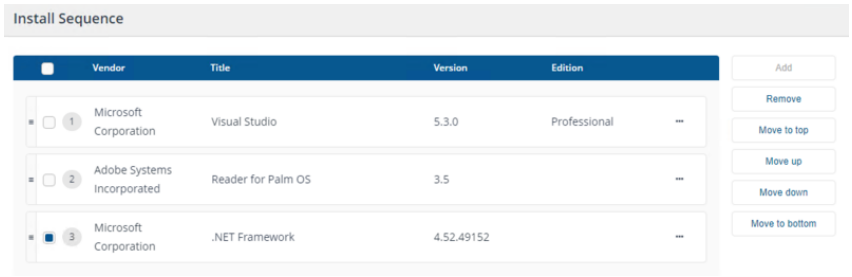
Click the **Move to bottom** button.

The application will be moved to the bottom of the sequence.

Before moving the application:



After moving the application:



11.3.7.2.5 Move an application up one spot

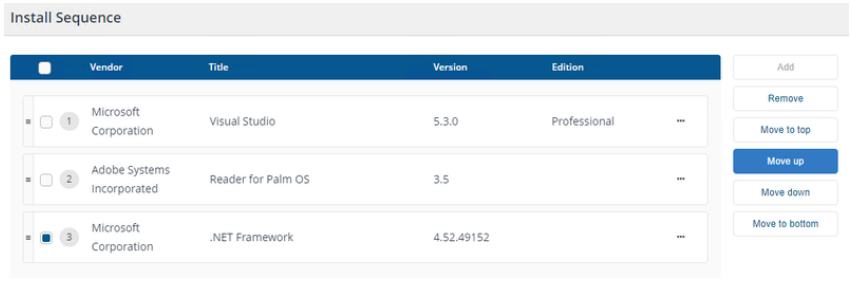
To move an application up one spot:

Select the application, for example .NET Framework.

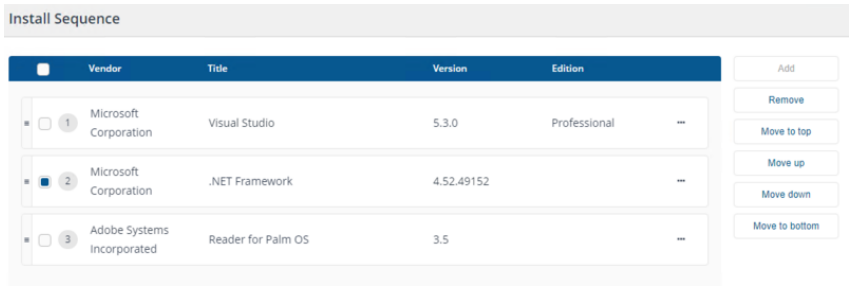
Click the **Move up** button.

The application will be moved one spot up in the sequence.

Before moving the application:



After moving the application:



11.3.7.2.6 Move an application down one spot

To move an application down one spot:

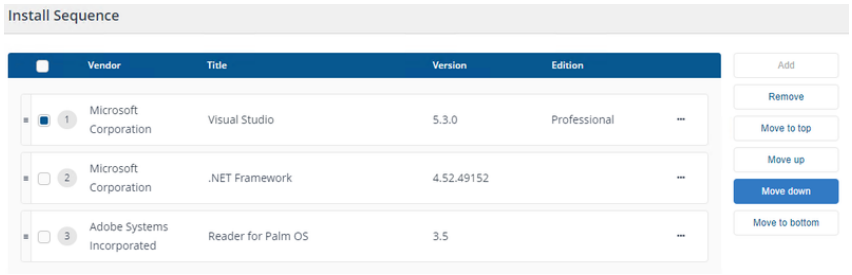
Select the application, for example Visual Studio.

Click the **Move down** button.

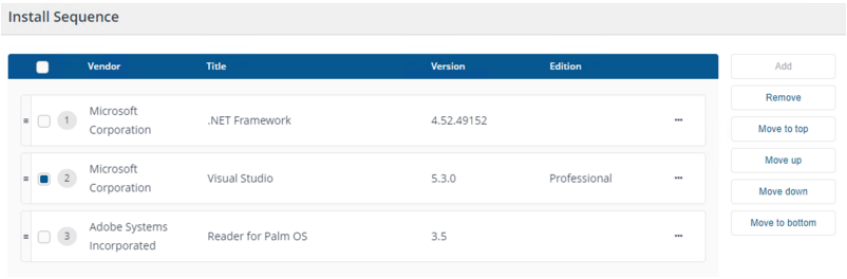
The application will be moved one spot down in the sequence.

> **Note**
>
> Users can only move one application at a time. Selecting multiple applications will disable the movement buttons.

Before moving the application:



After moving the application:

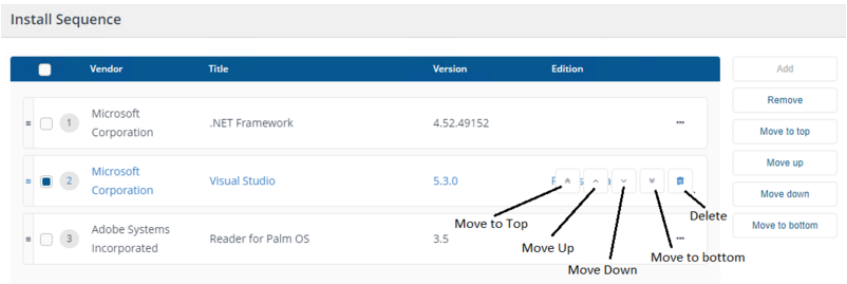


11.3.7.2.7 Move an application directly to the desired spot

A user can also move an application to the desired spot by simply dragging the application.

11.3.7.2.8 Alternate controls for operations

All the above operations (excluding the add operation) have shortcuts on each application row. These controls are visible by hovering over the ellipses.



11.3.7.3 Application Ordering

When the Application Migration step is executed in a Configuration Manager Task Sequence, applications will be sorted according to the following algorithm:

Applications added in the Install Sequence page are sorted in the ascending order of the install sequence.

Remaining applications are sorted as follows:

If any application (defined by Vendor, Title and Edition) has multiple versions to be installed and the migration rule or application set defines a full or readable version, these applications will be installed in ascending version order.

Applications with colloquial versions are not sorted at all but appear after applications with full or readable versions.

> **Note**
>
> To order versions in ascending order, Application Migration attempts to convert the version number defined in the target of the migration rule or role-based application set into a 10-part version number. For a version to successfully convert into a 10-part version, it should be separated by dots and each part should be a non-negative integer. There should be a minimum of 2 and a maximum of 10 parts separated by dots.

For example, if we have the following applications which are to be installed on a machine:

Vendor	Title	Version	Version Type	Edition
Microsoft Corporation	Visual Studio	2013	Colloquial	Professional
Microsoft Corporation	Visual Studio	2010	Colloquial	Professional
Microsoft Corporation	Visual Studio	2015	Colloquial	Professional
Microsoft Corporation	Visual Studio	2017	Colloquial	Professional
Microsoft Corporation	Visual Studio	1.12.47.803	Full	Professional
Microsoft Corporation	Visual Studio	1.11	Readable	Professional
Microsoft Corporation	Visual Studio	a.b.c.d	Full	Professional

and we have the following applications defined in the Install Sequence:

Install Sequence	Vendor	Title	Version	Edition
1	Microsoft Corporation	Visual Studio	2010	Professional
2	Microsoft Corporation	Visual Studio	2013	Professional

The the final order of applications will be:

Vendor	Title	Version	Edition	Comment
Microsoft Corporation	Visual Studio	2010	Professional	Defined in the Install Sequence page
Microsoft Corporation	Visual Studio	2013	Professional	Defined in the Install Sequence page
Microsoft Corporation	Visual Studio	1.11	Professional	1.11 converted to 10-part version is 1.11.0.0.0.0.0.0.0.0, which comes before the 10-part version 1.12.47.803.0.0.0.0.0.0
Microsoft Corporation	Visual Studio	1.12.47.803	Professional	1.12.47.803 converted to 10-part version is 1.12.47.803.0.0.0.0.0.0, which comes

Vendor	Title	Version	Edition	Comment
				after the 10-part version 1.11.0.0.0.0.0.0.0
Microsoft Corporation	Visual Studio	2015	Professional	Colloquial versions are not sorted
Microsoft Corporation	Visual Studio	2017	Professional	Colloquial versions are not sorted
Microsoft Corporation	Visual Studio	a.b.c.d	Professional	Considered as a colloquial version as a.b.c.d cannot be converted into a 10-part version

Note

If the applications defined in the Install Sequence use a combination of Configuration Manager Applications and Package/Programs, the installations may not follow the expected order. This is because in a Task Sequence, all Configuration Manager Applications are installed in one step and all Packages are installed in a different step.

For example, if in the above example, Visual Studio 2010 was installed using a Package/Program and Visual Studio 2013 was installed using an Application, then if the Install Package step in the Task Sequence was positioned after the Install Applications, Visual Studio 2013 would be installed first (with the Install Application step) followed by Visual Studio 2010 (with the Install Package step).

11.3.8 Using Application Migration in a task sequence

The actual process of migrating applications is performed during an OS deployment task sequence in Configuration Manager.

Application Migration uses a custom task sequence action that calls an Application Migration API. The API gets a list of Configuration Manager Applications and Packages that need to be installed on a computer based on previously installed software titles (determined through inventory) and the migration rules applying to those titles.

Task Sequence Tools Upgrade

When upgrading task sequence tools, you must remove the old **1E Application Migration** step and add the same step again in affected Task Sequences. Otherwise, the latest changes will not be accessible and may not work.

11.3.8.1 Testing the API and getting device details

You can test the API and observe the results for a specific computer from a browser with the following by replacing **<WebServiceBaseURL >**, **<Domain>**, and **<MachineName>** with the necessary details:

```
<WebServiceBaseURL>/platform/api/applicationmigration/getApplicationsToBeInstalled/?domainName=<Domain>&machineName=<MachineName>
```

where:

<WebServiceBaseURL> may be either of the host headers configured for Tachyon platform. See Web Service Base URL below for a more detailed description.

<domain> and **<MachineName>** specify the computer you are checking the results for.

Browsing to the URL returns a JSON file with a list of Applications and Packages that will be installed on the specified device when the task sequence executes.

This list is used to populate two series of task sequence variables (one for Applications and the other for Packages) that can be used by the standard Configuration Manager Install Application and Install Package steps to dynamically install each application and package returned by the API.

11.3.8.2 Modern Authentication support for TS Tools 2.6

Important

This feature is only available in 1E platform v9.1.

In 1E platform v9.1, the Authentication Proxy has been deprecated. In previous platform versions, the Authentication Proxy invoked the Application Migration TS API. From 1E 9.1, the Background Channel Proxy is employed to access the TS API by using the client computer certificate.

Upgrading earlier versions of the 1E Toolkit

Note

The 1E Toolkit v9.1 has been modified to remove its dependency on 1E Authentication Proxy and no longer supports it. As a result, if you are using a version of 1E Toolkit dependent on Authentication Proxy, you will not be able to upgrade to v9.1. You will need to uninstall your installed version of 1E Toolkit and install 1E Toolkit v9.1 where you can point to the 1E Platform URL instead of Authentication proxy URL.

Installed Version	Requires Authentication Proxy	Upgrade to 9.1
v8.1	No	Yes
v9.0	Yes	Reinstall

Configuring Background Channel Proxy

To call the TS API from 1E TS Tools, you must configure the Background Channel service web.config. You can do this by either, adding the entry manually or by using our PowerShell script.

Editing the web.config manually

In the manual web.config update, you should replace *your-host* in the *targetURL* with the value for your environment.

```
<ProxiedServers>
<Targets>

..
<add name="ApplicationMigrationTaskSequence" enabled="true" targetURL="https://
your-host/platform/api/applicationmigration/getApplicationsToBeInstalled" timeo
utSeconds="15" clientCertificateForTarget="" useWindowsAuthenticationForTarget=
"false" useServerTokenAuthenticationForTarget="true" deviceAuthentication="Cert
ificate" forwardCertificateFromDevice="false" loggingLevel="off" />
..

</Targets>

</ProxiedServers>
```

Editing the web.config using PowerShell

Run the script using PowerShell, and provide the SLAPlatform base url: *. \AddReclaimerBGProxy.ps1 https://{host}/Platform*

```
param(
    [Parameter(Mandatory = $true, HelpMessage = "Enter SLA platform base URL e.
g. : tachyon.testlab.com/platform or https://tachyon.testlab.com/platform")]
    [ValidateNotNullOrEmpty()]
    [string] $SLAPlatformBaseURL,

    [Parameter(Mandatory = $false, HelpMessage = "Path to web.config of the bac
kground channel web.config")]
    #[ValidateNotNullOrEmpty()]
    [string] $FilePath = "C:\Program Files\1E\Tachyon\Background\Web.config",

    [Parameter(Mandatory = $false, HelpMessage = "Enter the key Name to be used
in the Web.Config")]
    #[ValidateNotNullOrEmpty()]
    [string] $BGPKeyName = "ApplicationMigrationTaskSequence"
)

# load the XML from the web.config
$xml = New-Object XML
$xml = [xml](Get-Content $FilePath)

Write-Host "Using SLA platform base URL :"$SLAPlatformBaseURL
Write-Host "Using FilePath BG Web.config :"$FilePath
Write-Host "Using BGP Key Name:"$BGPKeyName

if (![System.IO.File]::Exists($FilePath)) {
    Write-Error "File doesnot exists with path $FilePath"
```

```
    return;
}

if ($xml.SelectNodes("//configuration/ProxiedServers").Count -eq 0) {
    Write-Host "Proxied Servers doesnot exists.";
    Write-Host "Adding Proxied Servers in Configuration";
    $proxiedServers = $xml.CreateElement("ProxiedServers")
    $proxiedServers.AppendChild($xml.CreateElement("Targets"))
    $xml.configuration.AppendChild($proxiedServers);
}
$SLAPlatformBaseURL=$SLAPlatformBaseURL.TrimEnd('/')
$nodes = $xml.SelectNodes("//configuration/ProxiedServers/Targets/add[@name='$B
GPKeyName']")
if ($nodes.count -eq 0) {
    #<add name="ApplicationMigration" enabled="true" targetURL="https://stalyon
.ntl.local:443/platform/api/applicationmigration/getApplicationsToBeInstalled"
timeoutSeconds="15"
    #clientCertificateForTarget="" useWindowsAuthenticationForTarget="false" us
eServerTokenAuthenticationForTarget="true"
    #deviceAuthentication="Certificate" forwardCertificateFromDevice="false" lo
ggingLevel="off" />
    Write-Host "Adding $BGPKeyName to ProxiedServers Targets."
    $setting = $xml.CreateElement('add')
    $setting.SetAttribute('name', $BGPKeyName)
    $setting.SetAttribute('enabled', 'true')
    $setting.SetAttribute('targetURL', $SLAPlatformBaseURL + '/api/applicationm
igration/getApplicationsToBeInstalled')
    $setting.SetAttribute('timeoutSeconds', '15')
    $setting.SetAttribute('clientCertificateForTarget', '')
    $setting.SetAttribute('useWindowsAuthenticationForTarget', 'false')
    $setting.SetAttribute('useServerTokenAuthenticationForTarget', 'true')
    $setting.SetAttribute('deviceAuthentication', 'Certificate')
    $setting.SetAttribute('forwardCertificateFromDevice', 'false')
    $setting.SetAttribute('loggingLevel', 'off')

    $xml.SelectNodes("//configuration/ProxiedServers/Targets")[0].AppendChild($
setting)
}
else {
    Write-Host "Updating the  $BGPKeyName in ProxiedServers Targets. "
    $setting = $nodes[0];
    $setting.SetAttribute('enabled', 'true')
    $setting.SetAttribute('targetURL', $SLAPlatformBaseURL + '/api/applicationm
igration/getApplicationsToBeInstalled')
    $setting.SetAttribute('timeoutSeconds', '15')
    $setting.SetAttribute('clientCertificateForTarget', '')
    $setting.SetAttribute('useWindowsAuthenticationForTarget', 'false')
    $setting.SetAttribute('useServerTokenAuthenticationForTarget', 'true')
    $setting.SetAttribute('deviceAuthentication', 'Certificate')
    $setting.SetAttribute('forwardCertificateFromDevice', 'false')
```

```
    $setting.SetAttribute('loggingLevel', 'off')
}
Write-Host "Saving to file inprogress.";
$xml.Save($FilePath)

Write-Host "Successfully updated the Web.config of Background channel for Proxy
."
```

Recreate your Application Migration Task Sequence step

To enable Modern Authentication, review your previous task sequences that used the Application Migration Task Sequence step; otherwise, they will not function correctly.

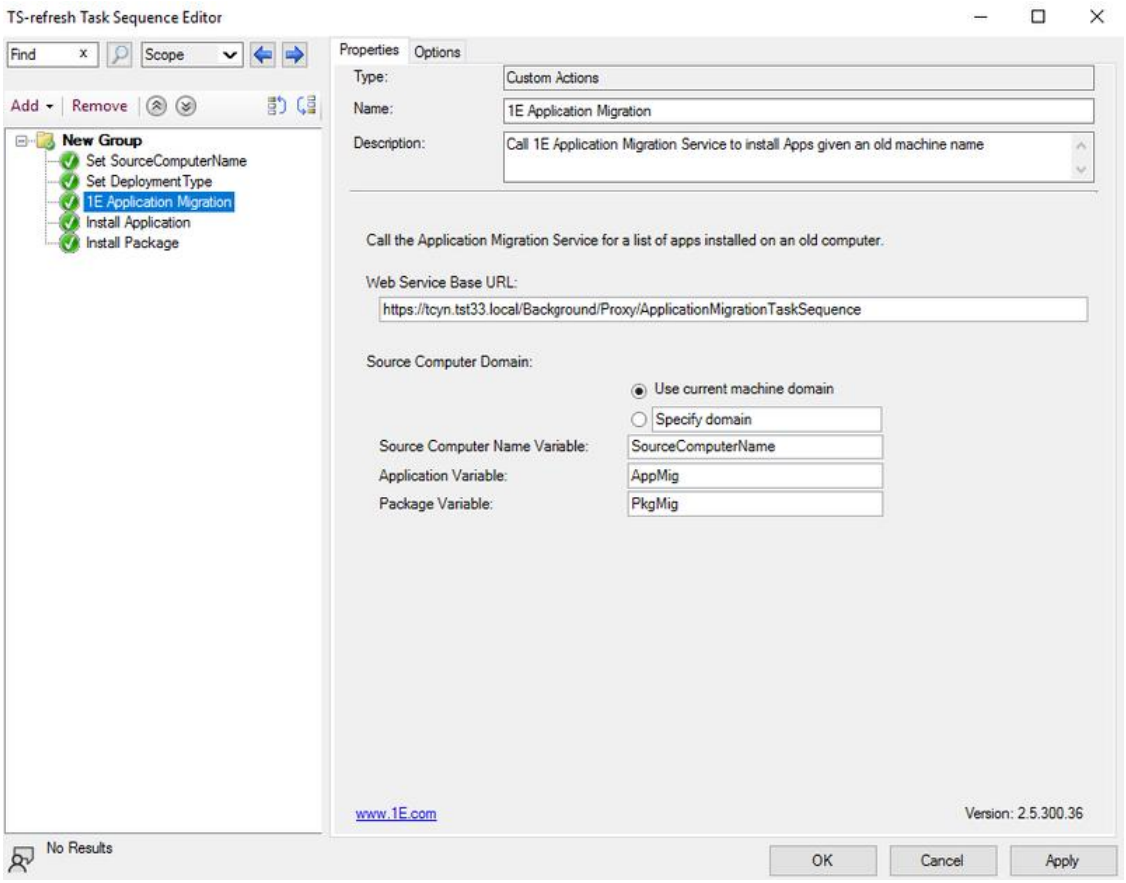
> **Note**
>
> You must have already applied the Application migration 9.1 hotfix, and configured the background channel proxy before following the guidance in this section.

Install Task Sequence Tool version 2.6.

Add a new Application Migration Task Sequence step immediately after your existing Application Migration Task Sequence step.

Transfer the values from the old step to populate your newly added Application Migration Task Sequence step. Ensure the **Web Service Base URL** value is
`https://{host}/Background/Proxy/ApplicationMigrationTaskSequence`

> **Important**
>
> Please note that if the name attribute value **ApplicationMigrationTaskSequence** is included in the background channel web configuration for the task sequence, the URL should remain unchanged as shown above. Otherwise, you should adjust the name according to the value specified in the web configuration.

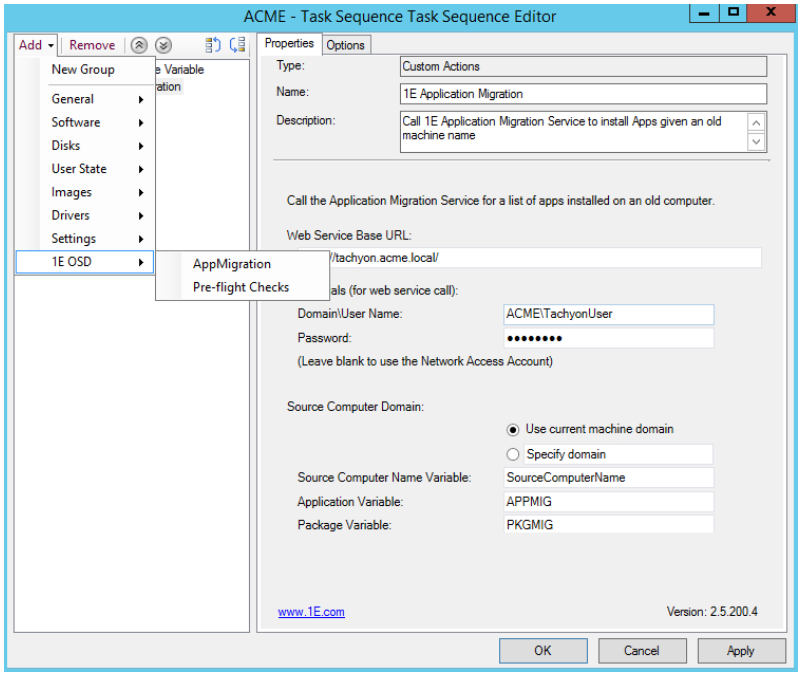


Remove the old Application Migration Task Sequence step.

Validate your updated Task Sequence by running it on a test computer.

11.3.8.3 Configuring the Application Migration Task Sequence step

The **AppMigration** action is used to create the **1E Application Migration** Task Sequence step, and has the following properties.



Web Service Base URL

Note

1E 9.1 users refer to Modern Authentication support for TS Tools 2.6 for changes to this section.

You can connect either using HTTP or HTTPS. In either case, the URL will be based on the settings made on the **Website Configuration** screen of the Tachyon setup program. Refer to Website configuration.

For example, if your platform server FQDN is **ACME-TCN01.ACME.LOCAL** and your platform DNS alias is **TACHYON.ACME.LOCAL**, and these have been configured as the host headers on the **Website Configuration** screen of the platform setup program, then you can use either of the following:

http://ACME-TCN01.ACME.LOCAL

https://TACHYON.ACME.LOCAL

If you have specified a custom port on the **Website Configuration** screen of the platform setup program, then this should also be added to the URLs:

http://ACME-TCN01.ACME.LOCAL:8080

https://TACHYON.ACME.LOCAL:8443

Credentials (for Web service call)

The username and password used to call the Application Migration API. This account must already exist as user on Tachyon platform.

If the **Domain\User Name** and **Password** are left empty, the Configuration Manager Network Access Account is used to fetch data from Application Migration (to use this option the Network Access Account must be added as a platform user).

Source Computer Domain

In most cases, the **Source Computer Domain** will be the same domain that the OS is being deployed in. If you are migrating computers from one domain to another through the OS deployment process, you must select the **Specify Domain** option and enter the Fully Qualified Domain Name of the originating domain, as this will be the domain that the computer belongs to in the platform from previous inventory.

Source Computer Name Variable

The name of the task sequence variable that is used to store the source computer name (the computer from which applications are being migrated).

> **Note**
>
> By default, the **Source Computer Name Variable** property is set to **SourceComputerName**. If the specified variable does not exist, the Application Migration step uses the current computer name as the source computer name.
>
> If you are using Nomad (included in Windows Servicing Suite) and have included the Get migration settings step in the task sequence, that step will set the **SourceComputerName** variable as follows:

In a **Computer Replace** scenario:

When the restore Task Sequence executes on the new computer, **Get Migration Settings** sets the **SourceComputerName** variable to the source computer defined in the **Computer Association** in Configuration Manager.

If the Task Sequence is initiated through the **Windows Servicing Assistant**, you do not need to create a **Computer Association**. **Get Migration Settings** sets the **SourceComputerName** variable to the name of

	the source computer selected by the user in the Windows Servicing Assistant. In a **Computer Refresh** scenario, the **SourceComputerName** variable is set to the current computer name. If you are adding the Application Migration step to an **In-place Upgrade** Task Sequence, set the **Source Computer Name Variable** to **_SMSTSMachineName** and do not use **Get Migration Settings**.
Application Variable	The base variable name which this task sequence step uses to define the Configuration Manager Applications to be installed. This is used to define the base variable in a later **Install Application** step that is configured to install applications according to a dynamic variable list. For example, if **Application Variable** is set to *APPMIG*, this step will dynamically set variables *APPMIG01*, *APPMIG02* etc. corresponding to the applications to be installed dictated by the application migration rules applied to the specified source computer.
Package Variable	The base variable name which this task sequence step uses to define the Configuration Manager Packages to be installed. This is used to define the base variable in a later **Install Package** step that is configured to install packages according to a dynamic variable list. For example, if **Package Variable** is set to *PKGMIG*, this step will dynamically set variables *PKGMIG001*, *PKGMIG002* etc. corresponding to the packages to be installed dictated by the application migration rules applied to the specified source computer.

11.3.8.4 Example

The following example illustrates how to add the Application Migration step to an existing OS Deployment task sequence. Your own task sequence may differ, but the general positioning of these steps is where Install Application steps would normally be placed (after **Install Updates** and before the **Restore User Files**).

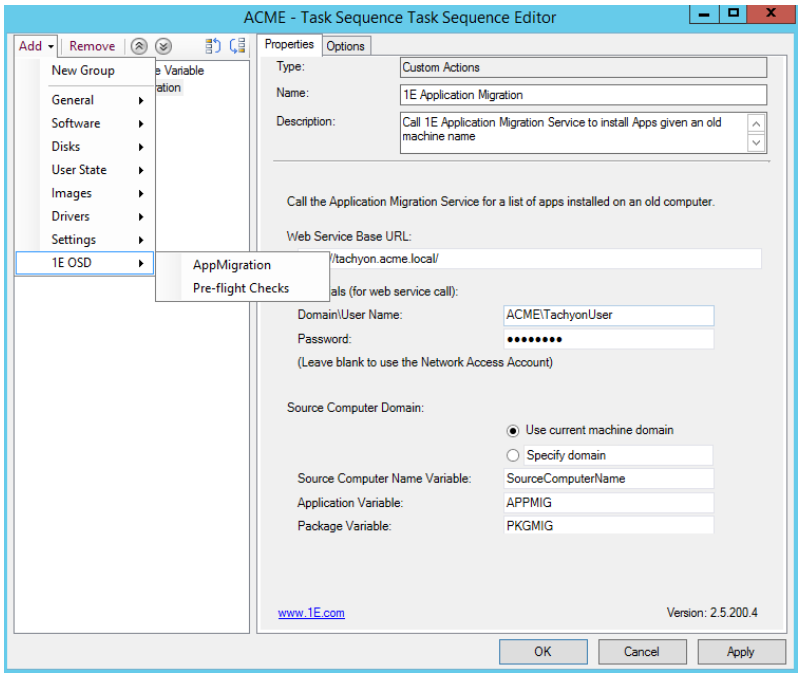
From the **Configuration Manager console**, select the **Software Library workspace**.

Expand the **Operating Systems** folder and select **Task Sequences**.

Right-click the task sequence that Application Migration is to be added to and from the context menu, select **Edit**.

11.3.8.4.1 Application Migration step

Choose **Add > 1E OSD > AppMigration**.



On the **Properties tab**, enter the following details.

> **Note**
>
> 1E 9.1 users refer to Modern Authentication support for TS Tools 2.6 for changes to this section.

In **Web Service Base URL**, enter the location for the platform, for example http://tachyon.acme.local/

Under **Credentials (for Web service call)** enter the **Domain\User Name** and **Password** for the platform user you want to use.

Source Computer Domain in most cases the source computer domain will be the same domain that the OS is being deployed in. If you are migrating computers from one domain to another through the OS deployment process, you must select the Specify Domain option and enter the Fully Qualified Domain Name of the originating domain, as this will be the domain that the computer belongs to in the platform from previous inventory.

In **Source Computer Name Variable** leave the value at its default *SourceComputerName*.

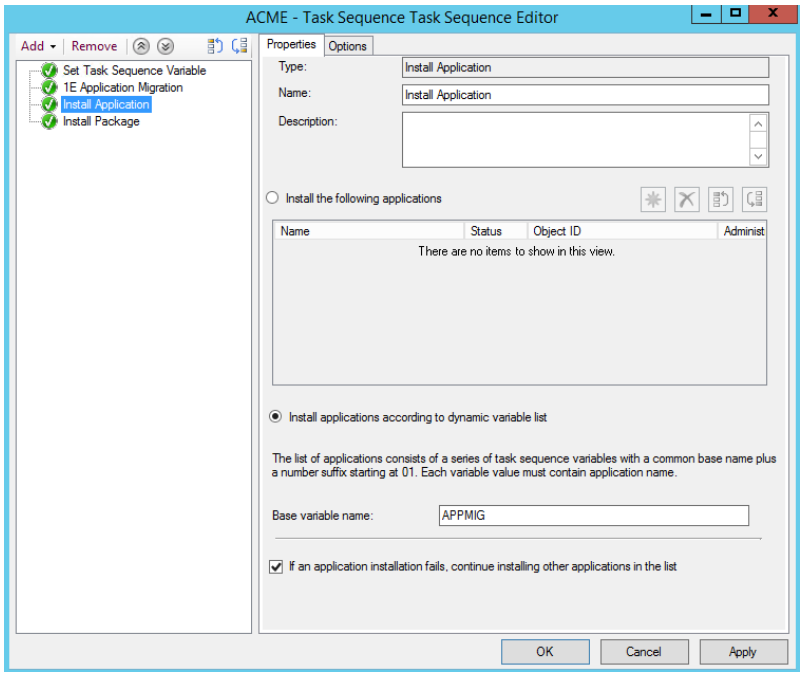
In **Application Variable** choose the base variable that is used to define the dynamic applications. In our example, it is *AppMig*.

In **Package Variable** choose the base variable that is used to define the dynamic packages. In our example, it is *PkgMig*.

Click **Apply**.

11.3.8.4.2 Install Application step

Choose **Add > Software > Install Application**.



On the **Properties tab**:

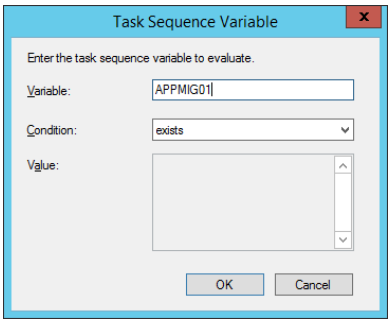
Select the **Install applications according the dynamic variable list** option.

In **Base variable name**, enter the application variable. In our example, it is *AppMig* (see step 5 above).

If you want the task sequence to continue installing other applications in the event if an application install fails, select the **If an application installation fails, continue installing other applications in the list** option.

On the **Options tab**:

Click **Add Condition** and enter condition to check if Task Sequence Variable **APPMIG01** exists (or the application variable you defined in the 1E Application Migration step with **01** appended).



Click **Apply**.

11.3.8.4.3 Install Package step

Choose **Add→Software→Install Package**.

On the **Properties tab**:

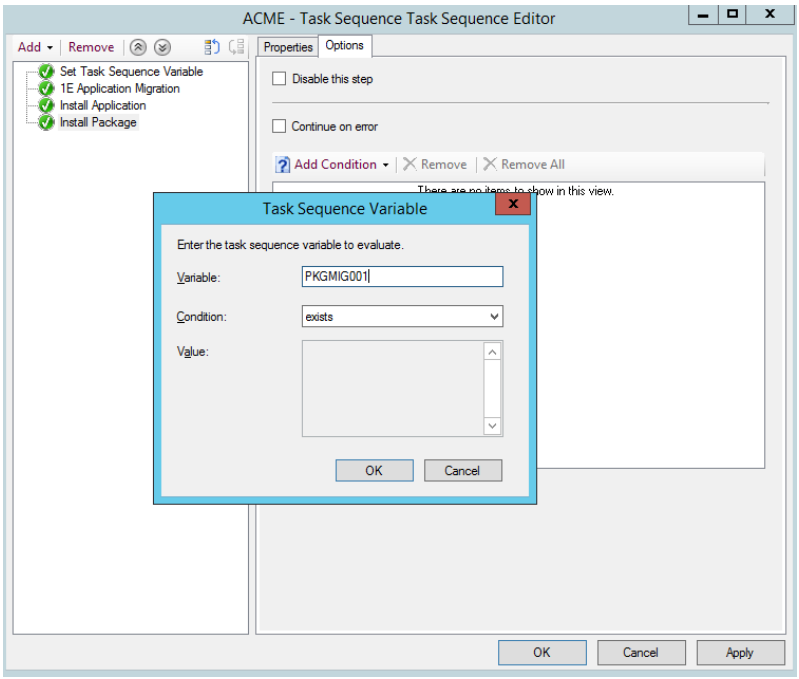
Select the **Install software packages according to dynamic variable list** option.

In **Base variable name**, enter the package variable name used in the 1E Application Migration step. In our example, it is *PkgMig* (see step 6 above).

If you want the task sequence to continue installing other applications in the event if an application install fails, select the **If installation of a software package fails, continue installing other packages in the list** option.

On the **Options tab**:

Click **Add Condition** and enter the condition to check if the task Sequence Variable **PKGMIG001** exists (or the package variable you defined in the 1E Application Migration step and append **001** to it). Click **OK** to save the condition.



Click **Apply** to save the changes to the Task Sequence step.

11.3.8.5 Task sequence variables used by Application Migration

There are five task sequence variables used by Application Migration:

Source Computer Name Variable - the name of the task sequence variable that is used to store the source computer name (the computer from which applications are being migrated), as described above

Application Variable - the base variable name used for Applications, as described above

Package Variable - the base variable name used for Packages, as described above

Role Base Application Sets variable - optional, the variable named **IncludeRoleBasedAppsForExistingPC** must be set to **true** if you are using Role Based Application Sets, described below

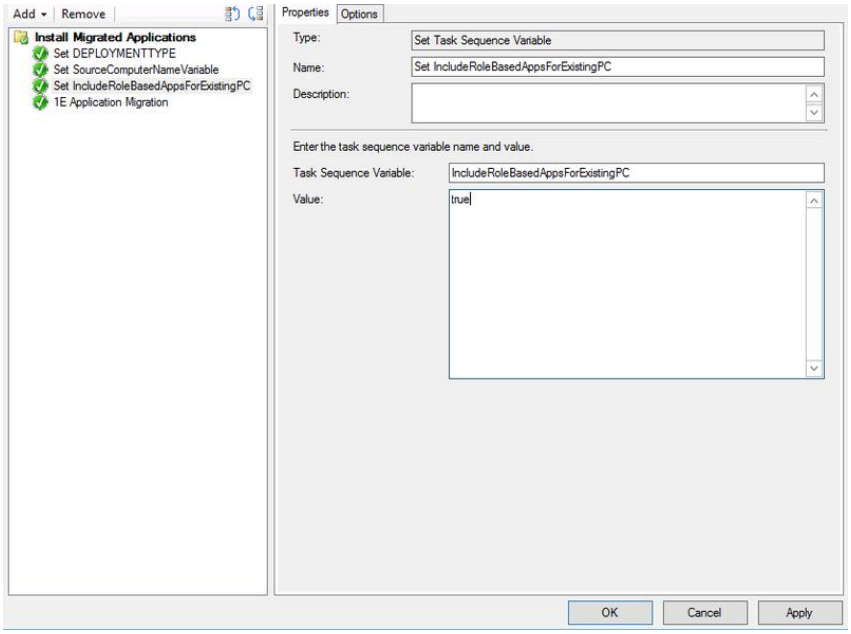
Deployment Type variable - the variable named **DeploymentType** must be set to one of the following values, and must be set prior to the **1E Application Migration** step

Value	Description of DeploymentType variable
Refresh	Also known as Wipe-and-Load, the data on the computer is backed up, the disk is wiped, a new OS is installed and applications are installed subject to their respective migration rules. If no application migration rule exists for an application, it will not be installed.
Replace	Data and applications are migrated from one computer to another. Applications that are migrated to the new computer are subject to the application migration rules for the source computer. If no application rule exists for an application, it will not be installed on the new computer.
InPlace	Windows setup is executed on an existing computer to upgrade the OS. The disk is not wiped, so existing data and installed applications are preserved. In this instance, Application Migration will install only applications that are subject to a replace or upgrade migration rules. Retain rules are ignored.
NewComputer	Also known as bare-metal, this is a new build computer where no applications or data are being migrated. However, you can use the Role Based Application Sets feature to install applications on new computers.

11.3.8.6 Using migration rules and Role Based Application Sets

Role Based Application Sets can optionally be used in each of the deployment scenarios. A Role Based Application Set defines a set of applications that should be installed on a computer for a user performing a particular role, or perhaps working at a particular location.

For this to work, the task sequence must contain the variable **IncludeRoleBasedAppsForExistingPC** set to a value of **true**, as shown.



Note

When using **IncludeRoleBasedAppsForExistingPC** with a value of **true** for role-based application sets, the **DeploymentType** variable must be set appropriately in the task sequence before the **1E Application Migration** step.

11.3.8.7 Auto Install for Configuration Manager Applications and Packages

Application Migration uses the **Install Application** and **Install Package** steps in a Task Sequence to install migrated applications and packages. These Task Sequence steps are dependent on the relevant checkbox (auto install flag) being enabled for *each* application and package:

Allow this application to be installed from the Install Application task sequence action without being deployed.

Allow this program to be installed from the Install Package task sequence action without being deployed.

If a checkbox is not enabled, the software installation will fail for that application or package. An administrator can enable this checkbox for each application and package by using either of the following methods:

in Configuration Manager during or after creating each application and package.

using the **Auto Install** feature in Application Migration when creating application associations, rules or Role Based Application sets.

Note

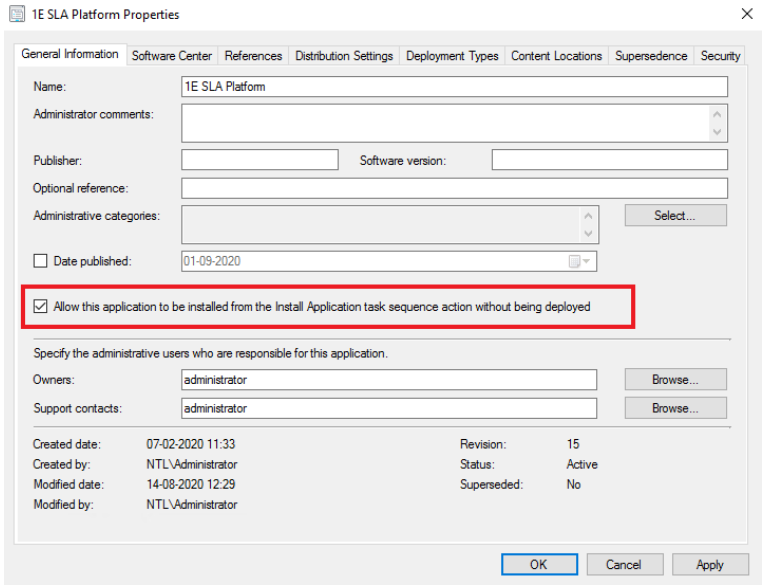
Application Migration's **Auto Install** feature is able to read the checkbox (auto install flag) for applications and programs, but in order for Application Migration to enable them for you, you'll need to configure related providers in the **Settings** module of

Tachyon platform. These should already be configured as a post-installation step. For configuration details, please refer to Post-install configuration.

Refer to Managing migration rules: Auto Install for Migration Rules and Role Based Application Sets: Auto Install for Configuration Manager Applications and Packages.

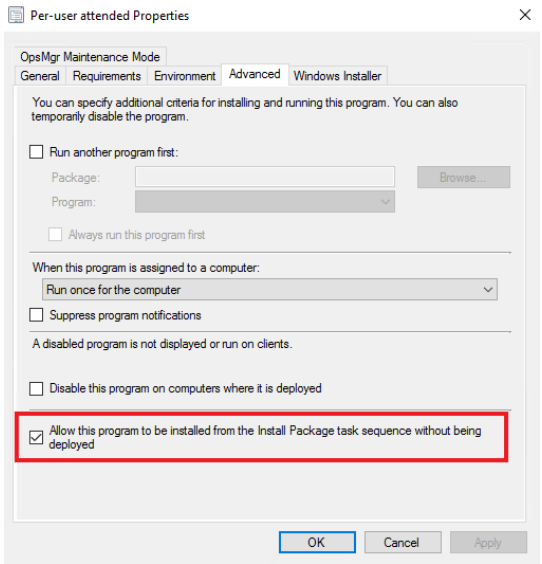
11.3.8.7.1 Applications

The checkbox is located on the **General Information** tab of the **Properties** window for a Configuration Manager Application as shown.



11.3.8.7.2 Packages

The checkbox is also present on the **Advanced** tab of the **Properties** window of a Configuration Manager Package program as shown.



11.3.8.8 Support for Computer Replacement scenario

If you intend to use Application Migration to migrate applications from an old computer to a new computer (**Replace** scenario), you may need to include the Get migration settings step in your Task Sequences. The Get Migration Settings Task Sequence step retrieves information from a Computer Association in Configuration Manager so it can determine the source computer when installing applications on the new computer. It is currently distributed with Nomad and is added to the Task Sequence Editor by installing NomadBranchTools.msi. Please refer to Installing Nomad Branch Tools for more information.

11.4 Troubleshooting

A general methodology for investigating issues as well as identifying key issues and their resolutions.

11.4.1 The technical support process

Read through the Troubleshooting pages to see if there are known issues, or quick resolutions to any problems you may have encountered.

Maintenance support customers can use the 1E Support Web Portal to review knowledge base articles and download hotfixes.

If still encountering problems, create a technical report (log files and details) and then contact the 1E technical support team.

11.4.1.1 Creating a technical report

If possible, please obtain the following details and log files before contacting 1E, to include in your technical report.

11.4.1.1.1 Version details

The OS, version number, and patch level for:

Tachyon Servers

1E Client

Configuration Manager - if used

Other 1E Server software, for example, Shopping, Nightwatchman, and WakeUp.

For Nomad and Shopping, please provide OS, version number, and patch level for:

Configuration Manager DPs

Nomad extensions used on Configuration Manager Consoles

ActiveEfficiency Server.

11.4.1.1.2 Environmental details

If there were any recent changes made to your configuration

The name of the machines, Configuration Manager Application and/or Package IDs for when the issue occurred

11.4.1.1.3 Problem details

When did the issue occur, ensure log files cover this period

The scope of the issue – did it affect a particular geographical location, group of users, or client machines

Details of any self-help troubleshooting steps you carried out

In the event of a service crash or if you are experiencing high CPU or memory usage, provide us with the dump file, event viewer logs, and traces. We will provide you with FTP details to upload these files.

11.4.1.2 Log files

11.4.1.2.1 Tachyon Server log files

For any issue, please provide a zip containing log files from the following locations:

%ALLUSERSPROFILE%\1E\Catalog*.log

%ALLUSERSPROFILE%\1E\ContentDistribution*.log

%ALLUSERSPROFILE%\1E\Platform Consumers*.log

%ALLUSERSPROFILE%\1E\SLA Platform*.log

%ALLUSERSPROFILE%\1E\Tachyon*.log

If you are having licensing issues, please include:

%ALLUSERSPROFILE%\1E\Licensing*

Please refer to the Tachyon Platform 8.1 - Log files page for more details.

11.4.1.2.2 1E Client logs on Windows

%ALLUSERSPROFILE%\1E\Client\1E.Client.log (used by 1E Client and Tachyon features, and Shopping client)

%ALLUSERSPROFILE%\1E\Client\NomadBranchUninstall-YYYY_MM_HHTMM_HH_SS_000Z.log

11.4.1.2.3 Nomad client log

%ALLUSERSPROFILE%\1E\NomadBranch\LogFiles\NomadBranch.log

11.4.1.2.4 WakeUp client log

%ALLUSERSPROFILE%\1E\Agent\WakeUpAgt.log

11.4.1.2.5 Shopping WSA client log

%ALLUSERSPROFILE%\1E\Client\WSA.log

11.4.1.2.6 Task Sequence errors

All the errors which occur in task sequence will be logged into **smsts** log in client machine, where the task sequence is targeted.

11.4.2 Known issues

Lists of the current known issues with implementing, configuring, and using Application Migration.

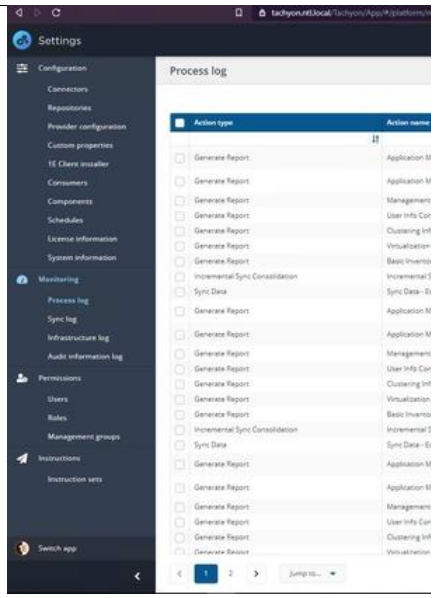
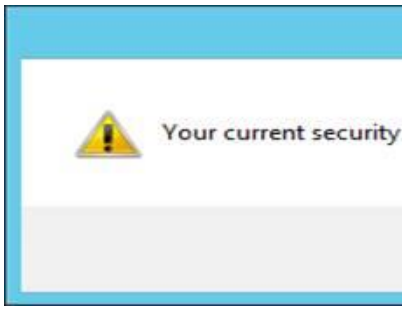
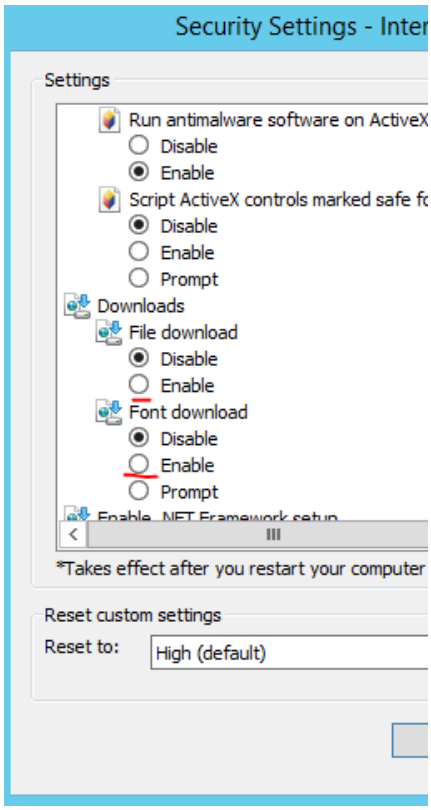
If you need further help, please refer to the Troubleshooting page for how to contact 1E Support and the technical support process.

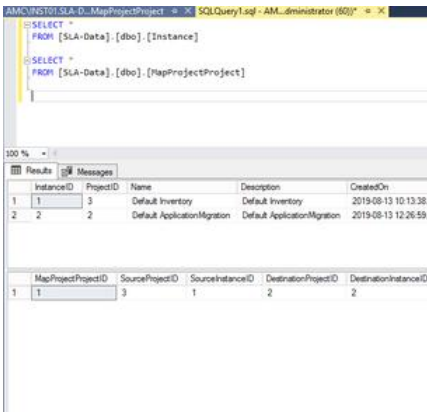
11.4.2.1 Issues with installation and upgrades

Issue	Description	Workaround
Unable to close the Application Migration installer by clicking **Finish** button on final screen.	This happens if any of the checkboxes on the Finish screen have been checked before clicking 'Finish' button.	Either close the opened log files. Or do not check the checkboxes on the Finish screen to open a log file.
After upgrade, user may find some rules might not get applied on preview device screens (Existing/New).	A target product in the migration rule was removed/updated in the database due to de-duplication logic in basic inventory consolidation.	Whichever rule is NOT being applied should be updated to change the value of vendor, title, version or edition value of the product.
Revision number of Application Migration app version shown on the Tachyon Portal landing page might not match with its corresponding Control Panel ARP entry.		To know the correct version of Application Migration please refer to ARP entry only.
Application Migration Administrators role is visible in the list of Tachyon system roles even when Application Migration is not installed.	Role Based Access control (RBAC) related information doesn't get removed from the Tachyon Master databasewhen Application Migration is uninstalled	

11.4.2.2 Issues using Application Migration

Issue	Description	Workaround
Any Tachyon user can see Application Migration in the Switch app menu and open the application even if the Application Migration Administrators role is not assigned to the user.	This is because the user's permissions are tested inside the application. Although a user can start the application they cannot use it unless assigned to the Application Migration Administrators role.	
Version search on Add rule screen times out or is incomplete.	A search may be incomplete if the user clicks anywhere on the screen while a large version list is being populated. Examples of large version lists are Chrome and SQL Server which each have over 9000 entries.	Don't click anywhere on screen while versions are being loaded.
Excluding a product having '--' (two successive hyphens) in Vendor, Title or Edition will not delete the migration rules linked to the product being excluded. For example, suppose you try to exclude 'M*Modal Fluency Direct -- Dermatology Recognizer' from 'MModal IP LLC'. If there are any migration rules linked to this product then their count will not be shown on the warning pop-up. Also, the linked migration rules will not get deleted when exclusion is done.	This is due to an existing bug in SLA Platform related to handling of special characters.	All the migration rules linked to the product being excluded need to be deleted manually from 'Manage Rules' screen.
When viewing the process log under Monitoring menu in the Settings app, the **Status** column doesn't refresh on its own to show	This is a known intermittent issue in the portal.	To refresh the screen you click the refresh icon in top right corner of the screen to view the latest status as shown in below screenshot:

Issue	Description	Workaround
the most recent status of any report being run.		
The export to excel feature from the installations view doesn't work while using Tachyon portal on Internet Explorer 11 and shows the following error message box:  You might also notice that the icons don't get downloaded on Internet Explorer 11.	This is due to default security settings of the browser which are very strict with respect to downloads.	To resolve this error, you need to ensure that following settings are set to **Enable**. 

Issue	Description	Workaround
The Application Migration Consolidation report doesn't run when the Basic Inventory Consolidation report is executed. This can happen when Application Migration repository is not correctly mapped to a valid inventory repository.	This happens when the linking of Inventory repository pointed by Application Migration repository is broken for some reason. The mapping of a healthy association can be seen in MapProjectProject table in the screenshot below: 	It is not possible to fix the linking from the web portal so this need to be fixed directly in the database. We need to ensure that Source IDs (SourceProjectID and SourceInstanceID) representing inventory repository , and Destination IDs(DestinationInstanceID, DestinationProjectID) representing Application Migration repository should match in the MapProjectProject table for the inventory repository for which IsFavorite flag is 1.
When using Application Migration v3.0 on Tachyon v5.1, CM application cannot be mapped to a VTVE while creating a rule or adding an application to role based sets.		Map the VTVE & CM application in inventory screen and it can be used while creating a rule or adding an application.

11.4.2.3 Issues with installing and using Task Sequence Tools

Issue	Description	Workaround
An error message "No HTTP resource was found.." error message is appearing in SMSTS logs when an Application Migration task sequence runs which causes the task sequence to fail.	This is an intermittent issue which is most often caused by issues in the environment.	

Issue	Description	Workaround
The 1E Application Migration step is not saved when added to an existing OSD task sequence and clicking Apply.	When you add the Application Migration step to an existing OS Deployment task sequence and click Apply, the step is not saved and may appear with a red X symbol.	Save the step by clicking OK instead.
Role-Based Applications not installed when IncludeRoleBasedAppsForExistingPC=true but DEPLOYMENTTYPE is not explicitly set	If the DEPLOYMENTTYPE TS variable is not explicitly set, the 1E Application Migration step will set it to Refresh but does not take into account IncludeRoleBasedAppsForExistingPC being true.	Set DEPLOYMENTTYPE variable before 1E Application Migration step.

11.5 Reference

Application Migration 8.1 reference material.

11.5.1 Installer properties

A list of the Windows installer properties for the Application Migration installers.

11.5.1.1 Application Migration

A table of the Windows installer properties for the Application Migration installer.

> **Warning**
>
> Tachyon Setup is the only supported method of installing, upgrading, and patching a Tachyon server.
>
> Installation using standalone **msi** or **msp** files is not supported unless advised by 1E, which may be necessary in complex installations, using non-interactive (quiet/silent) command-lines, and may require further post-install configuration steps.
>
> **Note**
>
> Mandatory properties must be provided when installing using a command-line.

The installer file is: **ApplicationMigration.msi**

Property	Default	Mandatory	Description
PLATFORMBASEURL	n/a	Yes	The URL used to access the Tachyon Portal website. You can connect either using HTTP or HTTPS. In either case, the URL will be based on the settings made on the **Website Configuration** screen of the Tachyon Setup program. Please refer to Website configuration for more details. For example, if your Tachyon server FQDN is **ACME-TCN01.ACME.LOCAL** and your Tachyon DNS alias is **TACHYON.ACME.LOCAL**, and these have been configured as the host headers on the **Website Configuration** screen of the Tachyon Setup program, then either of the following URLs can be used: http://ACME-TCN01.ACME.LOCAL https://TACHYON.ACME.LOCAL If you have specified a custom port on the **Website Configuration** screen of the Tachyon Setup program, then this should also be added to the URLs. For example: http://ACME-TCN01.ACME.LOCAL:8080 https://TACHYON.ACME.LOCAL:8443

Ensure all steps on the Requirements page have been completed before installation.

See Installation for more details about installations.

Ensure all Requirements have been met before installation.

Please refer to Installation: Installing Application Migration for more details about interactive and non-interactive installations.

11.5.1.2 1E Task Sequence tools

The installer file for 1E Task Sequence tools is: **1ETaskSequenceTools.msi**

There are no installer properties.

Install the 1E Task Sequence Tools on the following systems:

The Configuration Manager Primary Site server. In a multi-site hierarchy, install it on the CAS and each primary site.

If any site has one or more remote SMS Providers, install it on each remote SMS Provider server

Any remote Configuration Manager console systems that are used to edit task sequences.

Please refer to Installation: Installing the 1E Task Sequence tools for more details.

11.5.2 1E task sequence actions

In addition to the custom task sequence actions listed on this page, you may see additional custom action depending on the 1E OSD Tools that you have installed:

BIOS TO UEFI 1.4 - 1E OSD task sequence actions

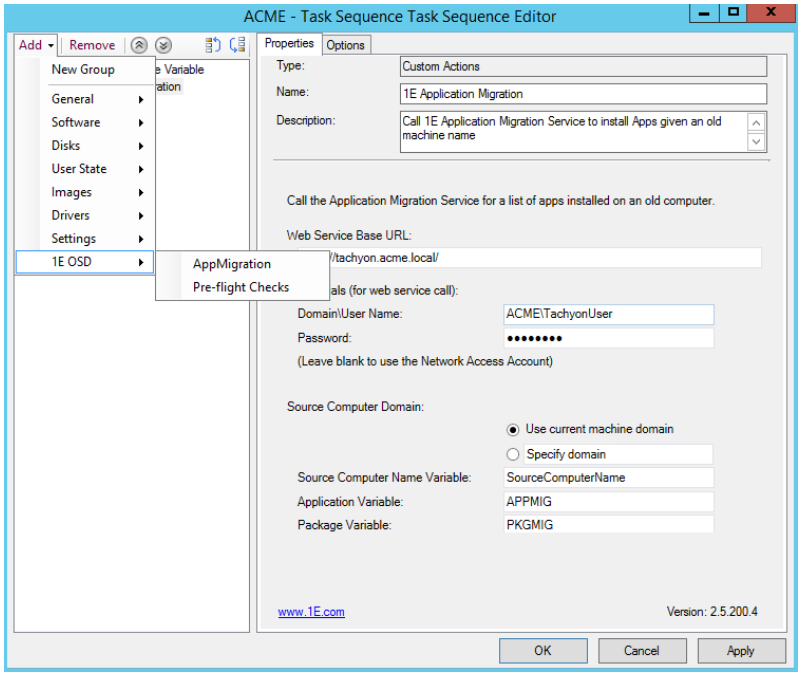
1E OSD task sequence actions

Please click on a heading below for more information about a custom task sequence action and its configuration.

11.5.2.1 AppMigration

11.5.2.1.1 AppMigration Task Sequence action

Application Migration uses a custom task sequence action that calls an Application Migration API. The API gets a list of Configuration Manager Applications and Packages that need to be installed on a computer based on previously installed software titles (determined through inventory) and the migration rules applying to those titles.



For details of how to use this action in a Task Sequence please refer to Using Application Migration in a task sequence.

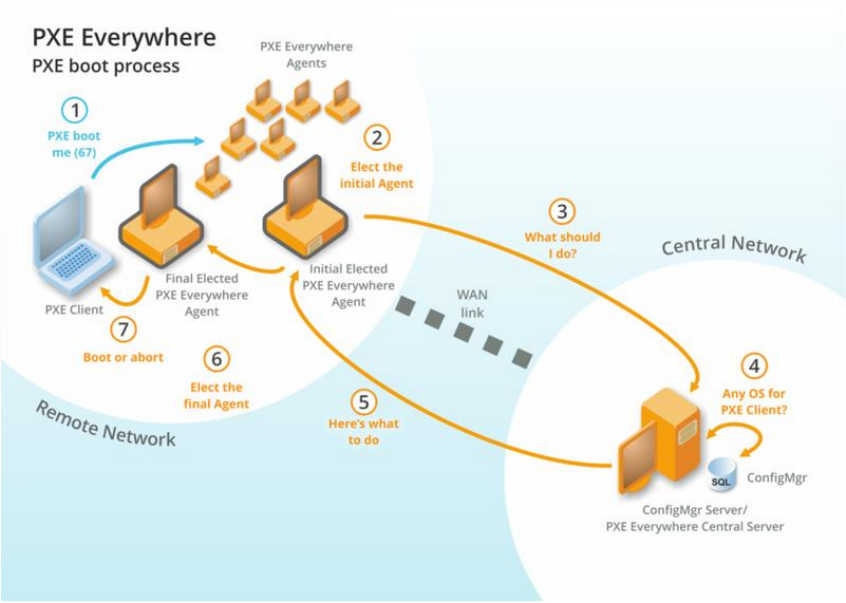
11.5.2.2 Get migration settings

This action is available with 1E Nomad OSD Tools. It provides support for encryption in PBA. Also enables PBA to be used for computer replacement scenarios. This task can be configured to run under either the capture phase or the restore phase. Its behavior differs depending on which phase it's run under.

For full details, refer to Get Migration Settings.

12 PXE Everywhere

PXE Everywhere allows computers to automatically boot up into Windows PE, which then allows a Windows Operating System to be installed.



12.1 Introducing PXE Everywhere

An introduction to the features of PXE Everywhere, what it does, how it can benefit your organization, and a high-level explanation of the PXE Everywhere architecture.

PXE Everywhere allows computers to automatically boot up into Windows PE, which then allows a Windows Operating System to be installed. The following deployment scenarios are supported:

Installing a Windows OS image for the first time (the 'New Computer' scenario, sometimes known as 'bare-metal')

Installing a Windows OS image when the current OS is not bootable (often referred to as 'break-fix')

Installing a Windows OS image when the current OS can be wiped and there is no requirement to retain user data (for example, when preparing a previously used computer for a new user).

Typically this is achieved using either USB media or booting directly from the network using the Pre-Execution Environment (PXE) code built in to the network adapter. Booting from the network requires one or more PXE servers to be implemented that serve the Windows PE boot image to the booting PXE client. Implementing PXE in Configuration Manager requires DPs with the PXE role enabled. To avoid PXE clients downloading the Windows PE boot image (anything upwards of 200MB) over the WAN, DPs need to be located wherever you need to use PXE. It is unlikely that you have Distribution Points in every location, especially if you are using 1E Nomad to eliminate remote Distribution Points. As PXE requests are broadcast on the local subnet, if there is no PXE server on the local subnet you need to configure IP helpers on routers to forward the PXE requests to the PXE server. The PXE client will then try to download the Windows PE boot image from the PXE server over the WAN, which can take hours on slow links and provides no bandwidth management.

PXE Everywhere addresses this issue by implementing a lightweight PXE server (the PXE Everywhere agent) on computers, enabling you to eliminate Configuration Manager PXE servers and instead make every computer (or as many as you want) on the network a potential PXE server. Each subnet therefore has one or more PXE servers available to serve the Windows PE boot image so there is no router configuration required unless DHCP Snooping is enabled, and the Windows PE boot image is not downloaded over the WAN. The boot image can be staged on the PXE Everywhere agent machines using Nomad, which ensures the boot image can be safely transferred to remote subnets ahead of deployments without slowing down other traffic on the network.

When a PXE client boots up, the PXE request is intercepted by each of the PXE Everywhere agents. These agents then elect one agent to check with Configuration Manager to see if there are any OS deployments targeted at the booting PXE client. If so, the PXE Everywhere agents will then hold a second election to determine which PXE Everywhere agent should respond to the booting PXE client. The elected agent sends the response and the booting PXE client downloads the boot image from the elected agent. PXE Everywhere supports booting BIOS and UEFI systems. It integrates with Configuration Manager and works with your existing OS Deployment Task Sequences.

12.1.1 Support for networks with DHCP Snooping enabled

DHCP Snooping is a network security measure implemented in network switches that stops DHCP packets from being forwarded to switch ports that are not authorized. The intention of this security measure is to prevent rogue DHCP servers from issuing IP addresses to devices on the network. A side effect of this measure being enabled is that PXE requests, which are a form of DHCP request, are also blocked. This prevents 1E PXE Everywhere from functioning as expected, as peers are no longer able to receive or respond to PXE requests as their switch ports are not authorized.

With PXE Everywhere 4.0, it is possible to set up one or more 'responders' that are connected to switch ports authorized to receive and respond to DHCP requests. The responder is simply a PXE server that provides the initial boot loader (as this is around 50K in size, it is safe to transfer over the WAN). As PXE clients will not be on the same subnet as the Responder, it is necessary to configure DHCP Relay agents on routers (known as IP helpers in Cisco terminology) to forward DHCP (including PXE) requests from each subnet to the Responder, in addition to any existing DHCP servers that you have configured. The Responder will discard any DHCP packets that are not PXE requests.

When the responder receives a PXE request, it responds with a boot loader that the booting PXE client downloads. The boot loader then broadcasts a new PXE request on a custom UDP port that is not blocked by the DHCP Snooping filter on the switch. The PXE Everywhere agents on the subnet are configured to listen on

the custom port and can therefore continue to function as normal - electing an agent to check for active deployments and respond with an offer of the appropriate boot image - unobstructed by DHCP Snooping.

12.1.2 PXE Everywhere components

PXE Everywhere includes the following components:

PXE Everywhere Central Server. PXE Everywhere Central is a web service that the PXE Everywhere Agents contact to determine if the booting PXE client requires a boot image. It does this by checking the Configuration Manager database to determine if there are any OS Deployment Task Sequences deployed to the booting PXE client (identified by that client's MAC address and SMBIOS GUID). The web service component of the PXE Everywhere Central Service can be installed on any IIS server that has good connectivity to the Configuration Manager Database server (it can be installed on the Configuration Manager site server if IIS is installed). PXE Everywhere Central also includes boot image tools, which can be installed on any system that has the Configuration Manager Console installed. To install, please refer to Installing PXE Everywhere Central.

PXE Everywhere Agent. PXE Everywhere Agent is a client module of the 1E Client (introduced in 1E Client 5.1 for PXE Everywhere v4.0). It is installed on all (or as many as you want) computers. It establishes a lightweight PXE service which listens for PXE boot requests broadcast on the local subnet. By default, the Agent listens on port 67, but will listen instead on port 2067 if the Agent has been configured to run in an environment that has DHCP Snooping enabled. When intercepted the agents will initiate an election and the elected agent will check, via the PXE Everywhere Central server, if there are any OS Deployment Task Sequences deployed to the booting PXE client. If so, the Agents will initiate a second election to determine the best agent to serve the Windows PE boot image to the booting PXE peer. The elected agent then responds to the booting PXE client with an offer of the boot image, which the PXE client then downloads over TFTP and boots into to start the Task Sequence. To install, please refer to Installing PXE Everywhere Agents.

PXE Everywhere Responder. PXE Everywhere Responder has its own installer (introduced in v4.0). It is only required to support networks that have DHCP Snooping enabled. DHCP snooping prevents PXE Everywhere Agents from receiving or responding to PXE requests on the standard UDP ports (67 & 68). As the PXE code built into the network adapter always broadcasts PXE requests on UDP port 67, it is necessary to load a custom boot loader from an authorized source (the PXE Everywhere Responder) that can then broadcast another request on the custom UDP port that is not blocked by the network switch and on which the Agents are configured to listen. Once the PXE Everywhere Agents intercept these requests on the custom port, the functionality of the agents remains the same as if DHCP snooping were not enabled. The network routers (IP helpers) must be configured to forward DHCP packets to the Responder and DHCP Snooping must be configured on network switches to authorize the Responder to receive and respond to DHCP requests. Booting PXE clients will always download the custom, light-weight boot loader (51KB) from the Responder but will download the much larger Windows PE boot image from a local peer. You can implement a single PXE Everywhere Responder for all clients, or you may prefer to implement regional or more localized Responders throughout your network. In either case, you will need to configure router IP helpers wherever DHCP Snooping is used, ensuring that the network configuration enables the designated Responder to receive and respond to PXE requests generated by PXE clients. To install, please refer to Installing PXE Everywhere Responder.

12.1.3 How it works

After PXE Everywhere installation and setup, during operation the PXE-booting of machines runs through the following sequence, as illustrated in the picture opposite:

PXE Boot me (67) - When the PXE client boots, it performs the normal DHCP request to get an IP address and also sends a normal PXE request

Elect the initial Agent - The PXE Everywhere Agents on the local subnet intercept the PXE request and elect a candidate for servicing the request.

What should I do? - The elected Agent contacts the PXE Everywhere Central Server to find out whether the PXE client should be served a boot image.

Any OS for PXE Client? - The PXE Everywhere Central Server checks the Configuration Manager database to see if there are any OS deployment task sequences deployed to the PXE client matching its MAC address and / or SMBIOS GUID.

Here's what to do - If a task sequence deployment is found, the PXE Everywhere Central Server replies to the elected Agent with the boot image ID referenced in the task sequence and information whether the deployment is mandatory or not. If more than one deployment is found, the last one is used. If no deployments are found, the Central Server indicates so in the reply.

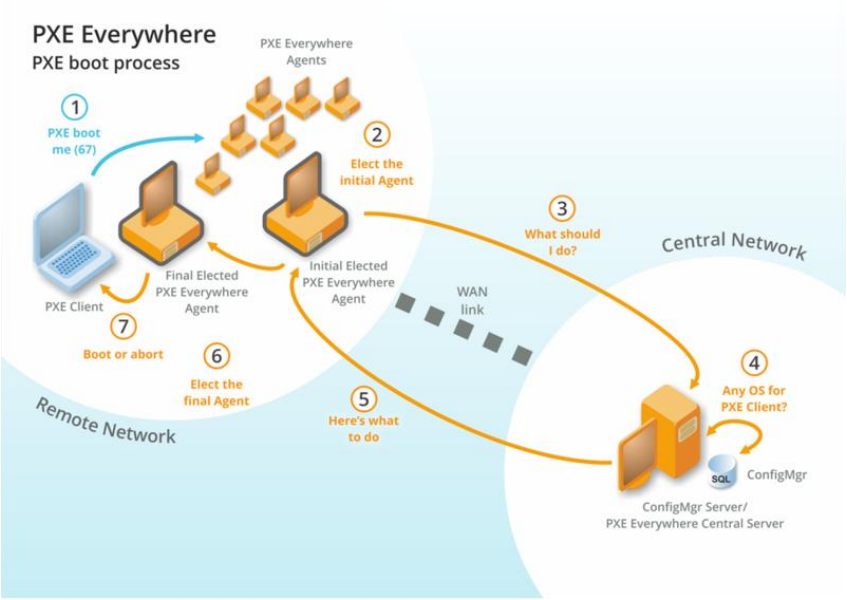
Elect the final Agent - Upon receiving the reply, the elected Agent holds a second election in the subnet to choose an Agent that will boot the PXE client. If an Agent other than itself wins the second election, the information received from Central Server is passed on to it.

Boot or abort - The winner of the second election boots responds to the PXE client which boots as follows:

If a mandatory deployment was found, the PXE client is booted using the WinPE boot image referenced in the deployed task sequence

If non-mandatory deployment was found, the PXE client is presented with an option to boot using a WinPE boot image, requiring user interaction at the machine

If no deployments were found, the PXE-boot is aborted allowing the PXE client to boot to a local OS, if any.



When DHCP Snooping is enabled on the network, the above process changes slightly, as illustrated in the picture opposite:

PXE Boot me (67) - When the PXE client boots, it performs the normal DHCP request to get an IP address and also sends a normal PXE request.

Router forwards the request - The PXE request is forwarded to the PXE Everywhere Responder by an IP helper configured on the router.

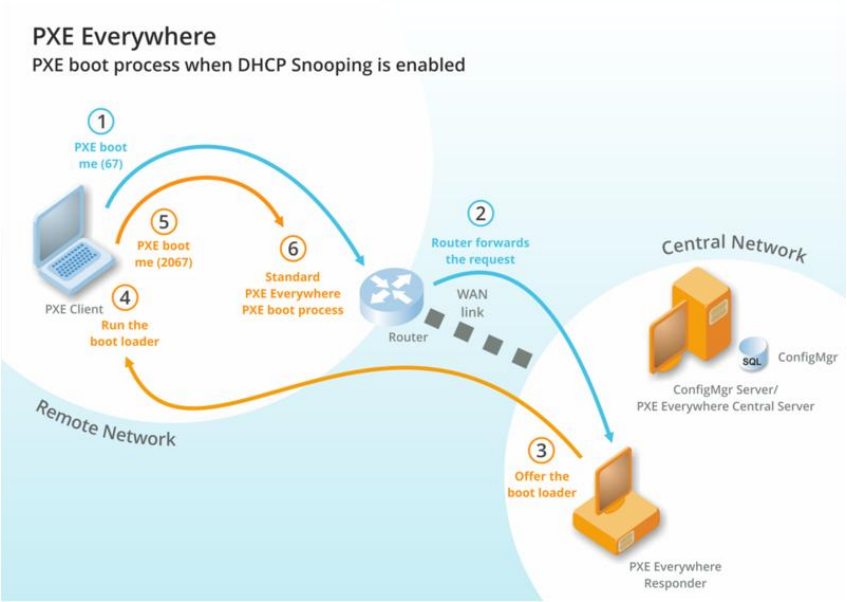
Offer the boot loader - The PXE Everywhere Responder offers the PXE client the appropriate (BIOS or UEFI) boot loader.

Run the boot loader - The PXE client downloads the boot loader from the PXE Everywhere Responder and executes it.

PXE boot me (2067) - The boot loader broadcasts a new PXE request on the custom port (2067). The PXE Everywhere Agents are also configured to listen on this custom port.

Standard PXE Everywhere PXE boot process - From this point on the process follows from step 2 in the standard process detailed above.

Please refer to Design Considerations for further explanation of how to get PXE Everywhere ready for use.



12.2 Implementing PXE Everywhere

Everything you need to know about getting PXE Everywhere installed and running on your network. This section is structured in a way that leads you through a typical implementation project.

12.2.1 Design Considerations

What you will need to prepare in advance of implementing PXE Everywhere in your network. Typically, these are tasks that may take some time to organize, depending on how your organization works. A comprehensive list of installation and software requirements is provided in Requirements.

If you are upgrading PXE Everywhere, please review this page and then refer to Upgrading PXE Everywhere.

12.2.1.1 Network Configuration

When implementing PXE Everywhere, it must be the only PXE solution on each LAN used by your PXE clients. This means any existing PXE services on these LANs must be disabled, and any existing DHCP relays (IP helpers) that forward requests to PXE servers must also be disabled. DHCP relays (IP helpers) used for DHCP requests should be kept.

A working DHCP implementation is required. You must remove DHCP Scope Options (66, 67) you may have previously used in native Configuration Manager because they will conflict with PXE Everywhere.

By default, the Agent listens on port 67, but will listen instead on port 2067 if the Agent has been configured to run in an environment that has DHCP Snooping enabled. If Agents use a port other than 67, then support for DHCP Snooping option is assumed, and PXE Everywhere Responders must be configured to use that port. If DHCP Snooping is not being used, then Agents must use port 67, and you do not need to install Responders.

Ensure client and network firewalls are configured to support Requirements: Firewall Ports.

12.2.1.1.1 DHCP Snooping

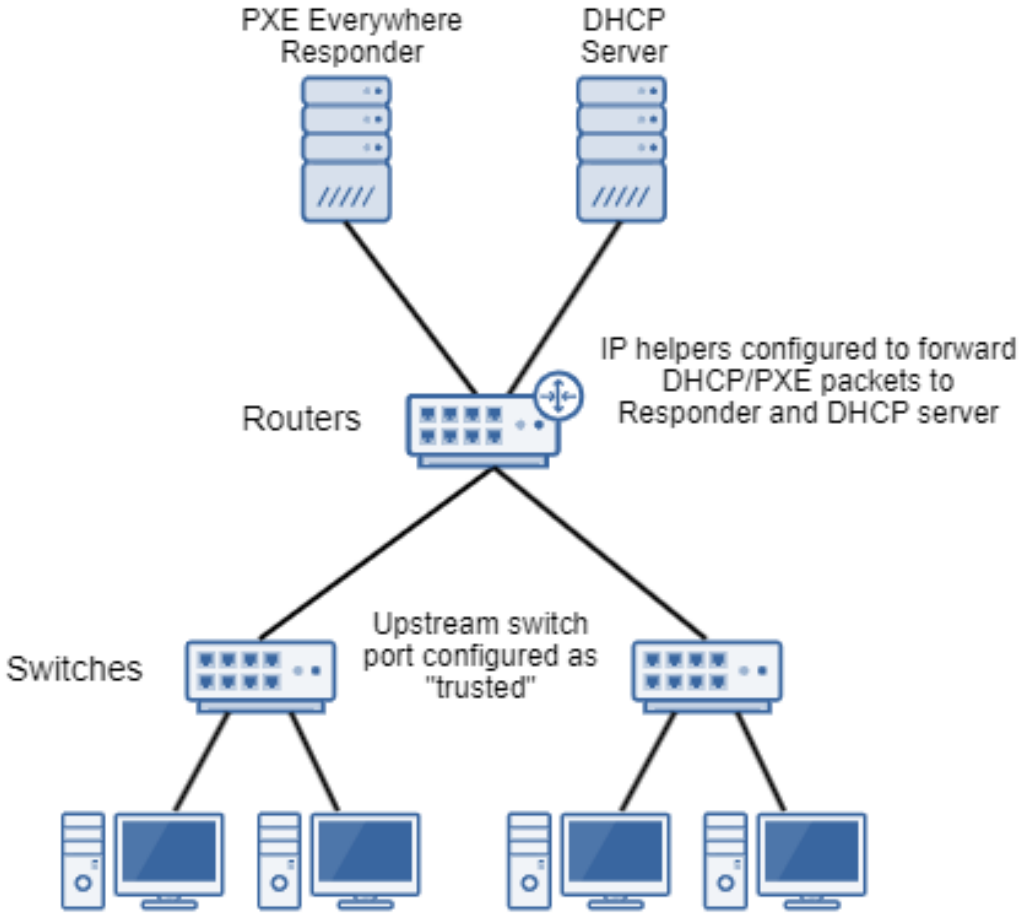
One or more PXE Everywhere Responders are required when network hardware or design prevents local DHCP traffic, for example when DHCP Snooping has been enabled. Your network devices may have other settings enabled which also prevent local DHCP. Therefore, you should test your network before proceeding and determine if you can reconfigure your network and/or install Responders.

> **Tip**
>
> One method of testing to see if local DHCP is blocked, is to put a network packet capture tool like Wireshark on a device you intend to use as PXE Everywhere Agent, start a capture and do a DHCP release/renew from another client on the same subnet. The capture tool must be in promiscuous mode. If you can see the DHCP traffic in the packet capture, then you probably do not need a Responder. If you don’t see any DHCP traffic then you will need to consider installing Responders.

If you decide to install PXE Everywhere Responders, you will need to configure network switches to allow the PXE Everywhere Responder to receive and respond to PXE requests on port 67. Typically, this requires configuring the switch port connected to the router as "trusted". Refer to the switch manufacturer's documentation for more details.

You will also need to configure DHCP Relays (IP helpers) on routers to forward DHCP/PXE packets to the PXE Everywhere Responder(s) in addition to any DHCP Relays you already have configured for the DHCP server(s).

PXE Everywhere Agents and Responders must use a common port, which is 2067 by default. All Agents and Responders must use the same port.



12.2.1.2 Infrastructure requirements

12.2.1.2.1 Microsoft System Center Configuration Manager

A working Configuration Manager system is required, with clients that are healthy and functioning properly.

To test PXE Everywhere, you will need a working OS deployment task sequence and at least one remote PXE Client.

Although Configuration Manager is recommended for deploying PXE Everywhere Agent and PXE Everywhere Responder, they have no dependency on Configuration Manager itself.

You will also use a Configuration Manager Task Sequence to stage the 1E PXE Everywhere boot images on each PXE Everywhere Agent computer.

12.2.1.2.2 PXE Everywhere Central server

This is a web application that the PXE Everywhere Agents use to determine if a PXE client should be served a boot image. In most cases, the only infrastructure required for PXE Everywhere is the PXE Everywhere Central server, in addition to a Configuration Manager site with at least one Distribution Point. During installation, the PXE Everywhere Central installer adds some stored procedures to the Configuration Manager database that are executed by the web application

when requested by PXE Everywhere Agents. In a multi-site hierarchy, the PXE Everywhere Central server should be connected to the CAS database server.

You will need to decide where to install it. You can install PXE Everywhere Central on a Configuration Manager site server, or on any other server that has IIS installed and has good connectivity to the Configuration Manager database, ideally equivalent to the connection that the site server has to its database. Suitable alternatives for hosting PXE Everywhere Central are ActiveEfficiency or Tachyon Platform server. By default, the PXE Everywhere web application will install under any website that has an HTTP binding using port 80. If there is more than one HTTP 80 binding, it will install under the first according to IIS Site order, which is **Default Web Site**, by default.

Please refer to Requirements for specific system requirements for the PXE Everywhere Central server, including Windows Server roles and features and Firewall Ports.

12.2.1.2.3 PXE Everywhere Agent

PXE Everywhere client provides a lightweight PXE server that responds to PXE boot requests from the local subnet and serves boot files to requesting PXE clients. It must therefore be installed on at least one client in each subnet where PXE booting is required, and preferably installed on all PCs in your environment, thereby providing maximum availability (redundancy) and scalability (load-balancing) for PXE boot requests.

To install PXE Everywhere Agent, you require the following:

At least 2MB of free disk space for the application, plus whatever size your boot images require (typically 130MB each).

Ensure client side firewalls have exceptions for the ports required by PXE Everywhere.

Antivirus exceptions

When upgrading, we recommend you update all versions of PXE Everywhere Agent running on a single subnet at the same time.

Refer to Requirements for other specific system requirements for the PXE Everywhere Agent.

For PXE clients to PXE boot into Windows PE, each PXE Everywhere Agent requires a boot image and supporting files. As this is a complex process, 1E recommends using Introducing 1E Client Deployment Assistant to configure and simultaneously deploy PXE Everywhere Agent with the boot image. CDA integrates with Configuration Manager to create packages and deployments. If you need to deploy boot images separately they are available in the Microsoft Windows Automated Deployment Kit (ADK) as described in Preparing and deploying 1E PXE Everywhere boot images.

> **Note**
>
> The PXE Everywhere Agent client module in 1E Client 5.1 and later does not require a license key. PXE Everywhere 4.0 does not require input of a license key, or relicencing when upgrading or updating. Customers are legally bound to use the software within the terms of the 1E software license agreement.

12.2.1.2.4 PXE clients

PXE clients are computers that will PXE boot into Windows PE and install or repair the Windows OS. They do not require PXE Everywhere to be installed on them.

The following are required for clients that need to PXE boot in order to install an operating system:

PXE must be enabled in the firmware settings. Refer to the hardware-specific documentation for details on how to enable PXE. You can also use the BIOS TO UEFI tool to enable UEFI PXE on Dell, Lenovo and HP systems in a Task Sequence.

Minimum hardware specification as required by the target operating system.

LAN connection 100Mbps or greater.

12.2.1.2.5 PXE Everywhere Responder

As described in DHCP Snooping above, if local DHCP traffic is blocked, for example by DHCP Snooping being enabled on your network switches, then you will need to implement at least one authorized PXE Everywhere Responder, preferably on a Server OS, and enable DHCP Snooping mode on Agents. Refer to Network Configuration above for additional network configuration required to support DHCP Snooping.

The Responder can be installed on a workstation OS, however for production environments it should be installed on a server OS, as all DHCP and PXE requests will be routed to this server (in addition to your existing DHCP servers). The Responder will simply discard DHCP requests and only process PXE requests. The Responder cannot be installed on an existing DHCP server.

> **Note**
>
> PXE Everywhere Responder cannot co-exist on the same computer as PXE Everywhere Agent, and are not supported together. Whilst it is possible to install them together, they will not work and will have issues such as failure to bind to ports.
>
> If you install 1E Client on the same computer then you must disable the client module for PXE Everywhere Agent. You can do this by adding

In most cases a single Responder will be sufficient. In larger environments, or environments where networks in different regions are managed by different parties, you can implement multiple PXE Everywhere Responders, each one managing different segments of your network. For example, you may choose to implement a Responder for each geographic region. This decision will often depend on your current network topology and how the network is currently managed.

To install PXE Everywhere Responder you require the following:

PXE Everywhere Responder is 64-bit only. A server OS is recommended.

Requires at least 2MB free disk space for the application

Ensure client side firewalls have exceptions for the ports required by PXE Everywhere.

See Anti-virus exceptions.

When upgrading, we recommend you update all versions of PXE Everywhere Agent running on a single subnet at the same time.

Refer to Requirements for other specific system requirements for the PXE Everywhere Responder.

When implementing PXE Everywhere in a network that has DHCP Snooping enabled, you will need to use and enable communication on custom UDP ports to allow the PXE client to communicate with the PXE Everywhere agents (the standard ports are blocked by the DHCP Snooping feature). By default, the custom UDP ports used in the initial boot loader served by the Responder are set to 2067 and 2068. To use different ports you must create the following registry values in*HKLM\Software\Wow6432Node\1E\PXELiteServer*on Responders, and ensure that the value of AltPxeServerPort is the same as used by DhcpPort on PXE Everywhere Agents. Do not change the value of DhcpPort on Responders.

Name	Type	Notes
AltPxeServerPort	REG_DWORD	This is the UDP port that the alternate boot loader will broadcast the custom PXE request on. The PXE Everywhere Agents must be configured to listen on this port, so it must be the same port defined by DHCPPORT when installing the PXE Everywhere Agent. If this registry setting does not exist then port 2067 is used.
AltPxeClientPort	REG_DWORD	This is the UDP port that the PXE Everywhere Responder will reply to the PXE client (alternate boot loader) on. If this registry setting does not exist then port 2068 is used.

Note

The PXE Everywhere Responder does not require a license key. PXE Everywhere 4.0 does not require input of a license key, or relicencing when upgrading or updating. Customers are legally bound to use the software within the terms of the 1E software license agreement.

12.2.2 Requirements

Software requirements that must be met in order for PXE Everywhere to be successfully installed and used.

12.2.2.1 Active Directory requirements

12.2.2.1.1 Installation account for PXE Everywhere Central

The account of the user that performs the PXE Everywhere Central installation must meet the following criteria, which can be temporary for installation only:

Must be a domain account (a local account cannot be used)

Must be assigned to the *Full Administrator* security role in Configuration Manager

Must have local admin rights (that is, the account is a direct or indirect member of the local Administrators group) on the server where you are installing PXE Everywhere Central

Must be assigned the sysadmin server role in the SQL Server instance which hosts the Configuration Manager database. This can be temporary during installation.

12.2.2.1.2 Installation account for PXE Everywhere Agent and PXE Everywhere Responder

Configuration Manager installs applications in the local system context, which is sufficient for the installation of the PXE Everywhere Agent and PXE Everywhere Responder.

If installed manually, the account used to install it must have local admin rights. That is, the account is a direct or indirect member of the local Administrators group) on the computer you are installing it on.

12.2.2.2 Microsoft ADK files

In addition to the binaries supplied by 1E, PXE Everywhere Agent requires a number of files that are distributed and licensed with the Microsoft Windows Automated Deployment Kit (ADK). The required files are listed in the table opposite, along with the location on the PXE Everywhere Agent that they need to be installed to.

As these files are licensed by Microsoft, 1E are unable to include them in the installation media. However, you can use the Introducing 1E Client Deployment Assistant to extract the required files from the ADK, create an installer transform and prepare an Application in Configuration Manager that will install the PXE Everywhere Agent with the appropriate settings and the additional Microsoft files.

The Windows Assessment and Deployment Kits (ADK) normally exist on the Configuration Manager CAS or Primary Site server, although they can be downloaded separately from the Microsoft website.

File	Destination Location (relative to TFTPROOT)
boot.sdi	*\boot.sdi*
abortpxe.com	*\boot\x86\abortpxe.com*
bootmgr.exe	*\boot\x86\bootmgr.exe*
pxeboot.com	*\boot\x86\pxeboot.com*
pxeboot.n12	*\boot\x86\pxeboot.n12*
bootmgfw.efi	*\boot\x86\bootmgfw.efi*
\boot\x64\bootmgfw.efi	
wgl4_boot.ttf (optional)	*\boot\fonts\wgl4_boot.ttf*

12.2.2.3 Supported Platforms

A list of all the platforms supported by PXE Everywhere, and the software required to allow PXE Everywhere Central and Responders to be installed or to work.

Please refer to Common client requirements for details of **PXE Everywhere Agent** client module of the 1E Client.

Category	PXE Everywhere Central	PXE Everywhere Responder	Notes
Windows OS	Windows Server 2022 Windows Server 2019 Windows Server 2016	Windows Server 2022 Windows Server 2019 Windows Server 2016 Windows 10 CB 21H2 Windows 11 CB 21H2 Windows 10 CB 21H1 Windows 10 CB 20H2	**Will only install on** computers running one of these OS. **Note** Installing PXE Everywhere Central on domain controllers is not a supported configuration. **Note** A server OS is recommended for PXE Everywhere Responder.
Web servers	IIS 10	Not applicable.	For PXE Everywhere Central: You **must** have one of these Web server versions installed. The installer **must** be run on the system hosting the Web server as it deploys the PXELite website on it. Requires the following OS roles and features: Web Server (Web-Server) ASP.NET 4.5 or later (Web-Asp-Net45)
Runtime libraries	.NET Framework 4.8	Visual C++ 2013 Redistributable	You**must**have one of these .NET Framework versions installed to install PXE Everywhere Central

Category	PXE Everywhere Central	PXE Everywhere Responder	Notes
			PXE Everywhere Responder installer includes the redistributable package for Visual C++ 2013.
Boot Image OS	Windows Server 2022 Windows Server 2019 Windows Server 2016 Windows 10 CB 21H2 Windows 11 CB 21H2 Windows 10 CB 21H1 Windows 10 CB 20H2	Not applicable.	**UpdateBootImage.exe** is supported only on these client OS. The Admin Tools feature of the PXE Everywhere Central installer installs a tool named **UpdateBootImage.exe** that uses the native Configuration Manager API used to generate boot media.
Configuration Manager	SCCM CB 2203 SCCM CB 2111 SCCM CB 2107 SCCM CB 2103 SCCM CB 2010	Not applicable.	You can install PXE Everywhere Central on a Configuration Manager site server, or on any other server that has IIS installed and has good connectivity to the Configuration Manager database, ideally equivalent to the connection that the site server has to its database.

12.2.2.3.1 Windows Server roles and features

The following roles, role services and features must be *installed/enabled* as a minimum on the PXE Everywhere Central server.

The Name column is the reference used in PowerShell commands; and for .NET Framework 4.X features the PowerShell name includes 45 instead of the actual version.

Role or Feature	Display Name	Name	Notes
Web Server	**Web Server (IIS)**	**Web-Server**	
Web Server Common HTTP Features	Default Document	Web-Default-Doc	Included in Web-Server
Directory Browsing	Web-Dir-Browsing	Included in Web-Server	
HTTP Errors	Web-Http-Errors	Included in Web-Server	
Static Content	Web-Static-Content	Included in Web-Server	
Web Server Health and Diagnostics	HTTP Logging	Web-Http-Logging	Included in Web-Server
Web Server Performance	Static Content Compression	Web-Stat-Compression	Included in Web-Server
Web Server Security	Request Filtering	Web-Filtering	Included in Web-Server
Web Server Application Development	.NET Extensibility 4.X	Web-Net-Ext45	Included in Web-Asp-Net45
ASP.NET 4.X	**Web-Asp-Net45**		
ISAPI Extensions	Web-ISAPI-Ext	Included in Web-Asp-Net45	
ISAPI Filters	Web-ISAPI-Filter	Included in Web-Asp-Net45	

Role or Feature	Display Name	Name	Notes
Web Server Management Tools	**IIS Management Console**	**Web-Mgmt-Console**	Recommended
.NET Framework 4.X Features	**.NET Framework 4.X**	**Net-Framework-45-Core**	
ASP.NET 4.X	Net-Framework-45-ASPNET	Included in Web-Asp-Net45	

12.2.2.4 Firewall Ports

Although a computer with PXE Everywhere Agent installed can also be a PXE client, it cannot be both at the same time.

Component	Ports	Protocol	Direction	Usage	Configurable
Central	80	HTTP	Inbound	PXE Everywhere Agent communicating with the PXE Everywhere Central web application. Browser connections to the PXE Everywhere Central website to verify installation.	Yes, post-installation on the Central server, and during installation of Agents by configuring the URL. If HTTPS is required, please contact 1E for advice.
Central	135 and 445 (initially)	WMI-DCOM TCP	Outbound	PXE Everywhere Central installer requires	No.

Component	Ports	Protocol	Direction	Usage	Configurable
				access to the Configuration Manager Site server, and to the server hosting the SMS Provider role. If there is only one SMS Provider, it is often on the Site server. In each case, TCP 135 and 445 are used to initiate communications and negotiate a dynamic RPC port. The dynamic range depends on the Windows OS version.	
Central	1433	(See usage for	Outbound	PXE Everywhere Central to access to the SQL	Depends on the Configuration Manager SQL Server instance. The Central installer determines the connection

Component	Ports	Protocol	Direction	Usage	Configurable
		protocol) TCP		database role for the selected Configuration Manager Site.	string by querying the Site's SMS Provider.
ConfigMgr Site Server (and SMS Provider)	135 and 445 (initially)	WMI (DCOM) TCP	Inbound	PXE Everywhere Central installer requires access to the Configuration Manager Site server, and each of the servers hosting the SMS Provider role. If there is only one SMS Provider, it is often on the Site server. In each case, TCP 135 and 445 are used to initiate communications and negotiate a dynamic RPC port. The	No.

Component	Ports	Protocol	Direction	Usage	Configurable
				dynamic range depends on the Windows OS version.	
ConfigMgr Site SQL database	1433	(See usage for protocol) TCP	Inbound	PXE Everywhere Central to access to the SQL database role for the selected Configuration Manager Site.	Depends on the Configuration Manager SQL Server instance.
Agent (1E.Client.exe)	80	HTTP TCP	Outbound	PXE Everywhere Agent communicating with the PXE Everywhere Central web application.	Yes, post-installation on the Central server, and during installation of Agents by configuring the URL. If HTTPS is required, please contact 1E for advice.
Agent (1E.Client.exe)	2012	UDP	Inbound & outbound	Election process inter-communication between PXE Everywhere Agents on a subnet.	Yes, during installation of PXE Everywhere Agents using the MODULE.PXEEVERYWHERE.COMMSPORT installer property.

Component	Ports	Protocol	Direction	Usage	Configurable
Agent (1E.Client.exe)	67 or 2067	BOOTP UDP	Inbound	Port 67 is the standard PXE discover port. PXE clients use this port to broadcast PXE discovers on the local subnet. PXE Everywhere Agents listen on this port for PXE discovers that are broadcast on the local subnet. If PXE Everywhere is configured to support DHCP Snooping, Agents use a custom port (default 2067) to listen for PXE requests, instead of	Only the DHCP Snooping ports are configurable, and must be the same on all Agents and Responders.

Component	Ports	Protocol	Direction	Usage	Configurable
				standard port 67.	
Agent (1E.Client.exe)	68 or 2068	BOOTP UDP	Outbound	Port 68 is the standard PXE offer port. PXE Everywhere Agent uses this port to respond with offers to PXE discovers on the local subnet. If PXE Everywhere is configured to support DHCP Snooping, Agents use a custom port (default 2068) instead of the standard port 68.	Only the DHCP Snooping ports are configurable, and must be the same on all Agents and Responders.
Agent (1E.Client.exe)	69	TFTP UDP	Inbound	Port 69 is the standard PXE TFTP port. The PXE client	No.

Component	Ports	Protocol	Direction	Usage	Configurable
				downloads the boot image from the elected PXE Everywhere Agent using TFTP. This port is also used if PXE Everywhere is configured to support DHCP Snooping.	
Agent (1E.Client.exe)	4011	UDP	Inbound	Port 4011 is the standard PXE port used by PXE clients to communicate with a PXE Server after the initial discover / offer, to unicast a request for the location of the TFTP boot image file. This port is not used if PXE Everywhere	No.

Component	Ports	Protocol	Direction	Usage	Configurable
				is configured to support DHCP Snooping.	
Responder (PXEEverywhereResponder.exe)	67	BOOTP UDP	Inbound	Port 67 is the standard PXE discover port. A Responder is only required when DHCP Snooping is enabled, and listens for PXE requests from PXE clients on this port. See note below about DHCP Snooping and DHCP Relays.	No.
Responder (PXEEverywhereResponder.exe)	68	BOOTP UDP	Outbound	Port 68 is the standard PXE offer port. A Responder is only required when DHCP Snooping is enabled,	No.

Component	Ports	Protocol	Direction	Usage	Configurable
				and responds to PXE clients with offers unicast on this port. See note below about DHCP Snooping and DHCP Relays..	
PXE client	67	BOOTP UDP	Outbound	Port 67 is the standard PXE discover port. PXE clients use this port to broadcast PXE discovers on the local subnet. If DHCP Snooping is being used these discovers are forwarded to a Responder. See note below about DHCP Snooping and	No.

Component	Ports	Protocol	Direction	Usage	Configurable
				DHCP Relays. .	
PXE client	68	BOOTP UDP	Inbound	Port 68 is the standard PXE offer port. PXE Everywhere Agent broadcasts on this port with an offer in response to PXE discovers on the local subnet. If DHCP Snooping is being used, then Responders respond with offers on this port. See note below about DHCP Snooping and DHCP Relays..	No.
PXE client	69	BOOTP UDP	Outbound	Port 69 is the standard PXE TFTP port. A PXE client uses TFTP to	No.

Component	Ports	Protocol	Direction	Usage	Configurable
				download the boot image from the elected PXE Everywhere Agent on the local subnet. This port is also used if PXE Everywhere is configured to support DHCP Snooping.	
PXE client	4011	UDP	Outbound	Port 4011 is the standard PXE port used by PXE clients to unicast a request to the PXE Everywhere Agent for the location of the TFTP boot image file, after the initial discover/offer. This port is not used if PXE Everywhere	No.

Component	Ports	Protocol	Direction	Usage	Configurable
				is configured to support DHCP Snooping.	
PXE client	2067	BOOTP UDP	Outbound	If PXE Everywhere is configured to support DHCP Snooping, a custom port is used (default 2067) to perform a PXE request after the PXE client has downloaded a boot loader from a Responder. Only used if DHCP Snooping is being used, and PXE Everywhere has been configured to use this port.	Yes. DhcpPort is configured during installation of Agents. AltPxeServerPort is manually configured on Responders.

Component	Ports	Protocol	Direction	Usage	Configurable
PXE client	2068	BOOTP UDP	Inbound	If PXE Everywhere is configured to support DHCP Snooping, a custom port is used (default 2068) to respond to a PXE request after the PXE client has downloaded a boot loader from a Responder. Only used if DHCP Snooping is being used, and PXE Everywhere has been configured to use this port.	Yes. AltPxeClientPort is manually configured on Responders.

Note

PXE client ports do not need to be configured on the OS firewall because it is the network interface which is doing the communicating. However you may need to configure intervening network firewalls for communication beyond the local subnet.

PXE Everywhere Responders communicate only with PXE clients; they do not communicate with PXE Central, PXE Everywhere Agents, other Responders, or Configuration Manager.

Note

If DHCP Snooping is enabled on networks, then DHCP Relays (IP helpers) must be configured to forward PXE requests (discovers) from client VLANs to specific Responders on port 67 and return the responses (offers) on port 68.

If DHCP Snooping is not enabled, then all PXE-boot traffic is on the local subnet, except for communication between the elected PXE Everywhere Agent and the PXE Everywhere Central server, and DHCP Relays are not required to forward PXE requests.

Note

Ports used by PXE clients to communicate with DHCP servers are not included in the above table. Communication with DHCP servers occurs before a PXE client PXE-boots, and typically use their own DHCP Relays (IP helpers).

Ports used by PXE clients to communicate with ConfigMgr Site systems are not included in the above table. Communication with ConfigMgr occurs only after a PXE client has downloaded the WinPE boot image (referenced in the deployed task sequence) from a local PXE Everywhere Agent, and booted into WinPE to start the Task Sequence.

Ports used by ConfigMgr Administrator workstations to communicate with ConfigMgr Site systems are not included in the above table. ConfigMgr Console extensions for PXE Everywhere Admin Tools use the same ports as ConfigMgr Console.

12.2.2.5 Antivirus exceptions

PXE Everywhere functionality may be impaired by antivirus programs. Although we generally advise that no malware exclusions are used, it is justifiable in certain cases to isolate specific locations and files used by specific software. The following is a list of exclusions that could be added for PXE Everywhere Local, but before you implement them, make sure they are compatible with existing exclusions.

All PXE Everywhere component installations:

%SystemDrive%\ProgramData\1E\PXEEverywhere*.log & *.lo_

Additional exclusions required on PXE Everywhere Agents:

%SystemDrive%\Program Files\1E\Client\Extensibility\PXEEverywhere\CreateBcD.exe

%SystemDrive%\ProgramData\1E\PXEEverywhere\TftpRoot\boot.sdi

%SystemDrive%\ProgramData\1E\PXEEverywhere\TftpRoot\Boot\Fonts\wgl4_boot.ttf

%SystemDrive%\ProgramData\1E\PXEEverywhere\TftpRoot\Boot\x86\abortpxe.com

%SystemDrive%\ProgramData\1E\PXEEverywhere\TftpRoot\Boot\x86\Bootmgr.exe

%SystemDrive%\ProgramData\1E\PXEEverywhere\TftpRoot\Boot\x86\pxeboot.com

%SystemDrive%\ProgramData\1E\PXEEverywhere\TftpRoot\Boot\x86\pxeboot.exe

%SystemDrive%\ProgramData\1E\PXEEverywhere\TftpRoot\Images**.bcd

%SystemDrive%\ProgramData\1E\PXEEverywhere\TftpRoot\Images**.wim

12.2.3 Installing and Upgrading

How to install and upgrade PXE Everywhere components.

12.2.3.1 Installing PXE Everywhere Central

Using the PXE Everywhere Central installation wizard to check prerequisites, configure and install PXE Everywhere Central and/or PXE Everywhere Admin Tools.

12.2.3.1.1 The PXE Everywhere Central installer

The PXE Everywhere Central installer is included in the PXE Everywhere zip file that can be downloaded from the Nomad area of the 1E Support Portal.

Before you begin installation, please ensure you have reviewed Design Considerations and Requirements pages, and the installation steps below.

The installer is used to:

Install **PXE Everywhere Central** on any server that has IIS and other prerequisites installed

Install **PXE Everywhere Admin Tools** on any computer that has Configuration Manager Admin Console installed.

Both can be installed on a typical Configuration Manager site server.

A single instance of **PXE Everywhere Central** is required in any given environment. It can be installed on any server but must have good connectivity to the Configuration Manager database, preferably on the same subnet. The installer adds some stored procedures to the Configuration Manager database, where are used by the PXE Everywhere Central Web service whenever queried by PXE Everywhere Agents.

PXE Everywhere Admin Tools are required for preparing the Windows PE boot images for use by PXE Everywhere Agents, as described in Preparing and deploying 1E PXE Everywhere boot images. If you are only here to install the Admin Tools then you can skip to the PXE Everywhere Admin Tools installation steps.

12.2.3.1.2 Running the PXE Everywhere Central installer

Logon to the server using the PXE Everywhere Central installation account and then use the following instructions:

12.2.3.1.2.1 Installing PXE Everywhere Central with the wizard

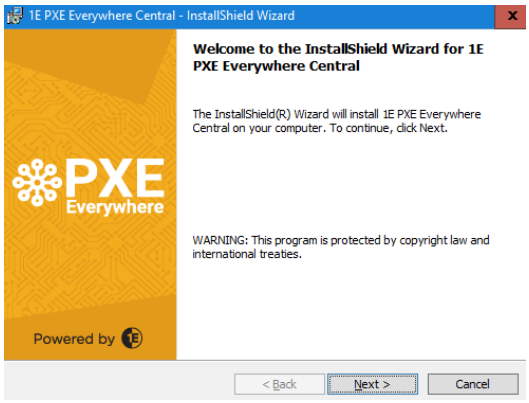
To install PXE Everywhere Central, start a command prompt with elevated rights, using **Run as administrator**, change directory to the location where you downloaded **PXEEverywhereCentral.msi** and run the following suggested command-line:

```
>msiexec /i PXEEverywhereCentral.msi /l*v PXEEverywhereCentral.log
```

12.2.3.1.2.1.1 Welcome to the InstallShield Wizard for 1E PXE Everywhere Central

This screen provides the version number for PXE Everywhere Central and outlines what the wizard will do.

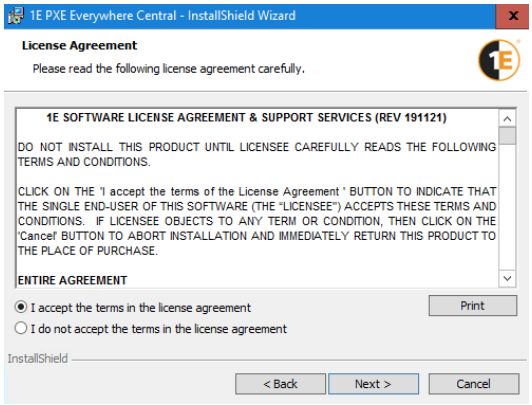
Click **Next** to go to the next screen.



12.2.3.1.2.1.2 License agreement

You must read and then accept this license information by checking the **I accept the terms in the license agreement** checkbox.

Click **Next** to go to the next screen.



12.2.3.1.2.1.3 PXE Everywhere Central Prerequisites

On this screen, background checks are run to ensure the prerequisites for successfully running the installer are met.

If all the checks have passed, click **Next** to got to the next screen. If any of the checks have failed, note them, exit the installer and add the missing ones to the computer where the installer is being run. When that is done re-run the installer and check that the prerequisites are now fully met before continuing.

> **Note**
>
> The features shown are dependent on what items are present on the computer, as described in the following table:

Conditions	Available Features
IIS present ConfigMgr Console on site server	Admin Tools PXE Everywhere Central WebService ConfigMgr Database stored procedure
IIS present No ConfigMgr Console	PXE Everywhere Central WebService ConfigMgr Database stored procedure
No IIS ConfigMgr Console on site server	Admin Tools

If the Configuration Manager Console is not present, you can still install PXE Everywhere Central, but you will need to install the Admin Tools on a computer that has the Configuration Manager Console installed.

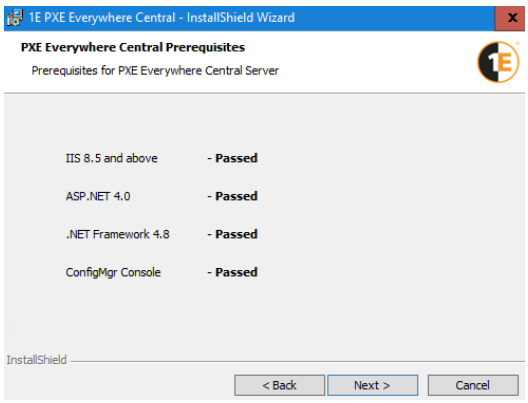
Note

Although the Admin Tools - specifically *UpdateBootImage.exe* - are not run directly from the Configuration Manager console, they will not work unless the following are both installed:

Configuration Manager console

Windows Assessment and Deployment Kit (ADK).

Installation of Admin Tools is shown in PXE Everywhere Admin Tools installation steps.



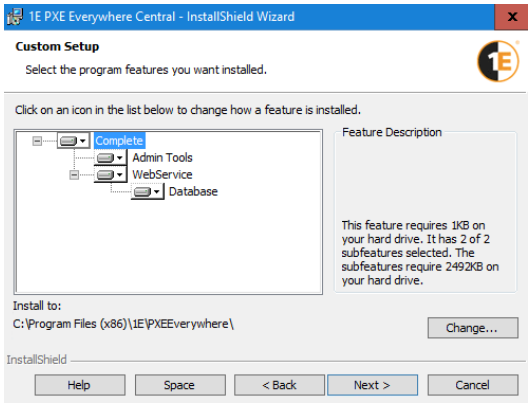
12.2.3.1.2.1.4 Custom Setup

On the **Custom Setup** screen, choose the features to install. As described above, the features available will correspond to whichever prerequisites have been met.

You can select which features are installed by clicking the drop-down against each feature and selecting the installation status from the context menu.

You can change the location for a particular feature by selecting it and clicking the **Change...** button. However, it is recommended that you install all features with the default location unless there is a good reason not to.

When you've finished selecting the components you want to install, click **Next** to continue.

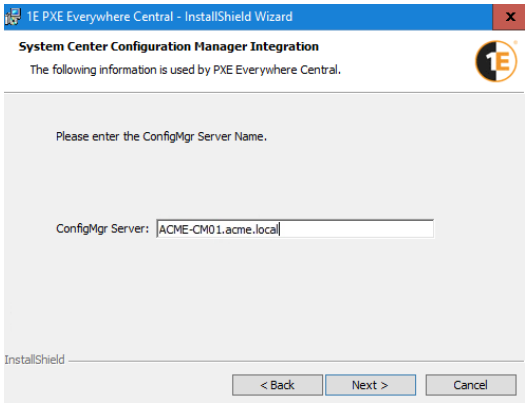


12.2.3.1.2.1.5 System Center Configuration Manager Integration

This screen is only displayed if the Configuration Manager console is not present on the server you are installing on.

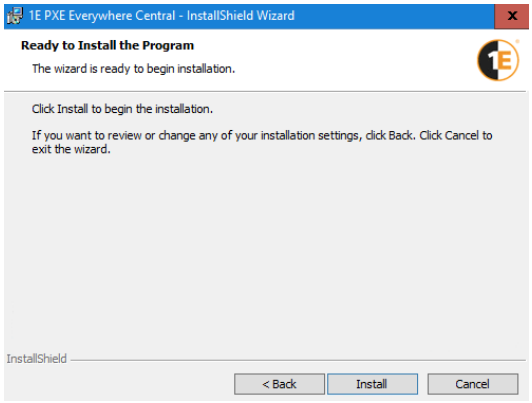
Here you must enter the location of the remote Configuration Manager site server. This can be the name or FQDN of the server where Configuration Manager Primary Site is installed. In a multi-site hierarchy enter the name or FQDN of the CAS site server.

When you click **Next** to continue the installer account credentials will be validated against the selected **ConfigMgr Server**.



12.2.3.1.2.1.6 Ready to Install the Program

Click **Install** to start the PXE Everywhere Central installation.

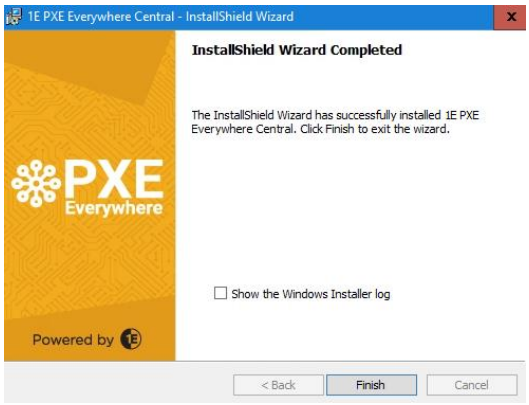


12.2.3.1.2.1.7 InstallShield Wizard Completed

This screen indicates whether the installation was a success or not. If any issues have been reported please refer to the troubleshooting section.

Here you can also optionally check to **Show the Windows Installer log**.

You can click **Finish** to close the installer.



12.2.3.1.2.2 PXE Everywhere Admin Tools installation steps

PXE Everywhere requires preparation of the Windows PE boot image. If PXE Everywhere Central is installed on the Configuration Manager site server or a server that has the Configuration Manager Console you have an option to install the **Admin Tools**, which includes a particular tool (**UpdateBootImage.exe**) that automates the preparation.

The **Admin Tools** can be installed on any computer with the Configuration Manager Console installed where you may want to prepare the Windows PE boot image for use by PXE Everywhere Agents.

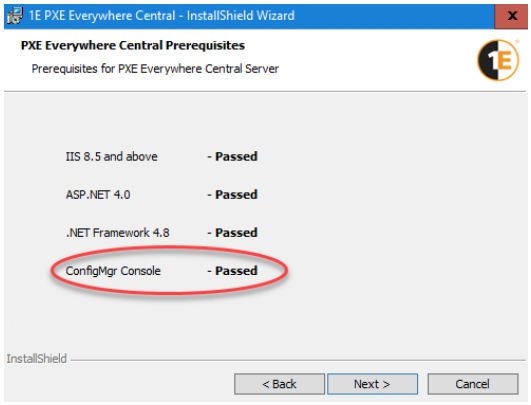
Run the PXE Everywhere Central installer as above, except for the following screens:

12.2.3.1.2.2.1 Prerequisites

On the **Prerequisites** screen, background checks are run to ensure the prerequisites for successfully running the installer are met.

To install the **Admin Tools** you need to confirm that the **ConfigMgr Console** prerequisite check has passed, the other prerequisites are not required for the **Admin Tools**.

Click **Next**.

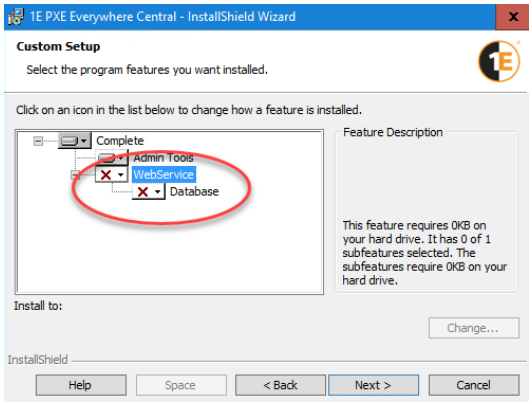


12.2.3.1.2.2.2 Custom Setup

On this screen ensure that the **Admin Tools** feature is the only selected feature. If other features are selected, change their install status to **This feature will not be available**.

Click **Next** when this has been confirmed.

Then click **Install** and allow installation to complete, then click **Finish**.



12.2.3.1.3 Next steps

To verify the PXE Everywhere Central installation, please refer to Verifying: PXE Everywhere Central.

To install the PXE Everywhere Responder, please refer to Installing PXE Everywhere Responder.

To install the PXE Everywhere Agents, please refer to Installing PXE Everywhere Agents.

To stage boot images on PXE Everywhere Agents, please refer to Preparing and deploying 1E PXE Everywhere boot images.

12.2.3.2 Installing PXE Everywhere Responder

Using the PXE Everywhere Responder installation wizard to check prerequisites, configure and install PXE Everywhere Responder. One or more PXE Everywhere Responders are required when network hardware or design prevents local DHCP traffic, for example when DHCP Snooping has been enabled. Please refer to Design Considerations: DHCP Snooping to determine if you need to

install Responders. Once you have decided you need them and have configured your network, please ensure you have reviewed all Requirements before installing.

The PXE Everywhere Responder installer is included in the PXE Everywhere zip file that can be downloaded from the Nomad area of the 1E Support Portal.

12.2.3.2.1 Running the PXE Everywhere Responder installer

Logon to the server using the PXE Everywhere Responder installation account and then use the following instructions:

12.2.3.2.1.1 Installing PXE Everywhere Responder with the wizard

The Responder is installed using the PXE Everywhere Responder installer: **PXEEverywhereResponder.msi**.

> **Note**
>
> Installing a PXE Everywhere Responder is a good choice whenever network hardware or design prevents local DHCP traffic, such as when DHCP snooping has been enabled.
>
> When deploying PXE Everywhere Agents for use with the PXE Everywhere Responder on a network you will need to configure them to use port 2067, which is the default used by the PXE Everywhere Responder, or a custom port if that has been set. Computers will also need an inbound firewall rule.

> **Note**
>
> The PXE Everywhere Responder and PXE Everywhere Agent cannot co-exist on the same computer and are not supported together. Whilst it is possible to install them together, they will not work and will have issues such as failure to bind to ports.
>
> To install a Responder on the same computer as 1E Client then you must disable the client module for PXE Everywhere Agent. For an existing installation of 1E Client, reconfigure the client by setting **Module.PXEEverywhere.Enabled=false**. When installing or upgrading 1E Client on a computer that has or will have a Responder, then you must add **MODULE.PXEEVERYWHERE.ENABLED=false** to the installer command line or edit the **mst** transform.

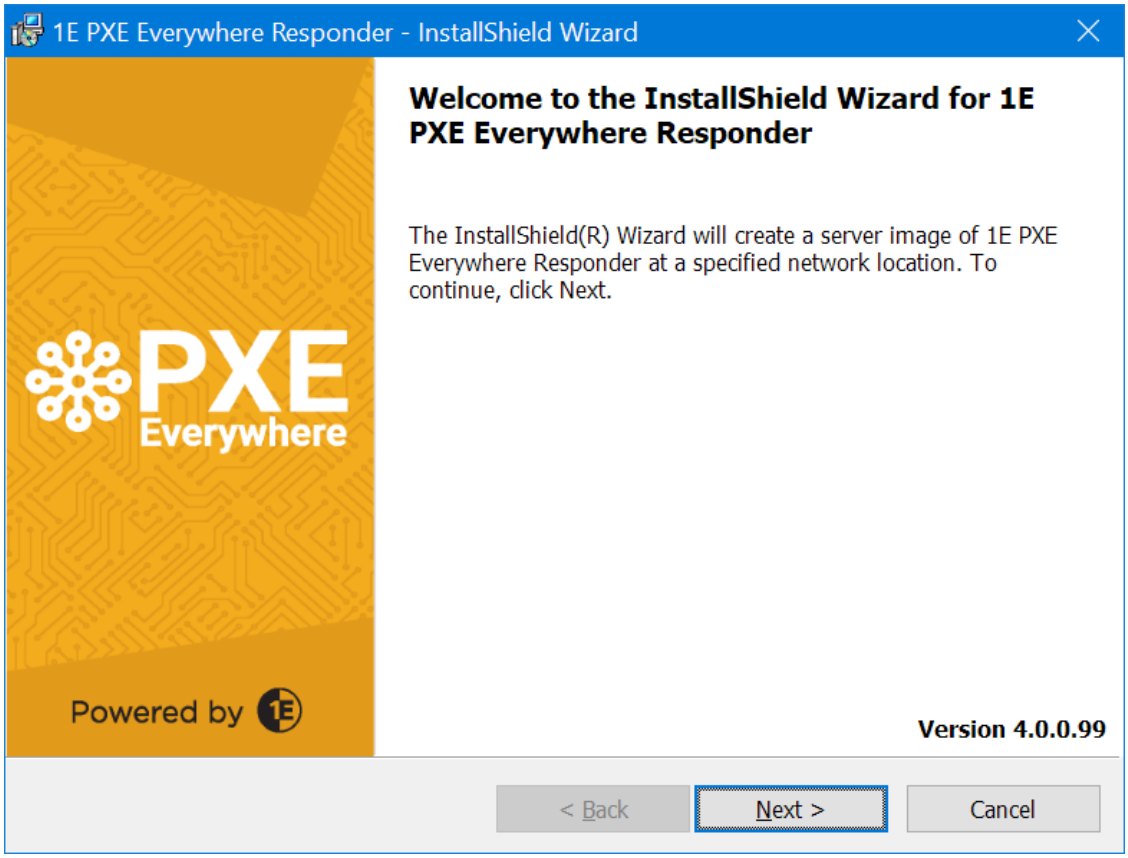
To install PXE Everywhere Responder, start a command prompt with elevated rights, using **Run as administrator**, change directory to the location where you downloaded **PXEEverywhereResponder.msi** and run the following suggested command-line:

```
msiexec /i PXEEverywhereResponder.msi /l*v PXEEverywhereResponder.log
```

12.2.3.2.1.1.1 Welcome to the InstallShield Wizard for 1E PXE Everywhere Responder

This screen provides the version number for PXE Everywhere Responder and outlines what the wizard will do.

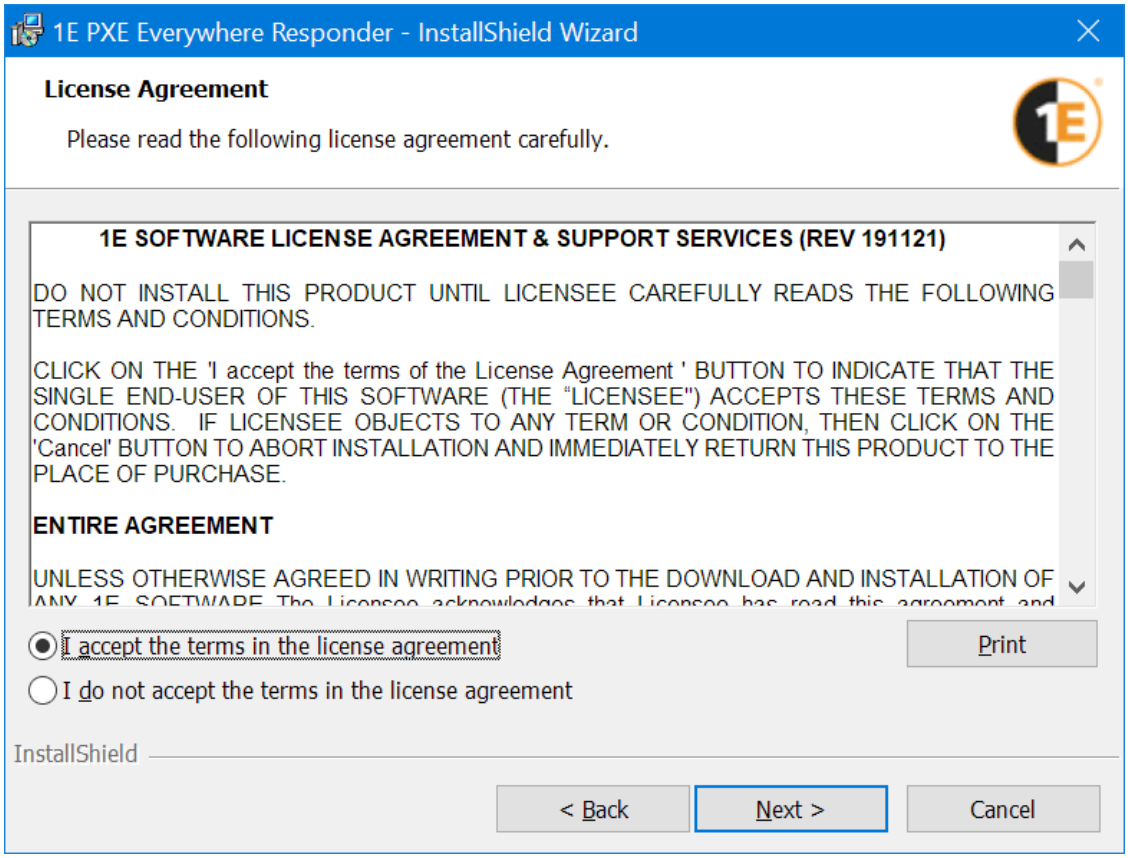
Click **Next** to go to the next screen.



12.2.3.2.1.1.2 License agreement

You must read and then accept this license information by checking the **I accept the terms in the license agreement** checkbox.

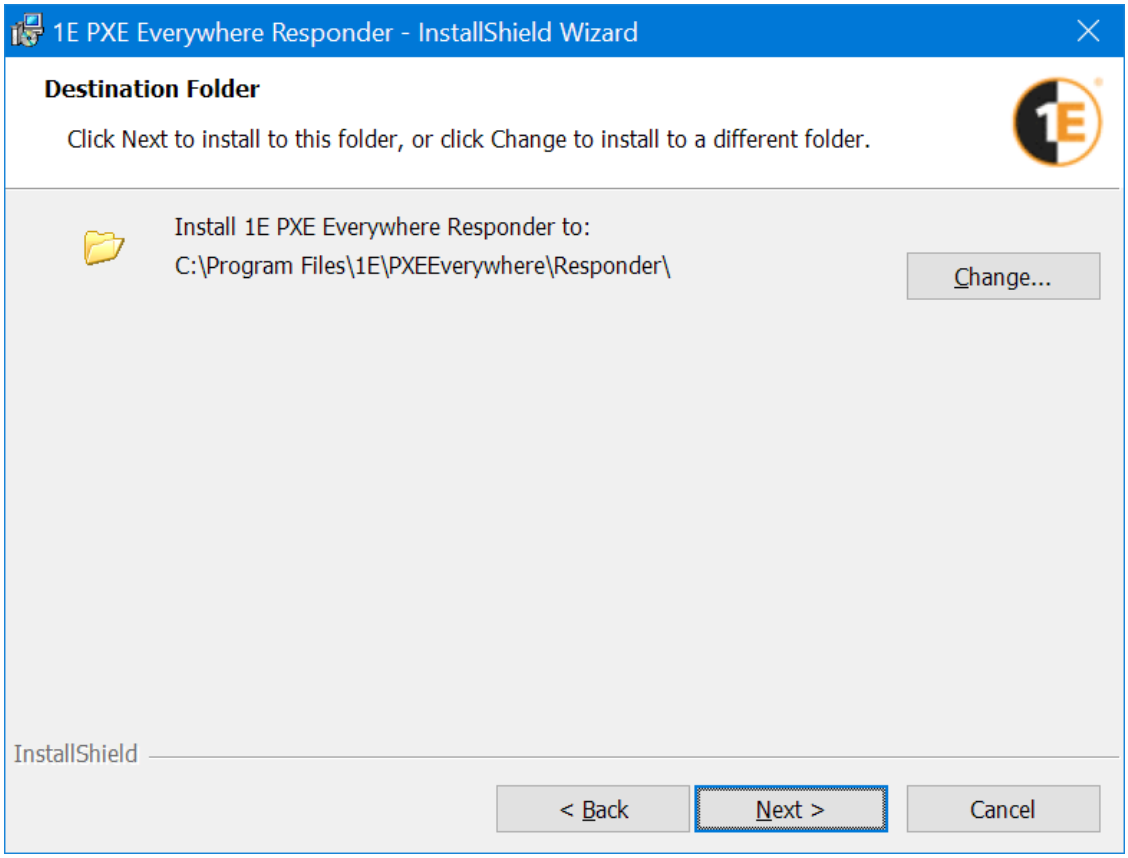
Click **Next** to go to the next screen.



12.2.3.2.1.1.3 Destination Folder

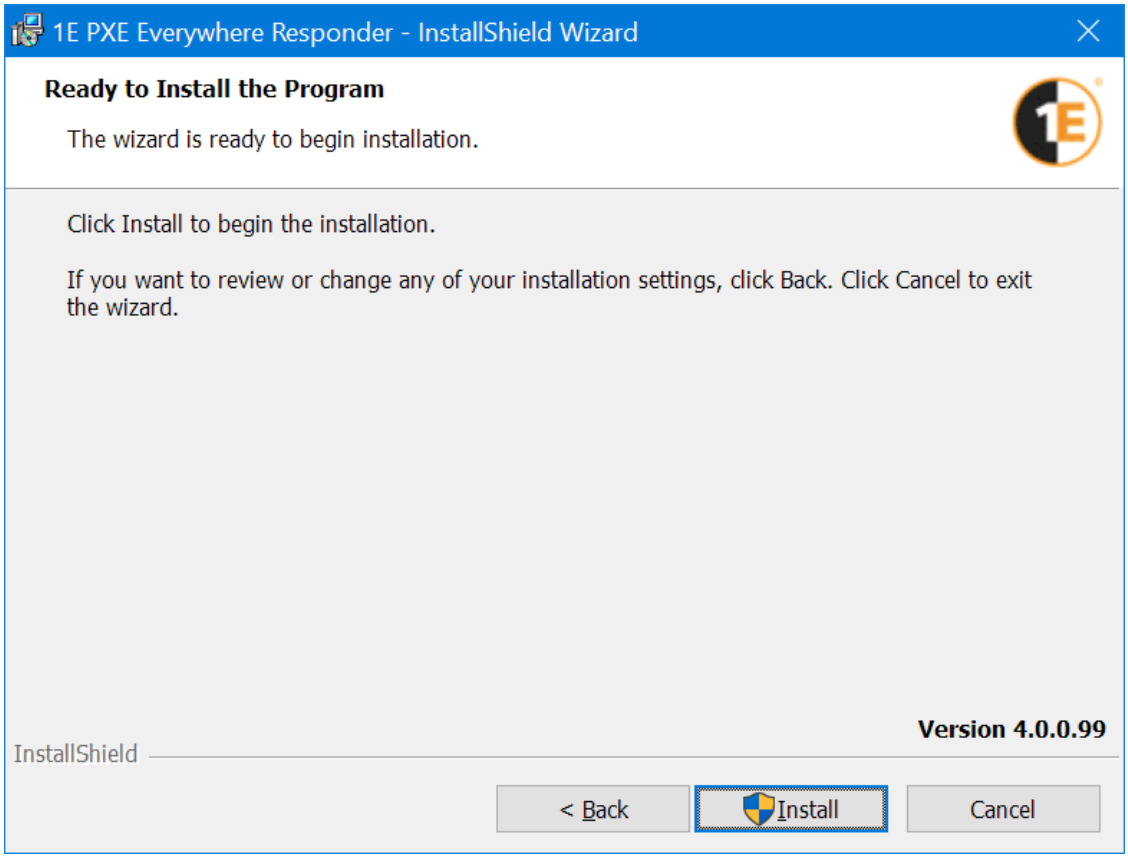
On this screen, you can set the destination folder for the installation. You can alter this from the default by clicking the **Change...** button and selecting a new folder.

Click **Next** to continue.



12.2.3.2.1.1.4 Ready to Install the Program

Click **Install** to start the PXE Everywhere Responder installation.

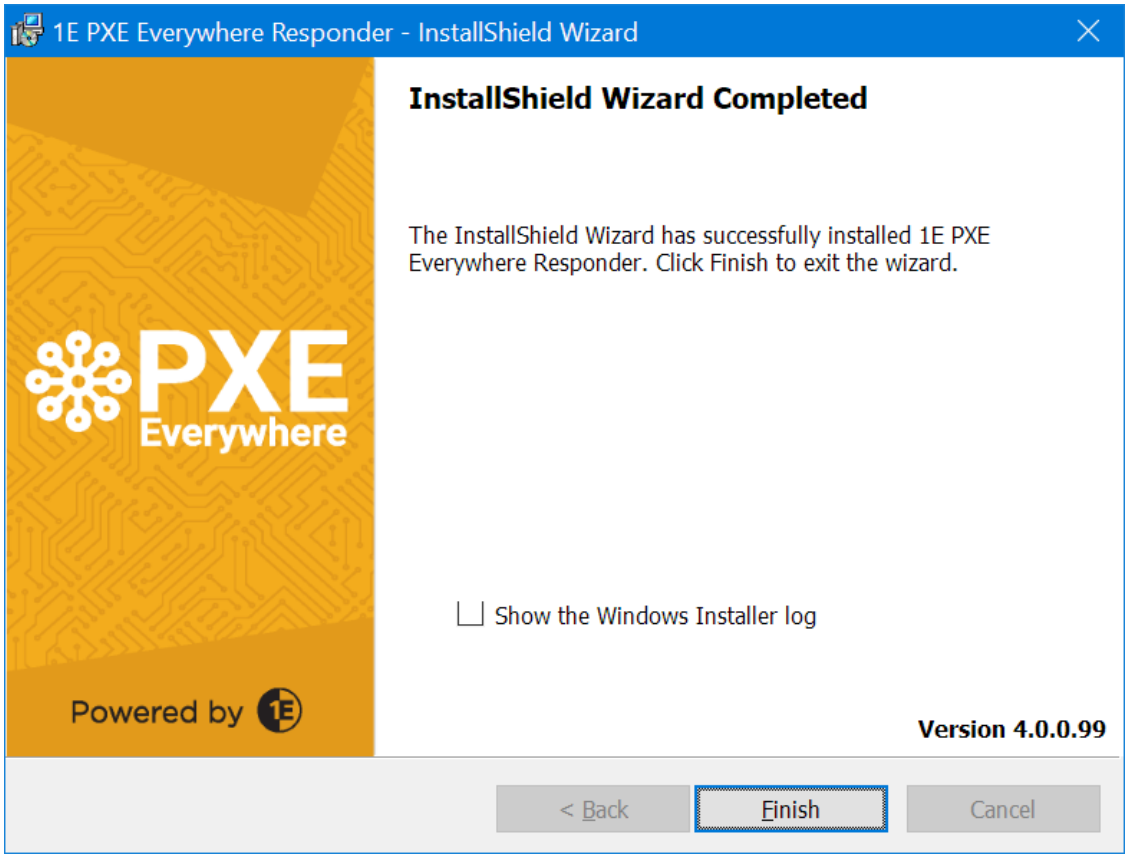


12.2.3.2.1.1.5 InstallShield Wizard Completed

This screen indicates whether the installation was a success or not. If any issues have been reported please refer to the troubleshooting section.

Here you can also optionally check to **Show the Windows Installer log**.

You can click **Finish** to close the installer.



12.2.3.2.1.2 Installing PXE Everywhere Responder without interaction

To install PXE Everywhere Responder without interaction, start a command prompt with elevated rights, using **Run as administrator** , change directory to the location where you downloaded **PXEEverywhereResponder.msi** and run the following suggested command-line:

```
msiexec /i PXEEverywhereResponder.msi /l*v PXEEverywhereResponder.log /qn
```

12.2.3.2.2 Next steps

To install the PXE Everywhere Central, please refer to Installing PXE Everywhere Central.

To install the PXE Everywhere Agents, please refer to Installing PXE Everywhere Agents .

Please refer to Verifying to verify your PXE Everywhere implementation.

12.2.3.3 Installing PXE Everywhere Agents

How to use the 1E Client Deployment Assistant (CDA) to create a Configuration Manager Applications to deploy PXE Everywhere Agents with Microsoft ADK files. Before you begin installation, please ensure you have reviewed Design Considerations and Requirements pages, and the installation steps below.

PXE Everywhere client provides a light-weight PXE server that responds to PXE boot requests from the local subnet and serves boot files to requesting PXE clients. It must therefore be installed on at least one client in

each subnet where PXE booting is required, and preferably installed on all PCs in your environment, thereby providing maximum availability (redundancy) and scalability (load-balancing) for PXE boot requests.

CDA is the recommended method of installing and upgrading PXE Everywhere Agent with Microsoft ADK files. The steps below are a summary of how you use CDA to deploy PXE Everywhere Agent with the Microsoft ADK files.

Please refer to Introducing 1E Client Deployment Assistant for full details of how to use CDA to deploy 1E Client with PXE Everywhere and optionally other 1E clients including Nomad, Shopping, WSA, Tachyon, WakeUp and NightWatchman. CDA is provided as a zip file that can be downloaded from the Nomad area of the 1E Support Portal.

If you are not using CDA, then you will need to:

Deploy the MSI separately and include PXE Everywhere Agent settings on the command-line or in an MST transform

Deploy ADK file as described in Deploying Microsoft ADK files.

Please ensure you have reviewed all Requirements before installing.

After you have deployed the Agent and ADK files, you will then need to prepare and deploy boot image(s) using Preparing and deploying 1E PXE Everywhere boot images.

12.2.3.3.1 Microsoft ADK files

In addition to the binaries supplied by 1E, PXE Everywhere Agent requires a number of files that are distributed and licensed with the Microsoft Windows Automated Deployment Kit (ADK). The required files are listed in the table opposite, along with the location on the PXE Everywhere Agent that they need to be installed to.

As these files are licensed by Microsoft, 1E are unable to include them in the installation media. However, you can use theIntroducing 1E Client Deployment Assistant to extract the required files from the ADK, create an installer transform and prepare an Application in Configuration Manager that will install the PXE Everywhere Agent with the appropriate settings and the additional Microsoft files.

The Windows Assessment and Deployment Kits (ADK) normally exist on the Configuration Manager CAS or Primary Site server, although they can be downloaded separately from the Microsoft website.

File	Destination Location (relative to TFTPROOT)
boot.sdi	*\boot.sdi*
abortpxe.com	*\boot\x86\abortpxe.com*
bootmgr.exe	*\boot\x86\bootmgr.exe*
pxeboot.com	*\boot\x86\pxeboot.com*
pxeboot.n12	*\boot\x86\pxeboot.n12*
bootmgfw.efi	*\boot\x86\bootmgfw.efi*

File	Destination Location (relative to TFTPROOT)
\boot\x64\bootmgfw.efi	
wgl4_boot.ttf (optional)	*\boot\fonts\wgl4_boot.ttf*

12.2.3.3.2 Installing PXE Everywhere Agents

The PXE Everywhere Agent is a client module in 1E Client, and is installed using the 1EClient installer (1EClient.msi).

> **Note**
>
> The PXE Everywhere Responder and PXE Everywhere Agent cannot co-exist on the same computer and are not supported together. Whilst it is possible to install them together, they will not work and will have issues such as failure to bind to ports.
>
> To install a Responder on the same computer as 1E Client then you must disable the client module for PXE Everywhere Agent. For an existing installation of 1E Client, reconfigure the client by setting **Module.PXEEverywhere.Enabled=false**. When installing or upgrading 1E Client on a computer that has or will have a Responder, then you must add **MODULE.PXEEVERYWHERE.ENABLED=false** to the installer command line or edit the **mst** transform.

12.2.3.3.2.1 Preparing a Configuration Manager Application for PXE Everywhere Agent using the 1E Client Deployment Assistant

The 1E Client Deployment Assistant (CDA) is used to create an Application in Configuration Manager that installs the PXE Everywhere agent with the appropriate settings and also adds the required Microsoft boot files from the Windows Automated Deployment Toolkit (ADK).

First download and extract the latest version of the1E Client Deployment Assistant (CDA) from the 1E Support Portal https://support.1e.com/.

Also check the 1E Support Portal to see if there are any Hotfixes for PXE Everywhere. Download the latest Accumulated Hotfix (Patch) and extract its MSP file to include in the CDA folder structure.

The following is a summary of steps described in PXE Everywhere settings but *only* for deploying PXE Everywhere Agent.

Right-click the extracted **1EClientDeploymentAssistant.exe** and select **Run as administrator**

On the **Welcome** screen click **Next**

On the **License Terms** screen accept the license and click **Next**

On the **ConfigMgr Connection** page

If you are running this on the CM site server select **Local ConfigMgr Site Server**

Otherwise, select **Remote ConfigMgr Site Server** and

Enter the site server name and username and password that should be used to connect to the CM site. In a multi-site hierarchy, enter the name of the CAS site server.

Click **Connect** to test the connection. Once connected, click **Next**

On the **General Settings** screen

Enter a UNC paths for Application Content Source and Package Content Source. The wizard will create a 1E\PXE Everywhere\4.0.x.x folder in these locations that will become the source for the CM Application Deployment Type.

Do not check the Distribute Content checkbox (we'll do that later). Click **Next**

On the **Agent Selection** screen, uncheck all products except **1E Client x.x** Click **Next**

On the **1E Client x.x** screen, uncheck **Create Package** and leave the remaining settings as is. Click **Next**

On the **Tachyon and the other client settings** screen, uncheck **Enable Tachyon** *and* all the other options. Click **Next**

On the **Nomad client settings** screen, uncheck **Enable Nomad** (which will disable all the other options). Click **Next**

On the **PXE Everywhere Settings** screen

Enter the location of the Windows ADK (the wizard needs to extract Microsoft files from the ADK and add them to the application source). If you are running the wizard on the CM site server, the ADK should be installed in C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit.

Modify the **PXE Everywhere Central web service URL**, replacing **pxe.contoso.com** with the FQDN of your PXE Everywhere Central web server

Check **Enable support for DHCP Snooping** *only* if you are also deploying PXE Everywhere Responders

Click **Next**

On the **Summary** screen, review the settings and click **Create**. The wizard will generate a transform MST file that includes all the custom properties and a CAB file that includes the files extracted from the ADK. It will then create a Collection, Application and Deployment in Configuration Manager.

When the wizard completes, click **Finish**

12.2.3.3.2.2 Verify Configuration Manager objects

Confirm that the application source files include the following, after which you can distribute to **Distribution Points**.

The 1E Client installer

An installer transform MST file

Files extracted from the Windows ADK.

In the Configuration Manager Admin Console, you should confirm that CDA has created:

An Application named **1E Client x.x**

A Collection named **1E Client x.x - Required**

Required Deployments for the 32-bit and 64-bit Deployment Types to the **1E Client x.x** Collection.

Please refer to Configuration Manager objects.

12.2.3.3.2.3 Deploying the 1E Client enabled PXE Everywhere Agent

You will need to distribute application source to Distribution Points.

Once distributed, simply add devices to the **1E Client x.x - Required** Collection in order to deploy the Agent to those devices.

12.2.3.3.3 Next steps

Please refer to Verifying to verify your PXE Everywhere implementation.

Prepare and deploy the boot image using Preparing and deploying the PXE Everywhere boot images.

12.2.3.4 Upgrading PXE Everywhere

Guidance for upgrading PXE Everywhere.

> **Note**
>
> The previous names **PXE Everywhere Local** and **PXELite** have been replaced by **PXE Everywhere Agent** which is a client module in **1E Client**. Please refer to Name changes introduced in PXE Everywhere 4.0 for full details including changes to log files.

Overview:

Review Requirements and read through the process below to understand what is involved.

Upgrade PXE Everywhere Central.

Upgrade or install PXE Everywhere Responders to support subnets where DHCP is blocked.

Deploy 1E Client with PXE Everywhere enabled.

Update Task Sequences.

> **Note**
>
> If you are implementing DHCP Snooping for the first time, at the same time as upgrading an existing implementation of PXE Everywhere, then:

please refer to guidance provided in Design Considerations - Infrastructure requirements regarding deployment of PXE Everywhere Responder(s) and configuring additional DHCP Relays (IP helpers)

on computers where 1E Client with PXE Everywhere module is installed, you must change the inbound firewall port from 67 to 2067 (or different custom port)

please refer to Known issues: Issues installing PXE Everywhere Responder regarding:

PXE Everywhere Agent and PXE Everywhere Responder are not supported on the same computer

Installing PXE Everywhere Responder on a legacy PXE Everywhere Agent that was previously installed with support for DHCP Snooping enabled - also see note below.

12.2.3.4.1 Upgrading to PXE Everywhere 8.1

The process for upgrading PXE Everywhere is:

On the PXE Everywhere Central server, perform any necessary pre-upgrade steps

Always make a backup of *web.config* file if any custom changes have been made to the default settings in it.

Ensure that any custom settings that have been modified in the PXELite Application pool are captured.

Create a backup of stored procedures deployed by the PXE Everywhere central installer if any custom changes are made to them.

Upgrade the PXE Everywhere Central components by following the steps described in Installing PXE Everywhere Central.

> **Note**
>
> Different versions of PXE Everywhere Central cannot co-exist on the same server.

Perform any necessary post-upgrade steps

Restore the backup of *web.config* file if any custom changes were made to the default settings prior to upgrade.

Perform modifications to any custom settings that were modified in the PXELite Application pool prior to upgrade.

Restore the backup of customized stored procedures that were created prior to upgrade.

> **Note**
>
> Some changes mentioned above require an IIS reset before they come into effect.

Verify the PXE Everywhere Central functionality by following the steps described in Verifying - PXE Everywhere Central.

If you are implementing in an environment that has DHCP blocked (for example using DCP Snooping), and you have existing Responders, they can be upgraded using the steps for Installing PXE Everywhere Responder.

> **Note**
>
> PXE Everywhere Responder v4.0 and later has its own installer, which can be used to upgrade the **Static Responders**. Previous versions of Responders (also known as Static Responders) are legacy PXE Everywhere Agents configured in Responder mode, with its DHCP Port fixed at 67.
>
> The PXE Everywhere Responder can also be used to upgrade a **normal Agent** to function as a new Responder. A known issue exists *if* the previous Agent had support for DHCP Snooping enabled. Then you will need to forcibly change its DHCP port back

to 67 by including DHCPPORT=67 as a command-line installer property when installing the Responder. You can optionally include this installer property when installing or upgrading other scenarios.

Upgrade all the PXE Everywhere Agents to the latest version by following the steps for Installing PXE Everywhere Agents.

Note

All Agents on a subnet must be upgraded together. Different versions of PXE Everywhere Agent cannot co-exist on the same subnet.

Warning

Introducing 1E Client Deployment Assistant is the recommended method of installing and upgrading PXE Everywhere Agent.

If you deployed the legacy PXE Everywhere Agent using a previous version of Client Deployment Assistant (CDA) then you should upgrade using the latest version of CDA. If you upgrade a CDA installation using the MSI, for example in a test lab, then the boot files (ADK files and boot image) will not be migrated to the new location used by the 1E Client's PXE Everywhere Agent, and you will need to deploy the ADK files and boot image as post-install tasks, as described in Deploying Microsoft ADK files.

Update any Task Sequences used to stage 1E PXE Everywhere boot images, with the new path for running **CreateBCD.exe**.

Note

Please refer to Preparing and deploying 1E PXE Everywhere boot images. The legacy PXE Everywhere Agent was only x86 therefore had different paths for x64 and x86 platforms. PXE Everywhere Agent in 1E Client has separate installers for x86 and x64, and only uses one path, and does not require any OS conditions. Existing Task Sequences will have two stage boot image steps:

Stage boot image (x64 systems)

Stage boot image (x86 systems)

Edit the Task Sequence (or a clone) as follows:

Delete one of the above steps, and edit the other remaining step

Change its name to **Stage boot image**

Change the command line as shown in the table below

Remove the existing conditions - click **Options** tab and **Remove All**

Click **OK** to save the Task Sequence

Platform	Legacy	New command-line
x64	"%ProgramFiles(x86)%\1E\PXE Lite\Server\x64\CreateBcd.exe"	"%ProgramFiles%\1E\Client\Extensibility\PXEEverywhere\CreateBcd.exe"
x86	"%ProgramFiles%\1E\PXE Lite\Server\i386\CreateBCD.exe"	

Deploy the updated/cloned Task Sequence to the 1E Client Collection as described in Preparing and deploying 1E PXE Everywhere boot images: Deploy the Task Sequence to stage a boot image.

You do not need to update boot images.

Update other OS Deployment Task Sequences to use the new 1E PXE Everywhere boot images.

12.2.3.4.2 Next steps

Please refer to Verifying to verify your PXE Everywhere implementation.

Prepare and deploy the boot image using Preparing and deploying 1E PXE Everywhere boot images.

12.2.3.4.3 Name changes introduced in PXE Everywhere 4.0

	PXE Everywhere Central	PXE Everywhere Responder	PXE Everywhere Agent			
MSI Name	PXELiteCentral.msi	PXE EverywhereCentral.msi	PXELiteLocal.msi	PXEEverywhereResponder.msi	PXELiteLocal.msi	1EClient.msi

	PXE Everywhere Central	PXE Everywhere Responder	PXE Everywhere Agent			
Program Files folder	1E\PXE Lite	1E\PXE Everywhere	1E\PXE Lite\Server	1E\PXEEverywhere\Responder	1E\PXE Lite\Server	1E\Client\Extensibility\PXEEverywhere
ProgramData Folder	1E\PXELite	1E\PXEEverywhere	1E\PXELite	1E\PXEEverywhere	1E\PXELite	1E\PXEEverywhere
Log File Name	WebService.log	WebService.log	PXELiteServer.log	PXEEverywhereResponder.log	PXELiteServer.log	PXEEverywhere.log
HKLM\SOFTWARE Registry	1E\PXELiteCentral	1E\PXELiteCentral	1E\PXELiteServer	1E\PXELiteServer	1E\PXELiteServer	1E\PXEEverywhere
Service Display name	n/a	n/a	1E PXE Lite Server	1E PXE Everywhere Responder	1E PXE Lite Server	1E Client
Service name	n/a	n/a	PXELite Server	PXEEverywhereResponder	PXELite Server	1EClient
IIS Site	PXELite	PXELite	n/a	n/a	n/a	n/a

12.2.4 Verifying

Basic verification tests for PXE Everywhere.

12.2.4.1 Log files

PXE Everywhere component	Folder	Log file
1E Client	C:\ProgramData\1E\Client	1E.Client.log
PXE Everywhere Central	C:\ProgramData\1E\PXELite	WebService.log

PXE Everywhere component	Folder	Log file
PXE Everywhere Responder	C:\ProgramData\1E\PXEEverywhere	PXEEverywhereResponder.log
PXE Everywhere Agent	C:\ProgramData\1E\PXEEverywhere	PXEEverywhere.log

Please also refer to Upgrading PXE Everywhere: Name changes introduced in PXE Everywhere 4.0.

If the issue is related to PXELite boot media creation/updating using CreateBootImage.exe then please provide:

C:\Program Files (x86)\Microsoft Configuration Manager\AdminConsole\AdminUILog\CreateTsMedia.log

If the issue is related to the deployment of PXELite boot image into the TFTP folder of PXELite agent then please provide:

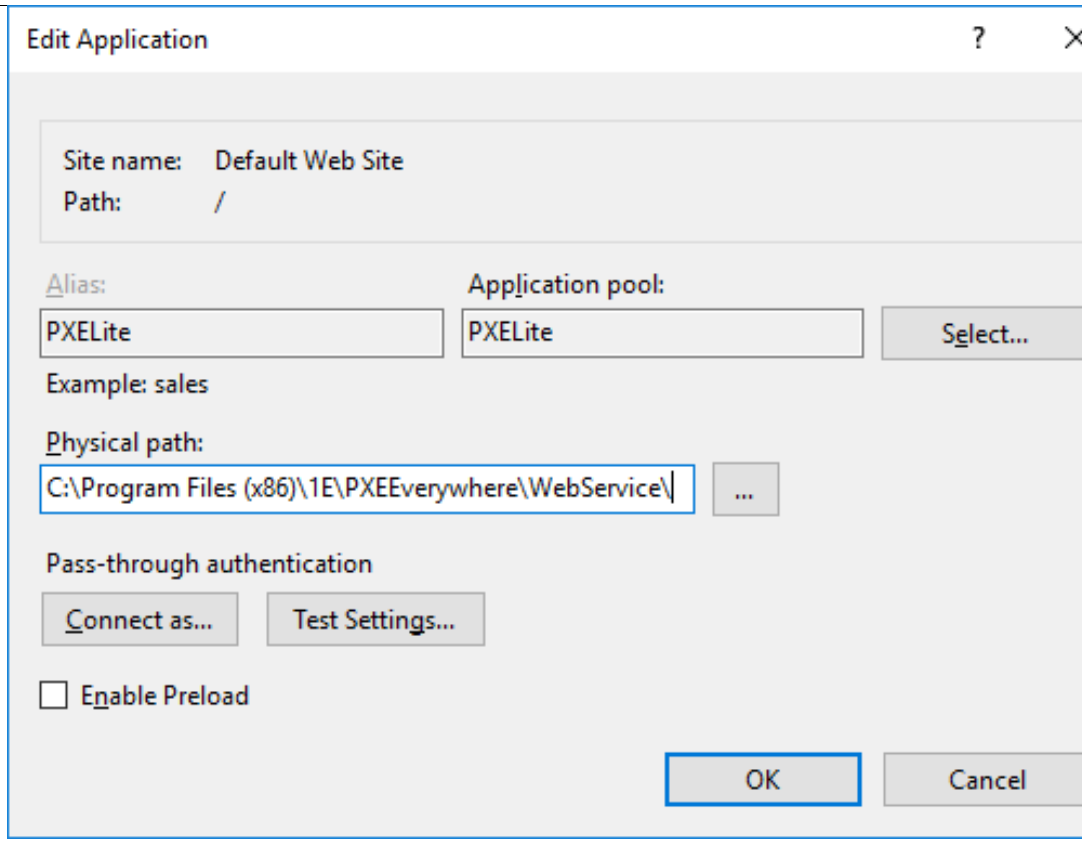
C:\ProgramData\1E\PXElite\CreateBCD.log

12.2.4.2 PXE Everywhere Central

If you get unexpected errors when using PXE Everywhere the following simple checks can be performed to confirm that the installation has been successful and that the appropriate permissions are present for the network service account:

Checks	Notes
PXE Everywhere installation directory	PXE Everywhere Central is a 32-bit application, and is only supported on the 64-bit server OS listed in Requirements. By default will install its files to the following location on 64-bit systems: `C:\Program Files (x86)\1E\PXEEverywhere`
Web Application and Application pool	Under **Default Web Site**, check that there is a web application named **PXELite**. Its physical path is the PXE Everywhere ***WebService*** directory in the PXE Everywhere installation directory. Its application pool is also called **PXELite** and uses the *NetworkService* identity.

Checks	Notes



Web service

You can use the PXE Everywhere configuration web service to check for correct installation. To do this run the following steps on the server where the PXE Everywhere website is installed:

Browse to *http://localhost/PXELite/PXELiteConfiguration.asmx*. You should see a **PXE Everywhere configuration** web page.

Click **GetVersion** and select **Invoke**. You should see a new browser window with the result of the version query listed - note the version number and reference this when contacting 1E support.

Checks	Notes

	The above test can also be performed using the following PowerShell commands:
	`$pxecentral = "localhost";`
	`$pxeLite = New-WebServiceProxy -uri "http://$pxecentral/pxelite/PXELiteConfiguration.asmx?wsdl";`
	`$pxeLite.GetVersion();`

web.config	The *web.config* file is located in the following directory: `C:\Program Files (x86)\1E\PXEEverywhere\WebService` The *web.config* file *<connectionStrings>* section specifies the location of the Configuration Manager database. Ensure that this is correctly set.
Log file	The *web.config* file stores information about the location of the log file, which is typically: `C:\ProgramData\1E\PXEEverywhere\WebService.log` Review the log file for errors.
Configuration Manager Database	During the installation of PXE Central, the following stored procedures are added to the Configuration Manager database: **1E_GetPXEAction** **1E_ProcessNBSMessage** To allow these stored procedures to be executed by the PXE Lite Application Pool running on the PXE Central Server, the installer also creates a new SQL login as a user of the Configuration Manager database. The name of the SQL login depends on where PXE Everywhere Central is installed in relation to the Configuration Manager database.

Checks	Notes
	NT AUTHORITY\NETWORK SERVICE- if PXE Everywhere Central is installed on the same sever as the Configuration Manager database **<DOMAIN>\<SERVER$>**- if installed on a different server, then DOMAIN\SERVER$ is the name of the server on which PXE Everywhere Central is installed This SQL Login is not assigned any roles on the ConfigMgr database, but is explicitly granted the following privileges on the 1E stored procedures and other objects in the database:

Type	Name	Permission(s)
Stored Procedure	**dbo.1E_GetPXEAction**	Execute
Stored Procedure	**dbo.1E_ProcessNBSMessage**	Execute
Stored Procedure	dbo.spProcessNBSMessage	Execute
Table	dbo.SetupInfo	Select
Table	dbo.UnknownSystem_DISC	Select

Note

When a PXE Everywhere Agent receives a PXE boot request from a peer, it will contact the PXE Everywhere Central web service, which in turn will execute the 1E_GetPXEAction stored procedure in the ConfigMgr database to determine if a Task Sequence has been advertised to the PXE-booting client, returning the results to the PXELite Local computer.

1E_GetPXEAction is responsible for returning the ConfigMgr OfferID (AdvertID, DeploymentID), BootImageID and whether the offer is mandatory or not. 1E_ProcessNBSMessage is used to set the PXE flag for required deployments. This is so that if PXE is the first in the boot order, it will not go into a perpetual PXE reboot loop.

PXE Everywhere Boot Action	The following test confirms the connection between PXE Everywhere Central and Configuration Manager. First, you need to confirm the test workstation is a known client in ConfigMgr and read its properties to get its MAC Address.

Checks	Notes

	Run the following PowerShell command using the workstation MAC Address, toreport whether it is targeted by a Task Sequence.
	
	Specify the IPv4 MAC Address in the format "A1-B2-C3-D4-E5-F6". If you are running the test on the PXE Everywhere Central server, then specify the server name as *localhost*, otherwise specify the FQDN of the server or its DNS Alias.
	
	`$macAddress = "<macaddress>"`
	`$pxecentral = "<PXE_Everywhere_Central_Servername_or_Alias>";`
	`$pxeLite = New-WebServiceProxy -uri "http://$pxecentral/pxelite/PXELiteConfiguration.asmx?wsdl";`
	`$pxeLite.GetBootAction("","$macAddress",[ref]$false)`
	
	If the workstation is not targeted, then a blank is returned.
	
	If the workstation is targeted, then the ConfigMgr package ID is returned for the boot image associated with the task sequence.

12.2.4.3 PXE Everywhere Agents

Ensure that PXE Everywhere Central is operational, and any Responders if you are using them.

Verify the PXE Everywhere Agent functionality:

Check the PXE Everywhere Agent logs, typically at *%PROGRAMDATA%\1E\PXEEverywhere*, and make sure there are no errors.

PXE boot a few test machines to ensure that PXE Everywhere is working properly.

Verify that boot files (Microsoft ADK files and 1E PXE Everywhere boot images) have been correctly deployed to PXE Everywhere Agents.

File	Destination Location (relative to TFTPROOT)
boot.sdi	*\boot.sdi*
abortpxe.com	*\boot\x86\abortpxe.com*
bootmgr.exe	*\boot\x86\bootmgr.exe*
pxeboot.com	*\boot\x86\pxeboot.com*
pxeboot.n12	*\boot\x86\pxeboot.n12*
bootmgfw.efi	*\boot\x86\bootmgfw.efi*

File	Destination Location (relative to TFTPROOT)
\boot\x64\bootmgfw.efi	
wgl4_boot.ttf (optional)	*\boot\fonts\wgl4_boot.ttf*

The 1E PXE Everywhere boot images should be found in an \Images folder relative to TFTPROOT.

Finally, target a PXE Client with an OS deployment task sequence (for example bare-metal), and observe the OS installation process end-to-end.

> **Note**
>
> When PXE booting a UEFI device in a non-mandatory deployment scenario, you may be presented with an option to
> **Press Enter to continue and Press F8 for Advanced boot menu**. However, the advanced boot menu options will not work for WinPE.

12.3 Using PXE Everywhere

How to administer and maintain the PXE Everywhere system. PXE Everywhere provides the ability to network boot PCs from peer PCs instead of Configuration Manager PXE Service Points (a Configuration Manager PXE Service Point is a Distribution Point with the PXE role enabled). Using PXE Everywhere removes the overhead of supporting dedicated PXE servers on branch networks.

12.3.1 Preparing and deploying 1E PXE Everywhere boot images

Steps for creating and staging 1E PXE Everywhere boot images.

All PXE Everywhere Agents require a x64 boot image at least, and another for x86 if you are also serving x86 platforms. These 1E boot images will be referenced in your OS Deployment Task Sequences, and are based on Configuration Manager boot images.

The following example process is for x64 but also applies to x86. Each boot image requires its own Task Sequence to stage it on *all* PXE Everywhere Agents. While 1E Client with PXE Everywhere Agent enabled has installers for x64 and x86, both platforms must be staged with both boot images, to serve both types of PXE client platform. You would only ignore x86 if you are sure you are not serving x86 platforms.

There are two main steps to configure a 1E PXE Everywhere boot image:

Creating the 1E PXE Everywhere boot images

Stage a 1E PXE Everywhere boot image.

12.3.1.1 Prerequisites

A computer with the **Configuration Manager console** and the **PXE Everywhere Admin Tools** installed.

Configuration Manager requires its Windows PE boot images to present a client authentication certificate. Configuration Manager automatically adds the certificate when deploying images to native Configuration

Manager PXE servers, but you need to manually add the certificate to each 1E PXE Everywhere boot image before deployment to PXE Everywhere Agents.

1E tool	Where to find it	What it does
UpdateBootImage	Included in the PXE Everywhere Admin Tools. The PXE Everywhere Admin tools can be installed using the PXE Everywhere Central installer, on any computer that has the Configuration Manager Admin Console. Please refer to Installing PXE Everywhere Central. The PXE Everywhere Central installer is provided in the **PXE Everywhere downlo ad zip** available from the Nomad download area of the 1E Support Portal.	This tool is used to update Windows PE boot images for use with PXE Everywhere. It uses the native Configuration Manager API to add a certificate, and update the **variables.dat** file included in the image. When the PXE client loads the boot image, the Configuration Manager executables load the encrypted variables file and attempt to connect to the specified Management Point.The tool takes advantage of a boot image reload feature introduced in Configuration Manager 1706 CB, which enables you reload the latest version of Windows PE (from the Windows ADK installation directory) into the boot image when you run the **Update Distribution Points** wizard. **Note** Whenever you reload the boot image while running the **Update Distribution Points** wizard, for example to replace a certificate that is about to expire, you must then re-run **UpdateBootImage.exe** to ensure the 1E components and settings are installed in the reloaded boot image. **Note** To include a client certificate, it must be provided as a PFX file in a Public Key Certificate Standard (PKCS #12) format, with private key exportable, and a known password. For details of CM certificates please refer to **Boot images for deploying operatin g systems** in PKI certificate requirements for System Center Configuration Manager

1E tool	Where to find it	What it does
		(https://docs.microsoft.com/en-us/mem/configmgr/core/plan-design/network/pki-certificate-requirements.
UpdateBootImage GUI	Included in the **PXE Everywhere download zip** with the installers for PXE Everywhere Central and Responder. **Note** Use v1.0.0.6 with PXE Everywhere 4.0	This tool provides a GUI where a user defines the parameters required by the **UpdateBootImage** tool. When executed it copies a command-line to the clipboard, which you then copy into an elevated command prompt and execute it. The tool is provided to reduce the chance of errors when typing in the long command-line required by the UpdateBootImage tool. The executable name is **1E.PS.UpdateBootImageGUI.exe** and requires .NET Framework 4.5 or later.
CreateBCD	Included in the installation of **1E Client** with PXE Everywhere enabled.	This tool is run by a **Stage boot image** Task Sequence on PXE Everywhere Agents to copy the 1E PXE Everywhere boot image referenced by the Task Sequence to the Images folder in the Agent's TFTPTOOT, configure a suitable TFTP Block Size, and create a boot configuration database on the Agent. CreateBCD only works within the context of a Configuration Manager task sequence. It will run outside a Task Sequence but have no effect. **Warning** **CreateBCD** does not validate the boot image - it will not detect a corrupt .wim file.

For full details of available command-line parameters for **UpdateBootImage.exe**, and **CreateBCD.exe** please refer to PXE Everywhere tools.

12.3.1.2 Creating the 1E PXE Everywhere boot images

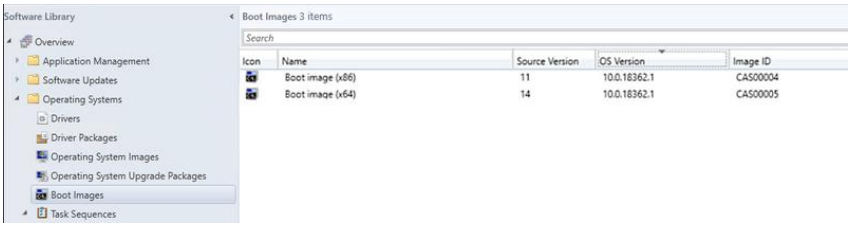
The 1E PXE Everywhere boot image is copied from an existing Configuration Manager boot image, and then modified using **UpdateBootImage** to add the required certificate, and configure other settings.

> **Note**
>
> In most environments only a x64 boot image will be required. If you are managing x86 devices you will also need to prepare a PXE Everywhere boot image for x86, by repeating all the steps for x86.

12.3.1.2.1 Copy an existing boot image

Use the following process to copy your existing production boot image ready for modification.

On the Configuration Manager site server, open the Configuration Manager Admin Console and from the **Software Library** workspace expand **Operating Systems > Boot Images**.



Right-click the current **Boot image (x64)** and select **Properties**, then select the **Data Source** tab to identify the location of the current boot image.

Open that location in Windows explorer and copy the boot.wim file to a folder in a shared location accessible to the CM site server (the location must be accessible using a UNC path and the folder should only contain the boot.wim file). If you have a content source share already created on the site server, that would be an ideal location to create the new folder and copy the boot.wim to.

> **Note**
>
> PXE Everywhere requires that the boot image is called **boot.wim** so you should ensure that your copy has this name.

In the Configuration Manager console, right-click the **Boot Images** node and select **Add Boot Image**.

In the **Add Boot Image Wizard** on the **Data Source** screen enter the UNC path to the copied boot image and click **Next**.

On the **General** screen, add the **Name** - for example **1E PXE Everywhere boot image (x64) -** version and any relevant comments you want to include and click **Next**.

On the **Nomad Settings** screen (if Nomad Branch Admin UI Extensions have been installed), select **Enable Nomad** and click **Next**.

Click **Next** on the following screens to complete the wizard.

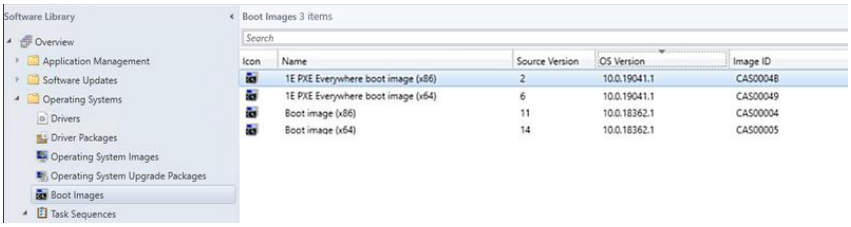
Right-click the new boot image and select **Properties**.

Select the **Drivers** tab and add any required network or storage drivers required to support your production systems, then click **OK**.

Right-click the new boot image and select **Distribute Content** to start the **Distribute Content Wizard**. Add the boot image to a local Distribution Point.

> **Note**
>
> This step is required before you can update the boot image with a certificate.

If you are serving x86 platforms, repeat the above steps to create boot image **1E PXE Everywhere boot image (x86)**.



> **Note**
>
> To inject a certificate into each boot image proceed with the steps under the heading Update a 1E PXE Everywhere boot image.
>
> Later you will create a deployment to Stage a 1E PXE Everywhere boot image on the PXE Everywhere Agents, so they can serve the PXE clients on their local subnets.

12.3.1.2.2 Update a 1E PXE Everywhere boot image

These update steps must be done on a computer that has the **Configuration Manager console** and the **PXE Everywhere Admin Tools** installed. The command-line uses **UpdateBootImage.exe** (installed with the **PXE Everywhere Central Admin Tools**) to mount the boot image, inject the client authentication certificate and unmount the boot image.

You will also need the certificate used for boot images, provided as a PFX file, and its password.

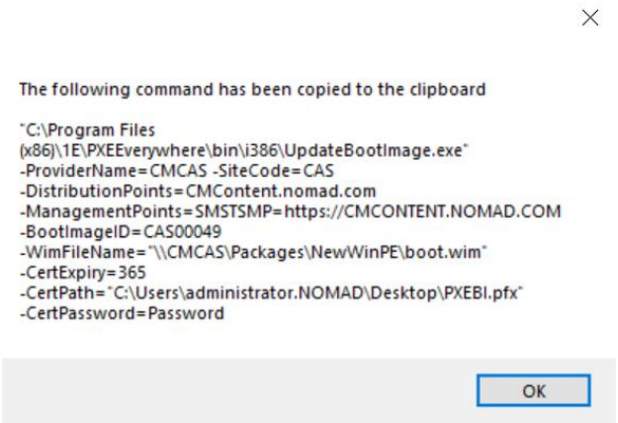
Extract the **UpdateBootImageGUI** tool and its supporting files from the download ZIP.

Open a command prompt (Run as Administrator), change the current directory to the ZIP extract folder, and run1E.PS.UpdateBootImageGUI.exe

Field	Details
SMSProvider Server	Enter the FQDN of the Configuration Manager Provider and hit the **Tab** key. Note that the **Site Code** field will now be populated with the site code.
Boot Image ID	Using the drop-down, select 1E PXE Everywhere boot image (x64) created earlier. Note the **WMI File Path\Name** field is automatically populated with the path to the **boot.wim** file.

Field	Details
Distribution Points	Select one of the Distribution Points that the boot image was previously added to.
Management Points	Select an available Management Point.
Certificate Expiry	Select an expiry date. This defaults to one year from today. This may be changed as required in a production environment. **Note** When the certificate is about to expire, this process will need to be repeated using a new certificate, and the updated boot images staged to all PXE Everywhere Agents.
PXEBoot Password	You can optionally set a boot password that would need to be entered by the user on the PXE client in order to load the Windows PE boot image and start any OS Deployment Task Sequence
Certificate Path	Enter the path to the PFX file that you exported earlier. This optional field is mandatory for injecting the certificate into the boot image.
Certificate Password	Enter the password for the specified PFX file. This optional field is mandatory!

Click the **Execute** button. The tool will display a dialog box similar to the following, indicating that the constructed **UpdateBootImage.exe** command line has been copied to the clipboard.



Start a command prompt (run as administrator)

paste the command line from the clipboard and execute

the process should complete within a couple of minutes and finish with **CreateBootMedia returns OK**.

Close the **UpdateBootImageGUI** program.

Return to the Configuration Manager console, right-click the new boot image and select **Update Distribution Points**. This will cause the boot image to be 'regenerated' and copied to the Distribution Point(s) that it was originally copied to.

If you are serving x86 platforms, repeat the above steps to update boot image **1E PXE Everywhere boot image (x86)**.

The 1E PXE Everywhere boot images are now ready to use in Task Sequences.

12.3.1.3 Stage a 1E PXE Everywhere boot image

Each PXE Everywhere boot image needs to be distributed to the PXE Everywhere Agents before they can be served to PXE clients. This is done using a custom Task Sequence that downloads the boot images then stages them in the TFTP folder structure from where the PXE client will download the relevant x64 or x86 boot image. Staging the boot images in the TFTP folder structure is done using **CreateBCD.exe**, which is installed on all PXE Everywhere Agents. CreateBCD.exe copies the deployed PXE Boot Image to the PXE Everywhere TFTP\Images folder and creates a boot configuration database (BCD file).

12.3.1.3.1 Create a Task Sequence to stage a 1E PXE Everywhere boot image

To distribute the boot image(s) to the correct locations on PXE Everywhere Agent computers, create a custom task sequence that will be deployed to the computers.

In the Configuration Manager console, from the **Software Library** work space, expand **Operating Systems**, right-click **Task Sequences** and from the context menu, choose **Create Task Sequence**.

On the first page of the **Create Task Sequence Wizard**, select **Create a new custom task sequence** and click **Next**.

> **Tip**
>
> **Nomad Settings** is only displayed when **Nomad Admin Console Extensions** is already installed on the Configuration Manager administration console computer you are using. If this is not present, then close the Configuration Manager Admin Console and install the Nomad Admin Console Extensions, and then create/edit the Task Sequence.
>
> If Nomad is installed on the Agent computers on which you'll be staging the boot image, then you should use Nomad to stage the boot images.

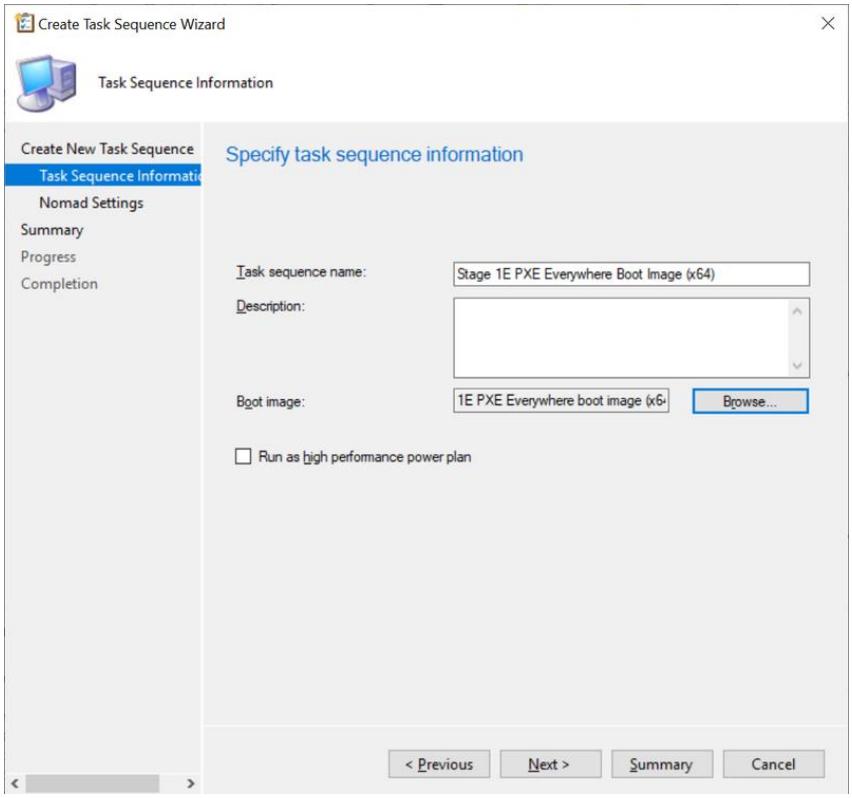
On the **Task Sequence Information** page, enter a suitable name for the Task Sequence, for example:

Stage 1E PXE Everywhere boot image (x64)

Stage 1E PXE Everywhere boot image (x86) - if you are serving x86 platforms

Click the **Browse** button and choose the boot image which you created earlier.

Click **Next**.

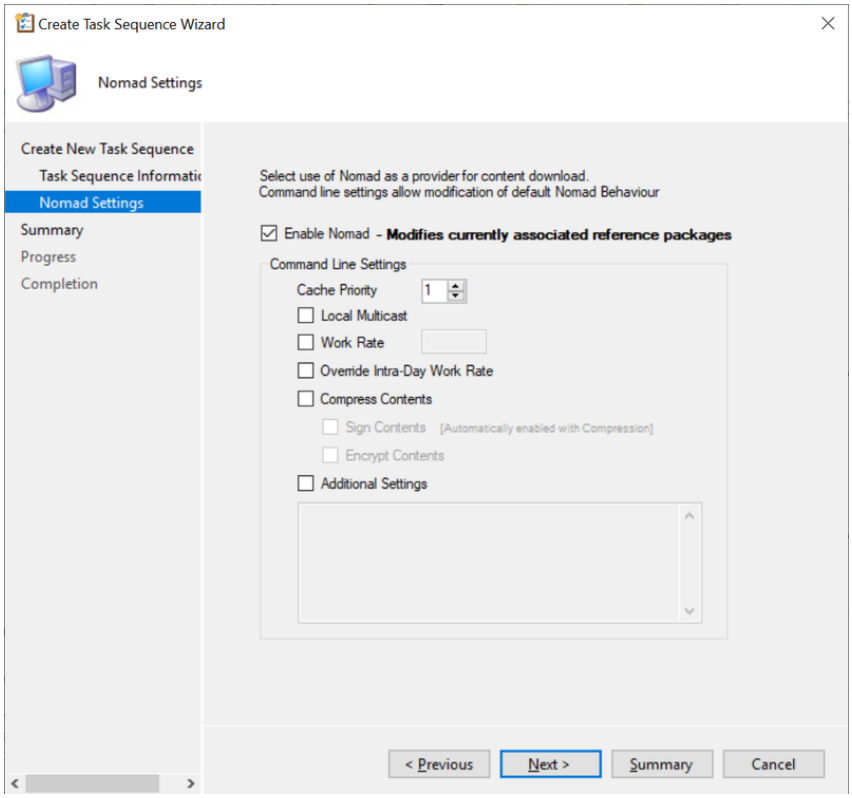


On the **Nomad Settings** page, select **Enable Nomad**.

> You may want to increase the **Cache Priority** from the default 1 to ensure the boot image remains in the cache if the cache is cleared to make space for other content.

Click **Next**.

> **Tip**
>
> Skip this step if you are not using Nomad.



On the **Summary** page click **Next**.

On the **Completion** page click **Close**.

Right-click the Task Sequence and select **Edit** to add tasks to the Task Sequence.

Add a task step to run **CreateBCD.exe** as follows.

From the Task Sequence editor, add a **Run Command Line** option with the following properties.

Property	Value
Name	Stage boot image
Command line	"%ProgramFiles%\1E\Client\Extensibility\PXEEverywhere\CreateBcd.exe" -tftpblocksize=8192

Tip

This command-line will work on x64 and x86 platforms, therefore you do not need to configure conditions.

If you are upgrading PXE Everywhere, you must remove the existing conditions - click **Options** tab and **Remove All**.

Legacy versions of PXE Everywhere Agent were x86 only, and required different command-lines for Agents on x64 and x86 platforms.

TFTP Block Size

Some hardware may not support block size values higher than 16384 bytes and hence may fail to PXE boot. We recommend you use a TFTP block size of 8192 bytes for best results.

An known issue has been observed on some Cisco switches when DHCP Snooping is enabled and a block size greater than 1471 is used. The issue is referenced in the following two Cisco bug reports. If you are affected by this Cisco issue, change the tftpBlockSize to 1471 or lower.

https://quickview.cloudapps.cisco.com/quickview/bug/CSCvk53444.

https://quickview.cloudapps.cisco.com/quickview/bug/CSCtw63707

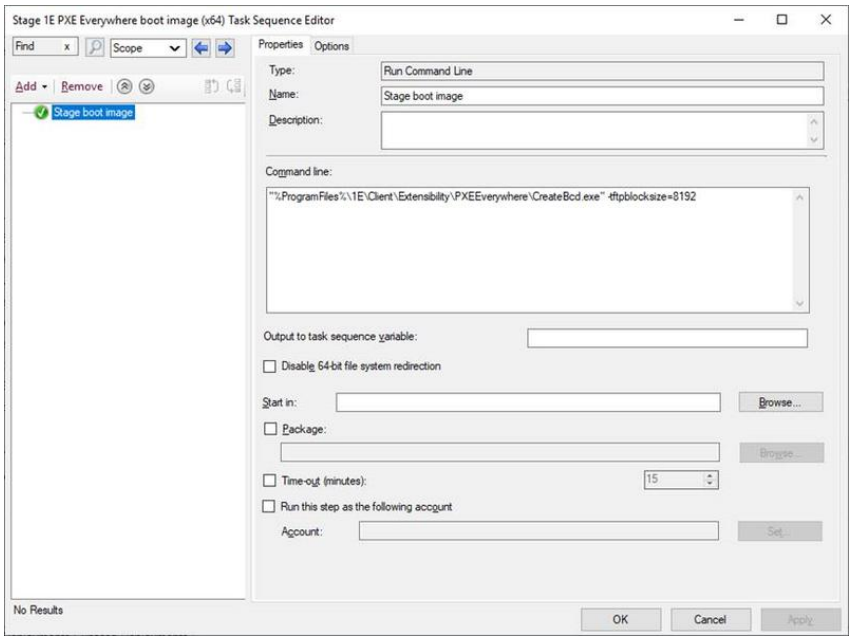
The issue may also be present in TP-Link switches.

The actual block size used for the tftp protocol is the lesser value of the **tftpBlockSize** and the **MaxBlockSize** registry values. Effectively, **MaxBlockSize** limits the **tftpBlockSize** specified in the **CreateBCD.exe** utility.

There is only one command-line switch for **CreateBCD.exe** which is used to set the **tftpBlockSize** for the RAMDisk (boot image). The notation for this is *`CreateBCD.exe -tftpBlocksize=blocksize`* where blocksize is measured in bytes.

Click **OK** to save the Task Sequence. The Task Sequence should now look like the picture opposite.

If you are serving x86 platforms, repeat the above steps to create Task Sequence **Stage 1E PXE Everywhere boot image (x86)**.



12.3.1.3.2 Deploy the Task Sequence to stage a boot image

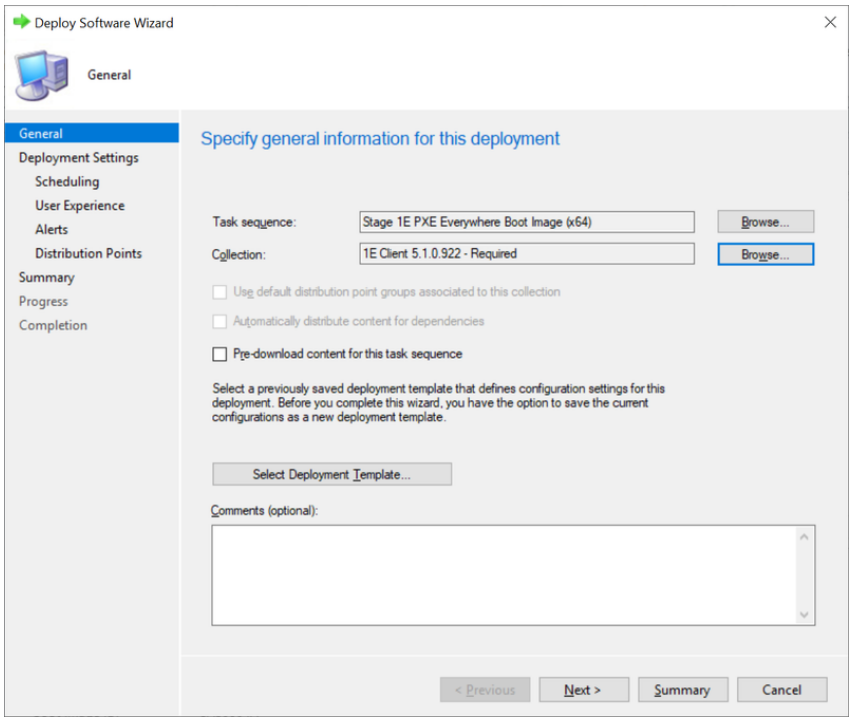
Each Staging Task Sequence must be deployed to all PXE Everywhere Agents. You will need to create a target Collection that includes all systems that have the 1E Client with PXE Everywhere enabled. You can use the same Collection that you used to deploy the 1E Client, such as the one

created by 1E Client Deployment Assistant (CDA). Or you can create a new Collection limited on the 1E Client Collection, or a query-based Collection.

From the Configuration Manager console, right-click the boot image staging Task Sequence and select **Deploy** to start the **Deploy Software Wizard**.

Browse for the target Collection - devices that already have 1E Client with PXE Everywhere enabled.

Click **Next**.

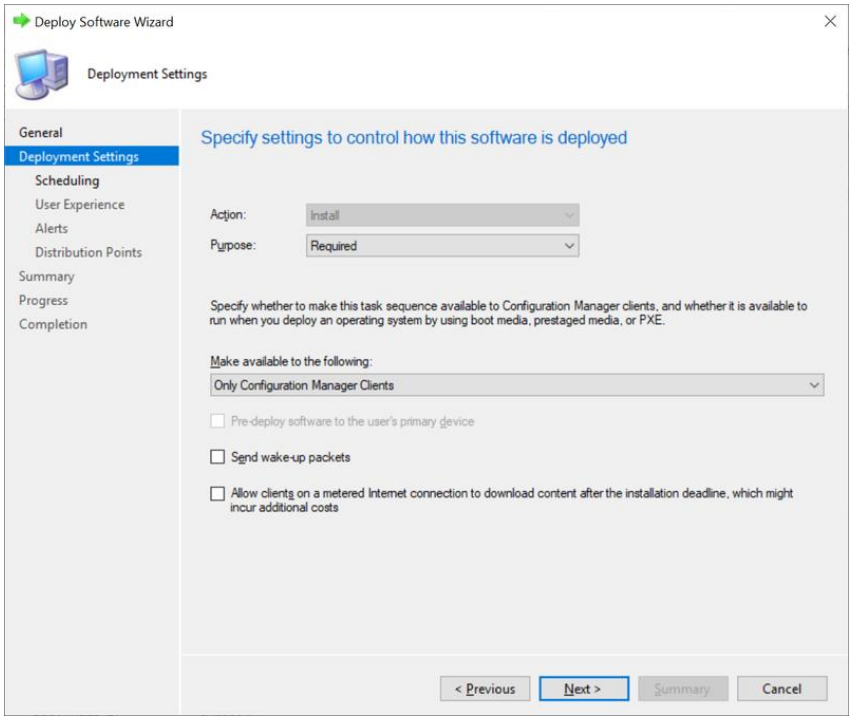


On the **Deployment Settings** page, change the purpose to **Required** and click **Next**.

On the **Scheduling** page, configure the assignment schedule according to your requirements and click **Next**.

On the **User Experience** page, uncheck **Show Task Sequence progress** and click **Next**.

On the **Alerts** page, click **Next**.



On the **Distribution Points** page under **Deployment options**, change the option to **Download all content locally before starting task sequence** is selected.

> This ensures that Nomad will download the PXE Everywhere boot image associated with the Task Sequence before executing the command lines to stage it in the TFTP folder.

Check the options:

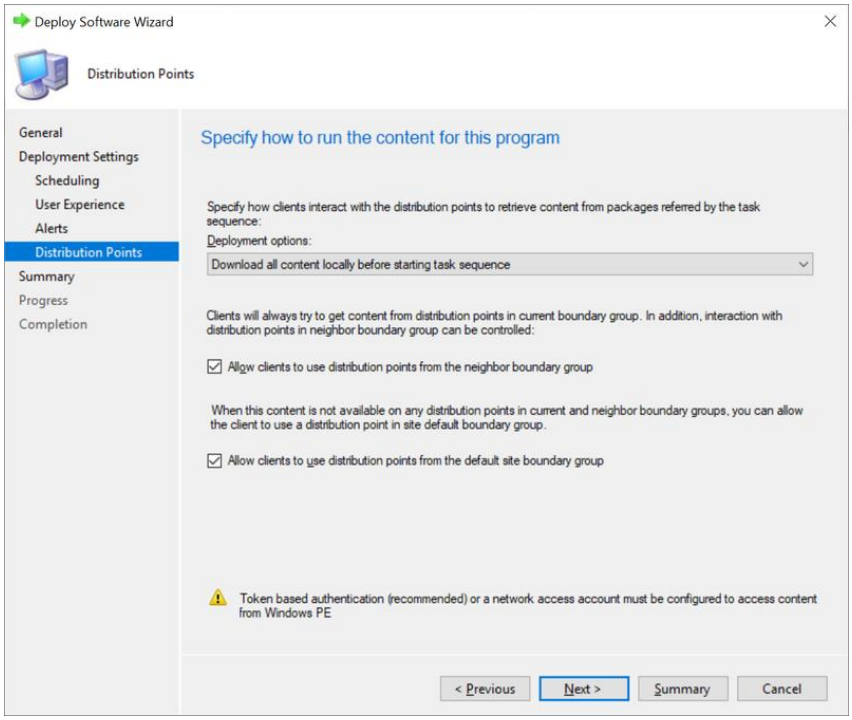
Allow clients to use distribution points from the neighbor boundary group

Allow clients to use distribution points from the default site boundary group

Click **Next**.

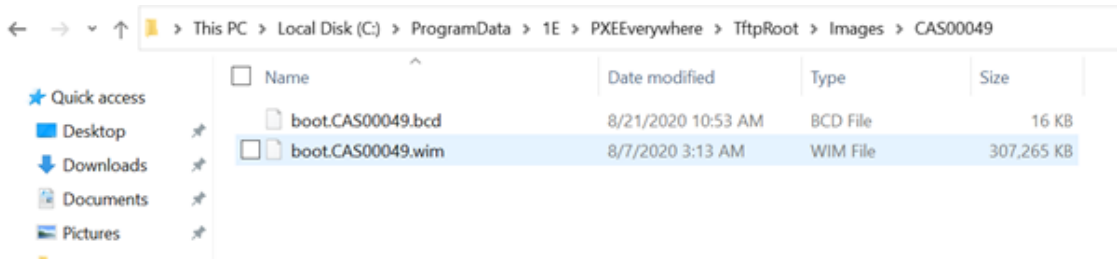
On the **Summary** page, click **Next**. When the wizard completes, click **Close**.

If you are serving x86 platforms, repeat the above steps to deploy **Stage 1E PXE Everywhere boot image (x86)**.



When Configuration Manager processes the Task Sequence on Agent computers, the associated boot image will be downloaded to the Nomad and CCM Client caches. The *CreateBCD.exe* utility copies the cached boot image file to the *C:\ProgramData\1E\PXEEverywhere\TFTPROOT\images* directory on the computer.

The picture opposite shows our example of the x64 image.



This PXE Everywhere Agent is now ready to serve the boot image to PXE clients.

Note

When PXE booting a UEFI device in a non-mandatory deployment scenario, you may be presented with an option to
Press Enter to continue and Press F8 for Advanced boot menu. However, the advanced boot menu options will not work for WinPE.

Please refer to Verifying for guidance on testing PXE Everywhere.

12.3.2 Deploying Microsoft ADK files

Steps for deploying Microsoft ADK files when not using 1E Client Deployment Assistant (CDA).

These steps are only required if you have installed PXE Everywhere Agent using the **1E Client** installer instead of using **1E Client Deployment Assistant (CDA)** which is the recommended method of including the Microsoft ADK files in the deployment of PXE Everywhere Agent.

A script similar to the one provided below was originally used for legacy versions of PXE Everywhere Agent and CDA which did not include the ADK files, and required the ADK files to be deployed as a post-installation task along with the 1E PXE Everywhere boot images.

12.3.2.1 Obtaining the Microsoft ADK files

In addition to the binaries supplied by 1E, PXE Everywhere Agent requires a number of files that are distributed and licensed with the Microsoft Windows Automated Deployment Kit (ADK).

As these files are licensed by Microsoft, 1E are unable to include them in the installation media. However, you can use the Introducing 1E Client Deployment Assistant to extract the required files from the ADK, create an installer transform and prepare an Application in Configuration Manager that will install the PXE Everywhere Agent with the appropriate settings and the additional Microsoft files.

The Windows Assessment and Deployment Kits (ADK) normally exist on the Configuration Manager CAS or Primary Site server, although they can be downloaded separately from the Microsoft website.

If you are not using CDA, then you must extract the files listed below from the Windows 10 ADK, and then deploy them to PXE Everywhere Agents.

boot.sdi

abortpxe.com

bootmgr.exe

pxeboot.com

pxeboot.n12

bootmgfw.efi

wgl4_boot.ttf

12.3.2.1.1 Script to extract the ADK files

The following example script can be used to extract the files from the Windows 10 ADK. It must be run on a standard Configuration Manager primary site server that has the Windows 10 ADK installed.

It extracts the required ADK files and copies them to the specified location.

If the script were saved as *ExtractADK.cmd* and you have created a folder called *C:\ADKFiles* to receive the extracted files, the command line syntax would be:

```
ExtractADK.cmd C:\ADKFiles
```

> **Note**
>
> The script assumes that ADK is installed in "C:\Program Files (x86)\Windows Kits\%WINVER%". For Windows 10, WINVER=10.

If you have ADK installed at in a different location then you will need to modify the script accordingly.

Click **Read more...** to view **ExtractADK.cmd** source or download the script Download ExtractADK.cmd...

```
 @ECHO OFF
IF %1.==. GOTO :INPUTERROR
SET TARGETPATH=%~dpn1
SET WINVER=10

call "C:\Program Files (x86)\Windows Kits\%WINVER%\Assessment and Deployment Ki
t\Deployment Tools\DandISetEnv.bat"

imagex /unmount "%tmp%\winpe"
rd "%tmp%\winpe" /s /q
md "%tmp%\winpe"
md "%TARGETPATH%\Boot"
md "%TARGETPATH%\Boot\x86"
md "%TARGETPATH%\Boot\x64"
md "%TARGETPATH%\Boot\Fonts"
REM Extract x86 files
imagex /mount "c:\Program Files (x86)\Windows Kits\%WINVER%\Assessment and Depl
oyment Kit\Windows Preinstallation Environment\x86\en-us\winpe.wim" 1 "%tmp%\wi
npe"

xcopy "C:\Program Files (x86)\Windows Kits\%WINVER%\Assessment and Deployment K
it\Windows Preinstallation Environment\x86\Media\Boot\boot.sdi" "%TARGETPATH%\"
/y
xcopy "C:\Program Files (x86)\Windows Kits\%WINVER%\Assessment and Deployment K
it\Windows Preinstallation Environment\x86\Media\Boot\Fonts\wgl4_boot.ttf" "%TA
RGETPATH%\Boot\Fonts\" /y
xcopy "%tmp%\winpe\Windows\Boot\PXE\abortpxe.com" "%TARGETPATH%\Boot\x86\" /y
xcopy "%tmp%\winpe\Windows\Boot\PXE\bootmgr.exe" "%TARGETPATH%\Boot\x86\" /y
xcopy "%tmp%\winpe\Windows\Boot\PXE\pxeboot.com" "%TARGETPATH%\Boot\x86\" /y
xcopy "%tmp%\winpe\Windows\Boot\PXE\pxeboot.n12" "%TARGETPATH%\Boot\x86\" /y
xcopy "%tmp%\winpe\Windows\Boot\EFI\bootmgfw.efi" "%TARGETPATH%\Boot\x86\" /y

imagex /unmount "%tmp%\winpe"
REM Extract x64 files
imagex /mount "c:\Program Files (x86)\Windows Kits\%WINVER%\Assessment and Depl
oyment Kit\Windows Preinstallation Environment\amd64\en-us\winpe.wim" 1 "%tmp%\
winpe"

xcopy "%tmp%\winpe\Windows\Boot\EFI\bootmgfw.efi" "%TARGETPATH%\Boot\x64\" /y

imagex /unmount "%tmp%\winpe"
GOTO DONE

:INPUTERROR
```

```
ECHO Please specify the path to where to create TFTPRoot files
ECHO.
ECHO Example: %0 C:\temp\pxebootfiles
ECHO.
GOTO :EOF

:DONE
CD /D %TARGETPATH%
```

12.3.2.2 Deploying the ADK files

The updated ADK files must be deployed to PXE Everywhere Agents, into their TFTPROOT directory, along with the 1E PXE Everywhere boot images.

Deploying 1E PXE Everywhere boot images is described in Preparing and deploying 1E PXE Everywhere boot images.

By default, TFTPROOT is %ALLUSERSPROFILE%\1E\PXEEverywhere\TftpRoot

The 1E PXE Everywhere boot images should be found in an \Images folder relative to TFTPROOT.

In addition to the binaries supplied by 1E, PXE Everywhere Agent requires a number of files that are distributed and licensed with the Microsoft Windows Automated Deployment Kit (ADK). The required files are listed in the table opposite, along with the location on the PXE Everywhere Agent that they need to be installed to.

File	Destination Location (relative to TFTPROOT)
boot.sdi	*\boot.sdi*
abortpxe.com	*\boot\x86\abortpxe.com*
bootmgr.exe	*\boot\x86\bootmgr.exe*
pxeboot.com	*\boot\x86\pxeboot.com*
pxeboot.n12	*\boot\x86\pxeboot.n12*
bootmgfw.efi	*\boot\x86\bootmgfw.efi*
\boot\x64\bootmgfw.efi	
wgl4_boot.ttf (optional)	*\boot\fonts\wgl4_boot.ttf*

12.4 Troubleshooting

A general methodology for investigating issues with PXE Everywhere, as well as identifying key issues and their resolutions.

For known issues relating to specific components, please refer to the respective troubleshooting pages:

Clients	Platform	Applications	Integration
1E Client	1E	Endpoint Automation	1E Core for ServiceNow
1E Client Deployment Assistant		Experience Analytics	1E ITSM Connect for ServiceNow
PXE Everywhere		Endpoint Troubleshooting	1E Service Catalog Connect for ServiceNow
		Writing 1E Instructions (1E SDK)	1E Virtual Assistant

12.4.1 1E Support contact details

12.4.1.1 Support Web portal

Maintenance support customers can log onto the 1E Support Web Portal at https://support.1e.com/ using the login details provided with their maintenance contract. This provides issue tracking, product hotfixes, and knowledge base articles related to each product.

12.4.1.2 Telephone support

Maintenance support customers can contact the technical support department at 1E through the following support numbers. Just phone the relevant number for your area, so your call can be routed quickly and efficiently to the correct support group:

US/Canada:	1-866-349-4032 (Toll-Free)
	1-917-339-2360 (Standard)
UK/Europe:	+44 (0)208 326 3499
India:	+91 120 402 4002
Australia:	+61 739 111 118

12.4.1.3 Email support

Maintenance customers can use the following email for additional support. Evaluation customers can also use this email with the temporary access code that is provided through customercare@1e.com as part of their evaluation.

support@1e.com

12.4.1.4 For customers evaluating Nomad and PXE Everywhere

If you are evaluating Nomad and PXE Everywhere, please contact 1E if you need guidance.

12.4.2 The technical support process

Read through the Troubleshooting pages to see if there are known issues, or quick resolutions to any problems you may have encountered.

Maintenance support customers can use the 1E Support Web Portal to review knowledge base articles and download hotfixes.

If still encountering problems, create a technical report (log files and details) and then contact the 1E technical support team.

12.4.2.1 Creating a technical report

If possible, please obtain the following details and log files before contacting 1E, to include in your technical report.

12.4.2.1.1 Version details

The OS, version number, and patch level for:

Tachyon Servers

1E Client

Configuration Manager - if used

Other 1E Server software, for example, Shopping, Nightwatchman, and WakeUp.

For Nomad and Shopping, please provide OS, version number, and patch level for:

Configuration Manager DPs

Nomad extensions used on Configuration Manager Consoles

ActiveEfficiency Server.

12.4.2.1.2 Environmental details

If there were any recent changes made to your configuration

The name of the machines, Configuration Manager Application and/or Package IDs for when the issue occurred

12.4.2.1.3 Problem details

When did the issue occur, ensure log files cover this period

The scope of the issue – did it affect a particular geographical location, group of users, or client machines

Details of any self-help troubleshooting steps you carried out

In the event of a service crash or if you are experiencing high CPU or memory usage, provide us with the dump file, event viewer logs, and traces. We will provide you with FTP details to upload these files.

12.4.2.2 Log files

PXE Everywhere component	Folder	Log file
1E Client	C:\ProgramData\1E\Client	1E.Client.log
PXE Everywhere Central	C:\ProgramData\1E\PXELite	WebService.log
PXE Everywhere Responder	C:\ProgramData\1E\PXEEverywhere	PXEEverywhereResponder.log
PXE Everywhere Agent	C:\ProgramData\1E\PXEEverywhere	PXEEverywhere.log

Please also refer to Upgrading PXE Everywhere: Name changes introduced in PXE Everywhere 4.0.

If the issue is related to PXELite boot media creation/updating using CreateBootImage.exe then please provide:

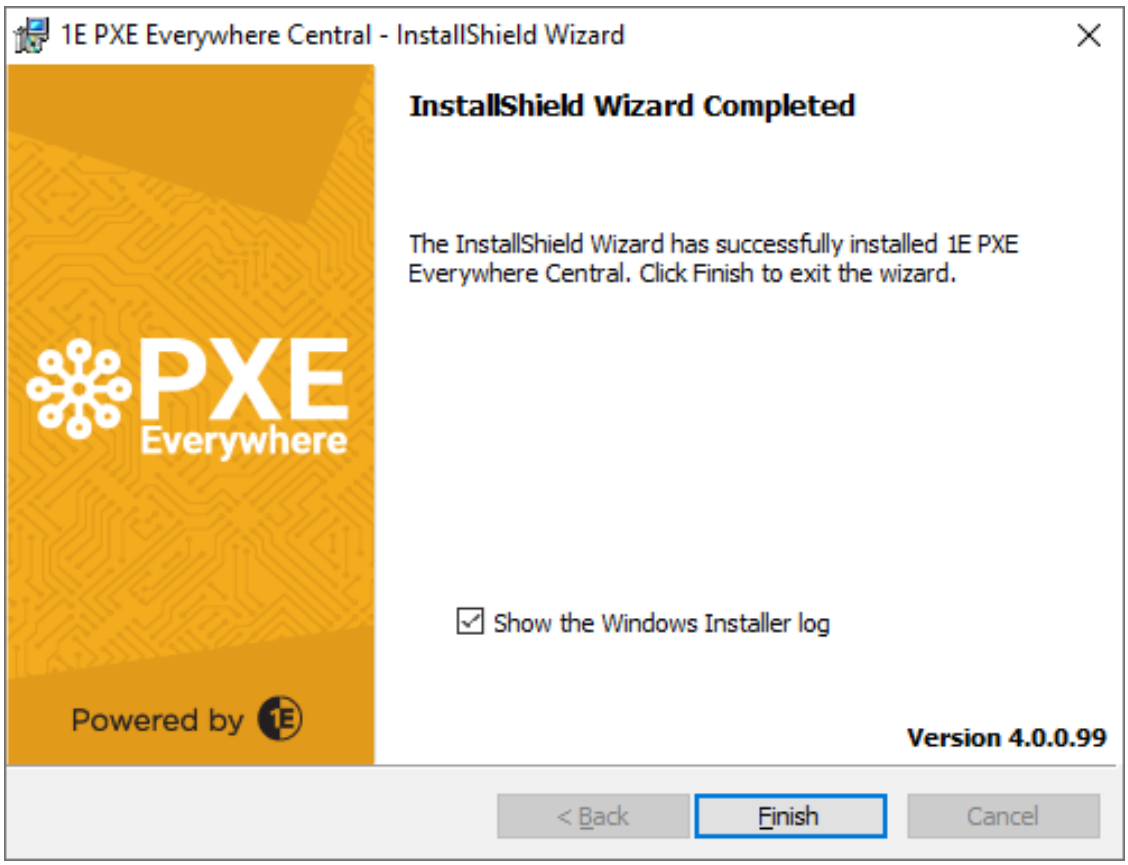
C:\Program Files (x86)\Microsoft Configuration Manager\AdminConsole\AdminUILog\CreateTsMedia.log

If the issue is related to the deployment of PXELite boot image into the TFTP folder of PXELite agent then please provide:

C:\ProgramData\1E\PXElite\CreateBCD.log

12.4.3 MSI Installer log

In case of problems during installation, each of the PXE Everywhere installers provide an option to view their installer log file at the end of the installation process. We recommend that you check the box and keep the log file handy until the installation has been validated. This way if there are any issues you can easily pass the installation log files on to the 1E Support department. Here is an example of the final page of the PXE Everywhere Central installer with the **Show the Windows Installer log** checkbox shown:



12.4.4 Known issues

Lists of the current known issues with implementing, configuring, using and upgrading PXE Everywhere.

If you need further help, please refer to the Troubleshooting page for how to contact 1E Support and the technical support process.

12.4.4.1 Issues using PXE Everywhere

Issue	Description	Workaround
UEFI PXE Boot Fails with error in the boot loader when a machine has more than one NIC	When machine has more than one Network Interface Card (NIC) and on performing PXE Boot from the secondary NIC card the PXE Boot will fail. This issue occurs only when you try boot from a NIC which is NOT the first NIC in the boot order.	If you boot from the first NIC the boot will complete without problem.

Issue	Description	Workaround
When Tftp session begins errors are noticed for file for which system cannot find the path specified	During PXE Boot UEFI firmwares requests few files however when not found boot still succeed.	These files are optional for the boot and not essential.
When a 1E PXE Everywhere boot image is created with blocksize values higher than 1471 bytes, TFTP transfers fail during PXE Boot	On Cisco and TPLink switches with DHCP Snooping enabled and block size value is higher than 1471 bytes PXE boot may fail. This is due a bug in the switch hardware itself. This issue does not occur when DHCP Snooping is off.	For details of how to change the block size used by TFTP, please refer to Preparing and deploying 1E PXE Everywhere boot images: TFTP Block Size.
CreateBCD.exe does not remove the *.prompt.bcd* files when it is re-run	The *boot.image_ID.prompt.bcd* and *boot.image_ID.prompt.bcd.LOG* files are not purged from the boot images under *TFTPROOT* when upgraded from previous versions.	Manually delete the log files.
Secure Boot won't work on Hyper-V (Gen-2) virtual machines.	PXE Booting Hyper-V (Gen-2) virtual machines with the Secure Boot option is not supported in PXE Everywhere.	None.
Command prompt crashes when arguments are passed to *UpdateBootImage.exe*	If you run a command prompt and pass arguments to *UpdateBootImage.exe*, it crashes the session.	Run the command prompt with elevated rights.
Create media fails when using UpdateBootImageGUI tool.	UpdateBootImageGUI does not throw an error when a site server is specified in the SMSProvider field which does not have a local SMS Provider. The command is generated successfully with the entered value of the site server name, however the create media fails.	
Temporary image file is left in the %temp% folder after UpdateBootImage.exe has executed successfully	During UpdateBootImage a temporary .WIM file is updated in %temp% folder. This image file is not deleted after a successful	Manually delete the image file.

Issue	Description	Workaround
	execution of UpdateBootImage.exe and can be removed manually.	

12.4.4.2 Issues installing PXE Everywhere Central

Issue	Description	Workaround
PXE Everywhere Central unattended installation succeeds even when prerequisites are not met.	PXE Central unattended installation creates an entry in Windows Program and Feature however, program files are not installed and the Web service is not created.	Ensure prerequisites are met when installing unattended.
While upgrading PXE Central to 3.2 or above from an older version where TLS 1.0 has been disabled, you get an exception - "Could not connect to Database"	While upgrading PXE Central to 3.2 or above from an older version TLS v1.0 has been disabled, you get an exception - "Could not connect to Database". You can ignore the error and click on ‘Next’ button, then installation would go through fine. That error occurs as a part of uninstallation of older version, when it tries to remove the stored procedures from DB. Since we don’t have TLS 1.2 support in old version, it fails to connect to DB.	Ignore the error and click on ‘Next’ button, then installation would go through fine.
After upgrading PXE Everywhere Central there are log files left in c:\programdata\1e\pxelite	From PXE Everywhere Central v4.0 onwards, the new default logpath is **c:\programdata\1e\pxeeverywhere**. The legacy logapth is **c:\programdata\1e\pxelite**. During upgrade the legacy log files are deliberately not deleted. This is partly to avoid contention with other legacy PXE Everywhere products installed on the computer, but also to avoid mixing old and new logs.	Manually delete the log files after all PXE Everywhere products have been upgraded.

12.4.4.3 Issues installing PXE Everywhere Responder

Issue	Description	Workaround

PXE Everywhere is not responding as expected. Log file shows messages similar to:
 	
`Error: failure to bind to 192.168.18228:69. The specified address is already in use`
`TFTP: retry in 1000ms`
`Error: failure to bind to 192.168.18228:4011. The specified address is already in use`
`DHCP: retry in 1000ms`
	PXE Everywhere Agent and PXE Everywhere Responder cannot co-exist on the same computer and are not supported together. Whilst it is possible to install them together, they will not work and will have issues such as failure to bind to ports.	Either uninstall PXE Everywhere Responder, or disable PXE Everywhere module in 1E Client. Then restart the computer, or restart the relevant service (PXE Everywhere or 1E Client).

Responder does not respond to Agents on port 67.	PXEEverywhereResponder.msi will upgrade legacy (3.2 or before) Responder and Agent if they exist, keeping the old registry settings. Upgrading a Responder will cause it to continue functioning as a Responder on port 67. Upgrading an Agent to a Responder will also allow it to function as a Responder, but if the Agent was previously configured to support DHCP Snooping then it will not be using port 67 and the Responder must be re-configured to use port 67.	Post-install fix is to reconfigure DhcpPort=67 on the Responder. Include DHCPPORT=67 as an installer property if you are upgrading legacy Agents to act as Responders.
After upgrading PXE Everywhere Responder there are log files left in c:\programdata\1e\pxelite	From PXE Everywhere Responder v4.0 onwards, the new default logpath is **c:\programdata\1e\pxeeverywhere**. The legacy logpath is **c:\programdata\1e\pxelite**. During upgrade the legacy log files are deliberately not deleted. This is partly to avoid contention with other legacy PXE Everywhere products installed on the computer, but also to avoid mixing old and new logs.	Manually delete the log files after all PXE Everywhere products have been upgraded.

12.4.4.4 Issues installing PXE Everywhere Agent in 1E Client

Issue	Description	Workaround

PXE Everywhere is not responding as expected. Log file shows messages similar to:
 	
`Error: failure to bind to 192.168.18228:69.`
`The specified address is already in use`
`TFTP: retry in 1000ms`
`Error: failure to bind to 192.168.18228:4011.`
`The specified address is already in use`
`DHCP: retry in 1000ms`
	PXE Everywhere Agent and PXE Everywhere Responder cannot co-exist on the same computer and are not supported together. Whilst it is possible to install them together, they will not work and will have issues such as failure to bind to ports.	Either uninstall PXE Everywhere Responder, or disable PXE Everywhere module in 1E Client. Then restart the computer, or restart the relevant service (PXE Everywhere or 1E Client).

PXE Everywhere Agent fails to connect to PXE Everywhere Central.	An incorrect URL has been specified during installation of PXE Everywhere Agent. The installer wizard does not validate the PXE Lite Central URL is provided during the PXE Lite Local GUI installation.	Ensure you specify the correct URL when installing PXE Everywhere Agent.
PXE Everywhere does not support RISC based architecture.	PXE Everywhere does not support RISC based architecture and therefore not able to PXE boot clients using RISC. For instance, architecture being used by Microsoft Surface Pro 10 LTE Models is ARM 64-BIT UEFI (11) which is a RISC architecture and *not* recognized by PXE Everywhere.	None.
PXE Everywhere Agent installation fails when an unprivileged user installs it after providing administrator credentials	PXE Everywhere Agent installation fails with error when an unprivileged user initiates PXE Everywhere Agent installation even after validating credentials after UAC prompt.	When installing the agent interactively, run the installer from a command prompt with elevated permissions.

Issue	Description	Workaround
(UAC prompted) for installation.		

12.4.5 Installation issues

Some issues when installing PXE Everywhere.

12.4.5.1 Log files

When you have issues, a first place to look is the log files.

PXE Everywhere component	Folder	Log file
1E Client	C:\ProgramData\1E\Client	1E.Client.log
PXE Everywhere Central	C:\ProgramData\1E\PXELite	WebService.log
PXE Everywhere Responder	C:\ProgramData\1E\PXEEverywhere	PXEEverywhereResponder.log
PXE Everywhere Agent	C:\ProgramData\1E\PXEEverywhere	PXEEverywhere.log

Please also refer to Upgrading PXE Everywhere: Name changes introduced in PXE Everywhere 4.0.

If the issue is related to PXELite boot media creation/updating using CreateBootImage.exe then please provide:

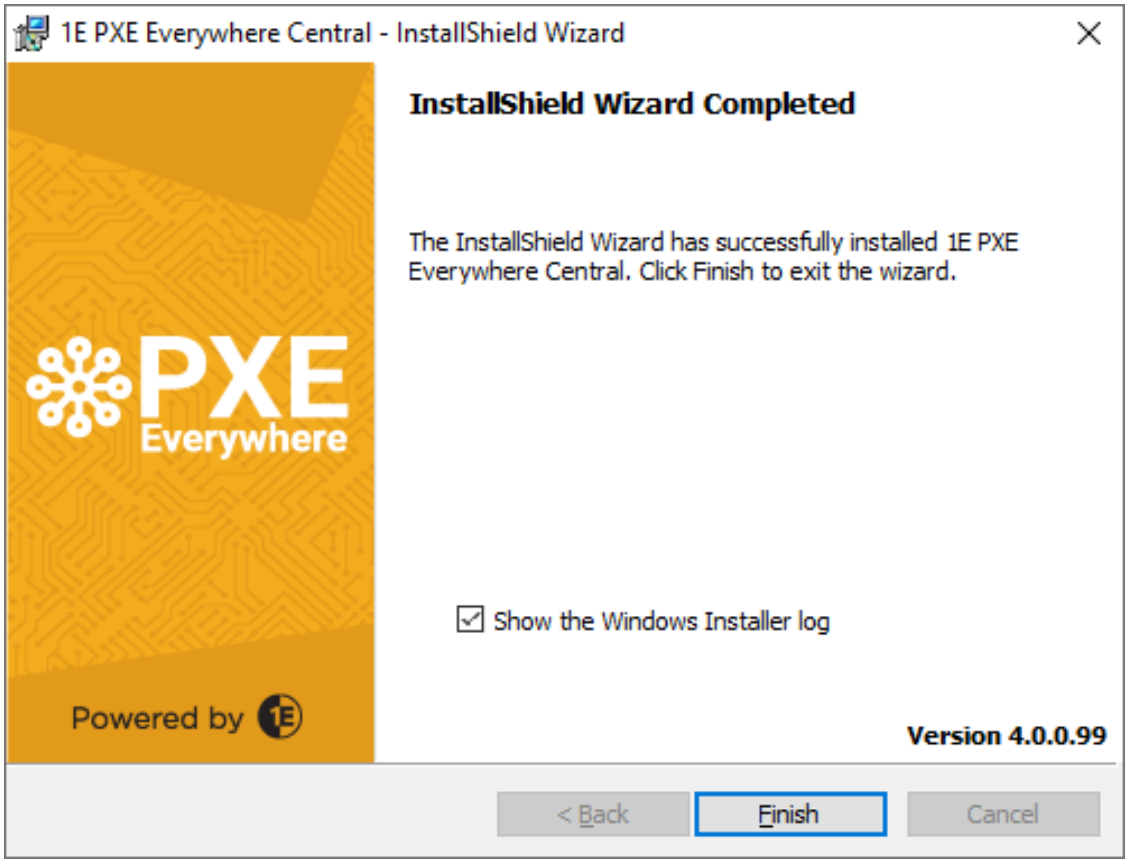
C:\Program Files (x86)\Microsoft Configuration Manager\AdminConsole\AdminUILog\CreateTsMedia.log

If the issue is related to the deployment of PXELite boot image into the TFTP folder of PXELite agent then please provide:

C:\ProgramData\1E\PXElite\CreateBCD.log

12.4.5.1.1 Windows Installer log

In case of problems during installation, each of the PXE Everywhere installers provide an option to view their installer log file at the end of the installation process. We recommend that you check the box and keep the log file handy until the installation has been validated. This way if there are any issues you can easily pass the installation log files on to the 1E Support department. Here is an example of the final page of the PXE Everywhere Central installer with the **Show the Windows Installer log** checkbox shown:



12.4.5.2 The installer takes 30 seconds (or more) to appear

Check to see if the computer has access to the Internet. The MSI files are digitally signed. This signature is verified during installation. Windows also checks to see whether the certificate used to generate the signature has been revoked. This requires Internet access, but will time out after 30 seconds.

Possible solutions are:

Allow this to happen. This does not affect the installation other than to delay by the time out period.

Connect the computer to the Internet.

Re-sign the MSI with your own key. Use one that is trusted by the computer, and does not need to access the Internet to find the certificate revocation list (CRL).

Please refer to Supported Platforms: Certificate limitations - signing certificates missing.

12.4.6 Resolving PXE Everywhere Agent issues

12.4.6.1 Legacy log files present after upgrading

After upgrading PXE Everywhere Central or PXE Everywhere Responder there are log files left in **c:\programdata\1e\pxelite**.

From PXE Everywhere v4.0 onwards, the new default logpath is **c:\programdata\1e\pxeeverywhere**. The legacy logpath is **c:\programdata\1e\pxelite**. During upgrade the legacy log files are deliberately not deleted. This is partly to avoid contention with other legacy PXE Everywhere products installed on the computer, but also to avoid mixing old and new logs. Please refer to Upgrading PXE Everywhere: Name changes introduced in PXE Everywhere 4.0.

You can manually delete the log files after all PXE Everywhere products have been upgraded.

12.4.6.2 Elections Not Working

A PXE Everywhere Agent responds to a PXE boot request and holds an election but no peer responds even though peers are present and the log looks like this:

```
PXEElection::hasResponse
Not replying to PXEClient DHCP DISCOVER from [18:03:73:28:53:34]
WARNING: Election timed out
Error hEvtDone 00000348 - The handle is invalid
DhcpListener::HandleRequest
```

This can happen for a number of reasons, but check that the firewall is not blocking the communications port used by PXE – for more detail please refer to PXE Everywhere Agent settings: CommsPort.

Furthermore, if the log file doesn't show any activity when you are PXE booting another local computer, check network access. Network features such as DHCP Snooping will prevent PXE Everywhere from being able to respond to PXE requests.

12.4.6.3 Bare-metal computer not able to PXE boot

In order to troubleshoot why a bare-metal computer is not PXE booting, open the PXE log file on the peer computer (that has PXE Everywhere installed) and look for a line similar to the following:

```
Configuration Service returned bootImageId = '', isMandatory = 0, clientSmbiosG
uid = '3119d64c-3540-11b2-a85c-c56de30503a2', clientMacAddress = '1E:1E:1E:CC:9
1:D8'
```

This log entry is the response back from PXE Central that describes what should be provided to the bare-metal computer, such as the Boot Image ID and if that is mandatory. If the Boot Image ID value is empty, then PXE Everywhere doesn't know what boot image to provide to the bare-metal computer. Ensure a Task Sequence (with associated boot image) has been correctly deployed to this bare-metal computer.

A failed PXE response - because their is no assigned boot image - looks like the following:

```
Completing MyElection Winner=PC0001 for=1E:1E:1E:CC:91:D8
Sending.. Election master PC0001(172.16.179.100) "1E:1E:1E:CC:91:D8" W=50ELCN
Election master from 172.16.179.100 Master=PC0001 for 1E:1E:1E:CC:91:D8
Configuration Service returned bootImageId = '', isMandatory = 0, clientSmbiosG
uid = '3119d64c-3540-11b2-a85c-c56de30503a2', clientMacAddress = '1E:1E:1E:CC:9
1:D8'
PxeResource::PxeResource xABORTx
ElectionMgr Removed 1E:1E:1E:CC:91:D8 from list
```

Another step is to ensure the correct boot image exists on the PXE Everywhere client computers.

The following log entries show that a boot image (for example PS10005E) has been correctly assigned to the bare-metal computer, but the PXE Everywhere client doesn't have the needed boot image pre-cached or available in the TFTPROOT folder. Ensure that you have distributed the boot image to the PXE Everywhere computers and executed the **CreateBCD.exe** tool. For more detail please refer to Preparing and deploying 1E PXE Everywhere boot images: Create a Task Sequence to stage a 1E PXE Everywhere boot image.

```
Client MAC:  1E:1E:1E:CC:91:D8
Client UUID: 3119d64c-3540-11b2-a85c-c56de30503a2
Client Arch: EfiBC (UEFI)
PxeResource::PxeResource
PxeElection::hasResponse PS10005E
WARNING: We are the master however we do not have the resource:'PS10005E'
Not replying to PXEClient DHCP DISCOVER from [1E:1E:1E:CC:91:D8]
```

12.4.6.4 PXE Central Web service is not accessible

If the PXE Everywhere Agent has been configured incorrectly, the PXE Everywhere Agent log will contain the following error:

```
PXEEverywhere Configuration endpoint: http://PXECENTRALSERVER/PXELite/PXELiteConfiguration.asmx

SOAP call failed: (null) 21/08/2020 20:02:10 816 (0x0330)

  Code:    29 (SOAP_HTTP_ERROR) (null) 21/08/2020 20:02:10 816 (0x0330)
```

If the PXE Web service on PXE Everywhere Central is not configured properly or is not running, the PXE Everywhere Agent log on the will contain the following error:

```
Code: -1 (Unknown)
```

Check the PXE Central installation. To resolve this, check that the PXE Web service URL is accessible and if it isn't:

Check that the PXE application pool is running in IIS

Check if there are any other issues preventing web access

12.5 Reference

All the reference information for PXE Everywhere.

12.5.1 Supported Platforms

A list of all the platforms supported by PXE Everywhere, and the software required to allow PXE Everywhere Central and Responders to be installed or to work.

Please refer to Common client requirements for details of **PXE Everywhere Agent** client module of the 1E Client.

Category	PXE Everywhere Central	PXE Everywhere Responder	Notes
Windows OS	Windows Server 2022 Windows Server 2019 Windows Server 2016	Windows Server 2022 Windows Server 2019 Windows Server 2016 Windows 10 CB 21H2 Windows 11 CB 21H2 Windows 10 CB 21H1 Windows 10 CB 20H2	**Will only install on** computers running one of these OS. **Note** Installing PXE Everywhere Central on domain controllers is not a supported configuration. **Note** A server OS is recommended for PXE Everywhere Responder.
Web servers	IIS 10	Not applicable.	For PXE Everywhere Central: You **must** have one of these Web server versions installed. The installer **must** be run on the system hosting the Web server as it deploys the PXELite website on it. Requires the following OS roles and features: Web Server (Web-Server) ASP.NET 4.5 or later (Web-Asp-Net45)
Runtime libraries	.NET Framework 4.8	Visual C++ 2013 Redistributable	You**must**have one of these .NET Framework versions installed to install PXE Everywhere Central PXE Everywhere Responder installer includes the redistributable package for Visual C++ 2013.

Category	PXE Everywhere Central	PXE Everywhere Responder	Notes
Boot Image OS	Windows Server 2022 Windows Server 2019 Windows Server 2016 Windows 10 CB 21H2 Windows 11 CB 21H2 Windows 10 CB 21H1 Windows 10 CB 20H2	Not applicable.	**UpdateBootImage.exe** is supported only on these client OS. The Admin Tools feature of the PXE Everywhere Central installer installs UpdateBootImage.exe , which uses the native Configuration Manager API used to generate boot media.
Configuration Manager	MECM CB 2303 MECM CB 2203 MECM CB 2111 MECM CB 2107 MECM CB 2103 MECM CB 2010	Not applicable.	You can install PXE Everywhere Central on a Configuration Manager site server, or on any other server with IIS installed and good connectivity to the Configuration Manager database, ideally equivalent to the connection the site server has to its database.

12.5.1.1 Constraints of Legacy OS

12.5.1.1.1

In this documentation, the following are referred to as legacy OS. Below are described some known issues for these OS.

1E does not provide support for 1E products on the following OS unless the OS is explicitly listed as being supported for a specific 1E product or product feature. This is because Microsoft has ended mainstream support for these OS or they are not significantly used by business organizations.

Windows XP *	**Windows Server 2003 ***
Windows Vista	**Windows Server 2008**
Windows 7	**Windows Server 2008 R2**
Windows 8.0	**Windows Server 2012**
Windows 8.1	**Windows Server 2012 R2**

> **Note**
>
> 1E Client 8.1 and later will not install on Windows XP and Windows Server 2003. Please contact 1E if you intend to continue using any of the other legacy OS. If you experience an issue, then please try replicating the issue on a supported OS.

For Microsoft product lifecycle details, please refer to https://support.microsoft.com/en-us/lifecycle/search.

12.5.1.1.2

Certificate limitations - expired root certificates

Ensure that your Root CA Certificates are up-to-date on clients and servers. The **Automatic Root Certificates Update** feature is enabled by default, but its configuration may have been changed or restricted by Group Policy **Turn off Automatic Root Certificates Update**.

If this GPO is enabled, then you will see *DisableRootAutoUpdate = 1 (dword)* in *HKLM\Software\Policies\Microsoft\SystemCertificates\AuthRoot.*

12.5.1.1.3

Certificate limitations - signing certificates missing

On Windows computers, the installation MSI files, and binary executable and DLL files of 1E software are digitally signed. The 1E code signing certificate uses a timestamping certificate as its countersignature. 1E occasionally changes its code signing certificate, and uses it for new releases and patches for older versions, as shown in the table(s) below.

Root Certificate Authorities are implicitly trusted to validate certificates, and their certificates must be correctly installed to do this. Your computers should already have the necessary **root CA** certificates installed, however this may have been prevented by your organization's security policies, or inability to connect to the

Internet, or they are legacy OS. In general this is not an issue because by default Windows allows software to be installed and run without validation, although you may see a warning or experience a delay. However, you *must* have relevant CA certificates installed if you are using 1E Client (which self-validates its own files), or your organization has applied more secure polices (for example UAC, AppLocker or SmartScreen).

Typical reasons for issues with signing certificate are:

If your organization has disabled **Automatic Root Certificates Update** then you must ensure the relevant **root CA** certificates are correctly installed on each computer

If computers do not have access to the Internet then you must ensure the relevant **root and issuing CA** certificates are correctly installed on each computer, numbered in the table(s) below.

The signature algorithm of the 1E code signing certificate is SHA256RSA. In most cases, the file digest algorithm of an authenticode signature is SHA256, and the countersignature is a RFC3161 compliant timestamp. The exception is on legacy OS (Windows XP, Vista, Server 2003 and Server 2008) which require the file digest algorithm of an authenticode signature to be SHA1, and a legacy countersignature.

12.5.2 Communication Ports

A list of communication ports used by PXE Everywhere. Useful, if needed, for network and device firewalls.

Although a computer with PXE Everywhere Agent installed can also be a PXE client, it cannot be both at the same time.

Component	Ports	Protocol	Direction	Usage	Configurable
Central	80	HTTP	Inbound	PXE Everywhere Agent communicating with the PXE Everywhere Central web application. Browser connections to the PXE Everywhere Central website to verify installation.	Yes, post-installation on the Central server, and during installation of Agents by configuring the URL. If HTTPS is required, please contact 1E for advice.

Component	Ports	Protocol	Direction	Usage	Configurable
Central	135 and 445 (initially)	WMI-DCOM TCP	Outbound	PXE Everywhere Central installer requires access to the Configuration Manager Site server, and to the server hosting the SMS Provider role. If there is only one SMS Provider, it is often on the Site server. In each case, TCP 135 and 445 are used to initiate communications and negotiate a dynamic RPC port. The dynamic range depends on the Windows OS version.	No.

Component	Ports	Protocol	Direction	Usage	Configurable
Central	1433	(See usage for protocol) TCP	Outbound	PXE Everywhere Central to access to the SQL database role for the selected Configuration Manager Site.	Depends on the Configuration Manager SQL Server instance. The Central installer determines the connection string by querying the Site's SMS Provider.
ConfigMgr Site Server (and SMS Provider)	135 and 445 (initially)	WMI (DCOM) TCP	Inbound	PXE Everywhere Central installer requires access to the Configuration Manager Site server, and each of the servers hosting the SMS Provider role. If there is only one SMS Provider, it is often on the Site server. In each case, TCP 135 and 445 are used to initiate communica	No.

Component	Ports	Protocol	Direction	Usage	Configurable
				tions and negotiate a dynamic RPC port. The dynamic range depends on the Windows OS version.	
ConfigMgr Site SQL database	1433	(See usage for protocol) TCP	Inbound	PXE Everywhere Central to access to the SQL database role for the selected Configuration Manager Site.	Depends on the Configuration Manager SQL Server instance.
Agent (1E.Client.exe)	80	HTTP TCP	Outbound	PXE Everywhere Agent communicating with the PXE Everywhere Central web application.	Yes, post-installation on the Central server, and during installation of Agents by configuring the URL. If HTTPS is required, please contact 1E for advice.
Agent (1E.Client.exe)	2012	UDP	Inbound & outbound	Election process inter-communication between PXE	Yes, during installation of PXE Everywhere Agents using the MODULE.PXEEVERYWHERE.COMMSPORT installer property.

Component	Ports	Protocol	Direction	Usage	Configurable
				Everywhere Agents on a subnet.	
Agent (1E.Client.exe)	67 or 2067	BOOTP UDP	Inbound	Port 67 is the standard PXE discover port. PXE clients use this port to broadcast PXE discovers on the local subnet. PXE Everywhere Agents listen on this port for PXE discovers that are broadcast on the local subnet. If PXE Everywhere is configured to support DHCP Snooping, Agents use a custom port (default 2067) to listen for	Only the DHCP Snooping ports are configurable, and must be the same on all Agents and Responders.

Component	Ports	Protocol	Direction	Usage	Configurable
				PXE requests, instead of standard port 67.	
Agent (1E.Client.exe)	68 or 2068	BOOTP UDP	Outbound	Port 68 is the standard PXE offer port. PXE Everywhere Agent uses this port to respond with offers to PXE discovers on the local subnet. If PXE Everywhere is configured to support DHCP Snooping, Agents use a custom port (default 2068) instead of the standard port 68.	Only the DHCP Snooping ports are configurable, and must be the same on all Agents and Responders.
Agent (1E.Client.exe)	69	TFTP UDP	Inbound	Port 69 is the standard	No.

Component	Ports	Protocol	Direction	Usage	Configurable
				PXE TFTP port. The PXE client downloads the boot image from the elected PXE Everywhere Agent using TFTP. This port is also used if PXE Everywhere is configured to support DHCP Snooping.	
Agent (1E.Client.exe)	4011	UDP	Inbound	Port 4011 is the standard PXE port used by PXE clients to communicate with a PXE Server after the initial discover / offer, to unicast a request for the location of the TFTP boot image file.	No.

Component	Ports	Protocol	Direction	Usage	Configurable
				This port is not used if PXE Everywhere is configured to support DHCP Snooping.	
Responder (PXEEverywhereResponder.exe)	67	BOOTP UDP	Inbound	Port 67 is the standard PXE discover port. A Responder is only required when DHCP Snooping is enabled, and listens for PXE requests from PXE clients on this port. See note below about DHCP Snooping and DHCP Relays.	No.
Responder (PXEEverywhereResponder.exe)	68	BOOTP UDP	Outbound	Port 68 is the standard PXE offer port. A Responder	No.

Component	Ports	Protocol	Direction	Usage	Configurable
				is only required when DHCP Snooping is enabled, and responds to PXE clients with offers unicast on this port. See note below about DHCP Snooping and DHCP Relays..	
PXE client	67	BOOTP UDP	Outbound	Port 67 is the standard PXE discover port. PXE clients use this port to broadcast PXE discovers on the local subnet. If DHCP Snooping is being used these discovers are forwarded to a Responder.	No.

Component	Ports	Protocol	Direction	Usage	Configurable
				See note below about DHCP Snooping and DHCP Relays. .	
PXE client	68	BOOTP UDP	Inbound	Port 68 is the standard PXE offer port. PXE Everywhere Agent broadcasts on this port with an offer in response to PXE discovers on the local subnet. If DHCP Snooping is being used, then Responders respond with offers on this port. See note below about DHCP Snooping and DHCP Relays..	No.
PXE client	69	BOOTP UDP	Outbound	Port 69 is the	No.

Component	Ports	Protocol	Direction	Usage	Configurable
				standard PXE TFTP port. A PXE client uses TFTP to download the boot image from the elected PXE Everywhere Agent on the local subnet. This port is also used if PXE Everywhere is configured to support DHCP Snooping.	
PXE client	4011	UDP	Outbound	Port 4011 is the standard PXE port used by PXE clients to unicast a request to the PXE Everywhere Agent for the location of the TFTP boot image file, after the initial	No.

Component	Ports	Protocol	Direction	Usage	Configurable
				discover/offer. This port is not used if PXE Everywhere is configured to support DHCP Snooping.	
PXE client	2067	BOOTP UDP	Outbound	If PXE Everywhere is configured to support DHCP Snooping, a custom port is used (default 2067) to perform a PXE request after the PXE client has downloaded a boot loader from a Responder. Only used if DHCP Snooping is being used, and PXE Everywhere has been	Yes. DhcpPort is configured during installation of Agents. AltPxeServerPort is manually configured on Responders.

Component	Ports	Protocol	Direction	Usage	Configurable
				configured to use this port.	
PXE client	2068	BOOTP UDP	Inbound	If PXE Everywhere is configured to support DHCP Snooping, a custom port is used (default 2068) to respond to a PXE request after the PXE client has downloaded a boot loader from a Responder. Only used if DHCP Snooping is being used, and PXE Everywhere has been configured to use this port.	Yes. AltPxeClientPort is manually configured on Responders.

Note

PXE client ports do not need to be configured on the OS firewall because it is the network interface which is doing the communicating. However you may need to configure intervening network firewalls for communication beyond the local subnet.

PXE Everywhere Responders communicate only with PXE clients; they do not communicate with PXE Central, PXE Everywhere Agents, other Responders, or Configuration Manager.

Note

If DHCP Snooping is enabled on networks, then DHCP Relays (IP helpers) must be configured to forward PXE requests (discovers) from client VLANs to specific Responders on port 67 and return the responses (offers) on port 68.

If DHCP Snooping is not enabled, then all PXE-boot traffic is on the local subnet, except for communication between the elected PXE Everywhere Agent and the PXE Everywhere Central server, and DHCP Relays are not required to forward PXE requests.

Note

Ports used by PXE clients to communicate with DHCP servers are not included in the above table. Communication with DHCP servers occurs before a PXE client PXE-boots, and typically use their own DHCP Relays (IP helpers).

Ports used by PXE clients to communicate with ConfigMgr Site systems are not included in the above table. Communication with ConfigMgr occurs only after a PXE client has downloaded the WinPE boot image (referenced in the deployed task sequence) from a local PXE Everywhere Agent, and booted into WinPE to start the Task Sequence.

Ports used by ConfigMgr Administrator workstations to communicate with ConfigMgr Site systems are not included in the above table. ConfigMgr Console extensions for PXE Everywhere Admin Tools use the same ports as ConfigMgr Console.

12.5.3 PXE Everywhere Central installer properties

Command-line installer properties that are available for an unattended installation for PXE Everywhere Central components.

Switch	Default value	Notes
CMSERVER		Mandatory. Sets the name of the Configuration Manager server
INSTALLDIR	C:\Program Files (x86)\1E\PXEEverywhere	The installation folder. PXE Everywhere Central is a 32-bit application, and is only supported on the 64-bit server OS.

Switch	Default value	Notes
INSTALLTYPE	COMPLETE	Type of installation. Values are: COMPLETE – installs the website, Configuration Manager database stored procedure and administration tools ADMINTOOLS – installs the administration tools only. A successful installation depends on Requirements being met.
LOGPATH	C:\ProgramData\1E\PXEEverywhere	The log folder used by the Web Service.

12.5.4 PXE Everywhere Responder settings

Configuration settings for PXE Everywhere Responder.

PXE Everywhere Responder is a 64-bit application, and its registry values exist under:
HKEY_LOCAL_MACHINE\SOFTWARE\1E\PXELiteServer

Note

Registry settings:

AltPxeClientPort | AltPxeServerPort | BindTo | Debug | DefaultBlockSize | DhcpPort | ElectionWaitSecs | ElectionWeight | EncryptionType | Flags | IgnoreGatewayAddress | IgnoreWireless | LogFileName | LogFormat | MaxLogFilesize | Mode | SessionTimeoutSecs | TftpRoot

Note

Installer properties:

DEBUG | DHCPPORT | ELECTIONWAITSECS | ELECTIONWEIGHT | USEFIPS | INSTALLDIR | LOGPATH | LOGFORMAT | MAXLOGFILESIZE | MODE | TFTPROOT

Registry name	Registry type	Installer property	Default value	Description
AltPxeClientPort	REG_DWORD	This value does not have an installer property.	Registry value is not created.	This is the UDP port that the PXE Everywhere Responder will reply to the PXE client

Registry name	Registry type	Installer property	Default value	Description
				(alternate boot loader) on. If this registry setting does not exist then port 2068 is used.
AltPxeServerPort	REG_DWORD	This value does not have an installer property.	Registry value is not created.	This is the UDP port that the alternate boot loader will broadcast the custom PXE request on. The PXE Everywhere Agents must be configured to listen on this port, so it must be the same port defined by DHCPPORT when installing the PXE Everywhere Agent. If this registry setting does not exist then port 2067 is used.
BindTo	REG_SZ	This value does not have an installer property.	Registry value is not created.	Comma-separated list of IP addresses which PXE Everywhere Responder listens for DHCP (PXE) and TFTP requests. If not present, PXE Everywhere Local listens on all IP addresses. Use this if there is more than

Registry name	Registry type	Installer property	Default value	Description
				one network interface.
Debug	REG_DWORD	**DEBUG**	1	The debug level. Leave this at *1* unless 1E Support recommends a change. The range is: *0x1*: Basic logging *0x4*: Extra "application-specific" logging *0x8*: Extra registry logging *0x10*: Increased general logging The following two bits will perform centralized logging via SOAP calls to the PXE Central Server: *0x1000*: Logs election results *0x2000*: Logs TFTP file transfer start and stop (includes statistics).
DefaultBlockSize	REG_DWORD	This value does not have an installer property.	Registry value is not created.	Default TFTP block size. 512 if not specified.

Registry name	Registry type	Installer property	Default value	Description
DhcpPort	REG_DWORD	**DHCPPORT**	67	For a new install, it is not necessary to use the DHCPPORT installer property on Responders, because DhcpPort must always be 67 (default). However, if you are upgrading a legacy PXE Everywhere Agent that has support for DHCP Snooping enabled, it will not be using DHCPPORT=67 and you will need to specify DHCPPORT=67 when upgrading it to be a Responder. If you are upgrading a legacy PXE Everywhere Responder (an Agent in Static Responder mode) to be a new PXE Everywhere Responder then it will retain DhcpPort=67 during the upgrade, and it is not necessary to use the DHCPPORT installer property.
ElectionWaitSecs	REG_DWORD	**ELECTIONWAITSECS**	1	Time (in seconds) to wait for responses

Registry name	Registry type	Installer property	Default value	Description
				to the election request before broadcasting the result. Can be any positive integer value above 0.
ElectionWeight	REG_DWORD	**ELECTIONWEIGHT**	50	When set, this manually created registry value determines the likelihood of the machine winning elections, all else being equal. The value must be between 0 and 99 inclusive. The higher the value the the higher the likelihood of winning. If no value is set, a default of 50 is used.
EncryptionType	REG_DWORD	**USEFIPS**	0	Use of FIPS compliant encryption for communications. You *must* use the same setting on all PXE Everywhere Agents. 0 – use default encryption 1 – use FIPS encryption

Registry name	Registry type	Installer property	Default value	Description
Flags	REG_DWORD	This value does not have an installer property.	Registry value is not created.	If set to ***1*** the DHCP listener adds an ASCII terminator character to the bootfile name in the DHCP acknowledgement message. Some HP machines require this. Any value other than **1** is treated as default 0.
IgnoreGatewayAddress	REG_DWORD	This value does not have an installer property.	Registry value is not created.	If set to any value other then ***0*** the DHCP listener ignores the gateway address. If not set then assumes default ***0*** .
IgnoreWireless	REG_DWORD	This value does not have an installer property.	0	If set to **1** then PXE Everywhere Agent does not bind on wireless adapters. Any value other than 1 is treated as default 0.
n/a		**INSTALLDIR**	%ProgramFiles%\1E\PXEEverywhere\Responder	Installation folder.
LogFileName	REG_SZ	**LOGPATH** **Note**	%ProgramData%\1E\PXEEverywhere\ PXEEverywhereResponder.log	The location of the PXE Everywhere Responder log file. The path is created if it does not exist.

Registry name	Registry type	Installer property	Default value	Description
		This property only specifies the location of the log file.		The logfile name is *PXEEverywhereResponder.log*
LogFormat	REG_DWORD	**LOGFORMAT**	1	Formatting depends on which bits are set: bit *0 (0x01)* use Configuration Manager-compatible format (default) bit *3 (0x08)* do no formatting bit *7 (0x80)* include milliseconds in the timestamp

Registry name	Registry type	Installer property	Default value	Description
MaxLogFilesize	REG_DWORD	**MAXLOGFILESIZE**	10485760	Maximum size for the log file in bytes. Once the file reaches the specified size, a copy is made with a *.lo_* extension in the same directory. A new log file will then be created. Default is 10485760 (10 MBytes).
Mode	REG_DWORD	**MODE**	3	Mode must be 3 – Responder mode
SessionTimeoutSecs	REG_DWORD	This value does not have an installer property.	Registry value is not created.	Timeout for the TFTP listener. 600 if not specified or 0 is specified. Can be any positive integer value.
TftpRoot	REG_SZ	**TFTPROOT**	*%ProgramData%\1E\PXEEverywhere\TftpRoot*	Location for the PXE Everywhere Responder *TFTPROOT* directory. **Warning** Do not change the location of TFTPROOT. If you need to do this then please

Registry name	Registry type	Installer property	Default value	Description
				contact 1E for guidance.

12.5.5 PXE Everywhere Agent settings

Installer and configuration settings for the PXE Everywhere Agent client module of the 1E Client supported only on Windows computers.

1E Client is available as 32-bit and 64-bit versions, and the correct version must be installed. This means the PXE Everywhere Agent registry location is the same for x86 and x64:

HKEY_LOCAL_MACHINE\SOFTWARE\1E\PXEEverywhere

Note

Registry settings:

AlwaysBootImageId | AlwaysIsMandatory | BindTo | CommsPort | ConfigServerAddress | Debug | DefaultBlockSize | DhcpPort | ElectionWaitSecs | ElectionWeight | EncryptionType | Flags | IgnoreGatewayAddress | IgnoreWireless | LogFileName | LogFormat | MaxBlockSize | MaxLogFilesize | Mode | ReserveSecs | SessionTimeoutSecs | TftpRoot

Note

Installer properties:

Module.PXEEverywhere.Enabled | MODULE.PXEEVERYWHERE.COMMSPORT | MODULE.PXEEVERYWHERE.CONFIGSERVERURL | MODULE.PXEEVERYWHERE.DEBUG | MODULE.PXEEVERYWHERE.DHCPPORT | MODULE.PXEEVERYWHERE.ELECTIONWAITSECS | MODULE.PXEEVERYWHERE.ELECTIONWEIGHT | MODULE.PXEEVERYWHERE.USEFIPS | MODULE.PXEEVERYWHERE.LOGPATH | MODULE.PXEEVERYWHERE.LOGFORMAT | MODULE.PXEEVERYWHERE.MAXLOGFILESIZE | MODULE.PXEEVERYWHERE.MODE | MODULE.PXEEVERYWHERE.RESERVESECS | MODULE.PXEEVERYWHERE.TFTPROOT

Note

Configuration file settings:

Module.PXEEverywhere.Enabled

12.5.5.1 PXE Everywhere Agent installation settings

This table lists the configuration settings visible in the PXE Everywhere screen during an interactive installation of the 1E Client. Other installer properties are available when using a command-line installation or a transform.

Note

You must use UPPERCASE when specifying the *name* of any installer property in a **mst** transform file, and preferably when including them in a msiexec command-line.

Names of settings stored in the configuration file are not case-sensitive. Setting names stored in the registry may be case-sensitive and should be specified as shown.

Settings that have numeric values must be set using decimal integers, unless otherwise specified.

Installer property	Mandatory	Default value	Description
Module.PXEEverywhere.Enabled	No	false	Set this property to **true** to enable the PXE Everywhere Agent client module. The default value is false. **Note** If enabled, when the 1E Client starts it will attempt to automatically remove any previous installations of PXE Everywhere Agent. This setting does not have an associated registry entry and is stored in the 1E Client configuration file.
MODULE.PXEEVERYWHERE.CONFIGSERVERURL	Yes	http://SERVER/PXELite/PXELiteConfiguration.asmx	URL for the PXE Everywhere Central web service in the format: *http://SERVER/PXELite/PXELiteConfiguration.asmx* where *<SERVER>* is the name of the server (or FQDN) where the PXE Everywhere Central web service is installed. **Note** The http prefix to the URL is case-sensitive and must be entered

Installer property	Mandatory	Default value	Description
			in all lower case letters. The URL is not verified by the installer, so you will need to ensure that the correct URL is entered. This setting has an associated ConfigServerAddress registry value.
MODULE.PXEEVERYWHERE.USEFIPS	No	0	You must use the same FIPS encryption setting on all PXE Everywhere Agents. Use of FIPS compliant encryption for communications. 0 – use default encryption 1 – use FIPS encryption This setting has an associated EncryptionType registry value.
MODULE.PXEEVERYWHERE.DHCPPORT	No	67	This installer property is set to 2067 if **Enable DHCP Snooping support** is checked during an interactive installation of the 1E Client installer. This is the UDP port on which the PXE Everywhere Agent will listen for PXE requests. If DHCP Snooping is not being used, then this port must be 67 (default), and you do not need to install Responders.

Installer property	Mandatory	Default value	Description
			When manually installing the PXE Everywhere Agent, if the DHCP Snooping option is enabled in the installer UI, the default port is changed from 67 (43 hex) to 2067 (813 hex). If the MODULE.PXEEVERYWHERE.DHCPPORT installer property is used to specify a port other than 67, the installer UI assumes the DHCP Snooping option is enabled. If DHCP Snooping is being used, then DhcpPort on Agents must be the same value as AltPxeServerPort on Responders. The default value of AltPxeServerPort is 2067. If a value other than 2067 is specified as a custom port number on Agents, you will also need to manually create the AltPxeServerPort (and AltPxeClientPort) registry values on Responders. This setting has an associated DhcpPort registry value.

12.5.5.2 PXE Everywhere Agent registry settings

This table lists all registry setting and their associated installer properties.

Note

You must use UPPERCASE when specifying the *name* of any installer property in a **mst** transform file, and preferably when including them in a msiexec command-line.

Names of settings stored in the configuration file are not case-sensitive. Setting names stored in the registry may be case-sensitive and should be specified as shown.

Settings that have numeric values must be set using decimal integers, unless otherwise specified.

Registry name	Registry type	Installer property	Mandatory	Default value	Description
AlwaysBootImageId	REG_SZ	This value does not have an installer property.	No	Registry value is not created.	A string value containing a valid package id of a boot image. If specified, do not get boot image ID from PXE Everywhere Central but use this one instead.
AlwaysIsMandatory	REG_DWORD	This value does not have an installer property.	No	Registry value is not created.	Whether the boot image is mandatory (value 1) or not (0). Only relevant in combination with *AlwaysBootImageId*.
BindTo	REG_SZ	This value does not have an installer property.	No	Registry value is not created.	Comma-separated list of IP addresses which PXE Everywhere Agent listens for DHCP (PXE) and TFTP requests. If not present, PXE Everywhere Local listens on all IP addresses. Use this if there is more than one network interface.
CommsPort	REG_DWORD	**MODULE.PXEEVERYWHERE.COMMSPORT**	No	2012	Used for UDP election broadcast messages, this must be opened in the Windows firewall.
ConfigServerAddress	REG_SZ	**MODULE.PXEEVERYWHERE.CONFIGSERVERURL**	Yes	http://SERVER/PXELite/PXELiteConfiguration.asmx	URL for the PXE Everywhere Central web service in the format:

Registry name	Registry type	Installer property	Mandatory	Default value	Description
					http://SERVER/PXELite/PXELiteConfiguration.asmx where *<SERVER>* is the name of the server (or FQDN) where the PXE Everywhere Central web service is installed. **Note** The http prefix to the URL is case-sensitive and must be entered in all lower case letters. The URL is not verified by the installer, so you will need to ensure that the correct URL is entered.
Debug	REG_DWORD	**MODULE.PXEEVERYWHERE.DEBUG**	No	1	The debug level. Leave this at *1* unless 1E Support recommends a change. The range is: *0x1*: Basic logging *0x4*: Extra "application-specific" logging *0x8*: Extra registry logging

Registry name	Registry type	Installer property	Mandatory	Default value	Description
					0x10: Increased general logging The following two bits will perform centralized logging via SOAP calls to the PXE Central Server: *0x1000*: Logs election results *0x2000*: Logs TFTP file transfer start and stop (includes statistics).
DefaultBlockSize	REG_DWORD	This value does not have an installer property.	No	Registry value is not created.	Default TFTP block size. 512 if not specified.
DhcpPort	REG_DWORD	**MODULE.PXEEVERYWHERE.DHCPPORT**	No	67	This is the UDP port on which the PXE Everywhere Agent will listen for PXE requests. If DHCP Snooping is not being used, then this port must be 67 (default), and you do not need to install Responders. When manually installing the PXE Everywhere Agent, if the DHCP Snooping option is enabled in the installer UI, the default port is changed from 67 (43 hex) to 2067 (813 hex). If the

Registry name	Registry type	Installer property	Mandatory	Default value	Description
					MODULE.PXEEVERYWHERE.DHCPPORT installer property is used to specify a port other than 67, the installer UI assumes the DHCP Snooping option is enabled. If DHCP Snooping is being used, then DhcpPort on Agents must be the same value as AltPxeServerPort on Responders. The default value of AltPxeServerPort is 2067. If a value other than 2067 is specified as a custom port number on Agents, you will also need to manually create the AltPxeServerPort (and AltPxeClientPort) registry values on Responders.
ElectionWaitSecs	REG_DWORD	**MODULE.PXEEVERYWHERE.ELECTIONWAITSECS**	No	1	Time (in seconds) to wait for responses to the election request before broadcasting the result. Can be any positive integer value above 0.
ElectionWeight	REG_DWORD	**MODULE.PXEEVERYWHERE.ELECTIONWEIGHT**	No	50	When set, this manually created registry value determines the

Registry name	Registry type	Installer property	Mandatory	Default value	Description
					likelihood of the machine winning elections, all else being equal. The value must be between 0 and 99 inclusive. The higher the value the the higher the likelihood of winning. If no value is set, a default of 50 is used.
EncryptionType	REG_DWORD	**MODULE.PXEEVERYWHERE.USEFIPS**	No	0	You must use the same FIPS encryption setting on all PXE Everywhere Agents.Use of FIPS compliant encryption for communications. 0 – use default encryption 1 – use FIPS encryption
Flags	REG_DWORD	This value does not have an installer property.	No	Registry value is not created.	If set to ***1*** the DHCP listener adds an ASCII terminator character to the bootfile name in the DHCP acknowledgment message. Some HP machines require this. Any value other than **1** is treated as default 0.acknowledgment
IgnoreGatewayAddress	REG_DWORD	This value does not have an installer property.	No	Registry value is not created.	If set to any value other than ***0*** the DHCP

Registry name	Registry type	Installer property	Mandatory	Default value	Description
					listener ignores the gateway address. If not set then assumes default ***0*** .
IgnoreWireless	REG_DWORD	This value does not have an installer property.	No	0	If set to **1** then PXE Everywhere Agent does not bind on wireless adapters. Any value other than 1 is treated as default 0.
LogFileName	REG_SZ	**MODULE.PXEEVERYWHERE.LOGPATH** **Note** This property only specifies the location of the log file.	No	%ALLUSERSPROFILE%\1E\PXEEverywhere PXEEverywhere.log	The location of the PXE Everywhere log file. The path is created if it does not exist. The logfile name is *PXEEverywhere.log*
LogFormat	REG_DWORD	**MODULE.PXEEVERYWHERE.LOGFORMAT**	No	1	Formatting depends on which bits are set: bit *0 (0x01)* use Configuration Manager-compatible format (default) bit *3 (0x08)* do no formatting bit *7 (0x80)* include milliseconds in the timestamp

Registry name	Registry type	Installer property	Mandatory	Default value	Description
MaxBlockSize	REG_DWORD	**Note** This value does not have an installer property, but is configurable when deployed using 1E Client Deployment Assistant. Please refer to Installing PXE Everywhere Agents: Preparing a Configuration Manager Application for PXE Everywhere Agent using the 1E Client Deployment Assistant.	No	Registry value is not created.	Maximum value for the block size (in bytes). PXE Everywhere uses the system MTU to derive the size of TFTP packets. May require limiting when using VPN tunnels. In most cases, this value should not be altered. Default is 8192 (8 kbytes). **Note** The actual block size used for the TFTP protocol is the lesser value of the **tftpBlockSize** and the **MaxBlockSize** registry values. The **tftpBlockSize** value is specified in the **CreateBCD.exe** utility command-line, and does not have a registry entry or installer property.

Registry name	Registry type	Installer property	Mandatory	Default value	Description
MaxLogFilesize	REG_DWORD	**MODULE.PXEEVERYWHERE.MAXLOGFILESIZE**	No	10485760	Maximum size for the log file in bytes. Once the file reaches the specified size, a copy is made with a *.lo_* extension in the same directory. A new log file will then be created. Default is 10485760 (10 MBytes).
Mode	REG_DWORD	**MODULE.PXEEVERYWHERE.MODE**	No	2	Mode must be one of the following: 0 – no elections 1 – the election instigator becomes the master (only to be used for testing) 2 – with elections (default)
ReserveSecs	REG_DWORD	**MODULE.PXEEVERYWHERE.RESERVESECS**	No	60	Time (in seconds) an election result remains active. 60 if not specified or 0 is specified. Can be any positive integer value.
SessionTimeoutSecs	REG_DWORD	This value does not have an installer property.	No	Registry value is not created.	Timeout for the TFTP listener. 600 if not specified or 0 is specified. Can be any positive integer value.

Registry name	Registry type	Installer property	Mandatory	Default value	Description
TftpRoot	REG_SZ	**MODULE.PXEEVERYWHERE.TFTPROOT**	No	*%ALLUSERSPROFILE%\1E\PXEEverywhere\TftpRoot*	Location for the PXE Everywhere Agent *TFTPROOT* directory. If you change the location of *TFTPROOT*, you need to change the location that you copy the additional PXE boot files to.

12.5.6 PXE Everywhere tools

Reference for command-line options used by 1E tools. These tools are used for Preparing and deploying 1E PXE Everywhere boot images.

1E tool	Where to find it	What it does
UpdateBootImage	Included in the PXE Everywhere Admin Tools. The PXE Everywhere Admin tools can be installed using the PXE Everywhere Central installer, on any computer that has the Configuration Manager Admin Console. Please refer to Installing PXE Everywhere Central. The PXE Everywhere Central installer is provided in the **PXE Everywhere download zip** available from the Nomad download area of the 1E Support Portal.	This tool is used to update Windows PE boot images for use with PXE Everywhere. It uses the native Configuration Manager API to add a certificate, and update the **variables.dat** file included in the image. When the PXE client loads the boot image, the Configuration Manager executables load the encrypted variables file and attempt to connect to the specified Management Point. The tool takes advantage of a boot image reload feature introduced in Configuration Manager 1706 CB, which enables you reload the latest version of Windows PE (from the Windows ADK installation directory) into the boot image when you run the **Update Distribution Points** wizard. **Note** Whenever you reload the boot image while running the **Update Distribution Points** wizard, for example to replace a certificate

1E tool	Where to find it	What it does
		that is about to expire, you must then re-run **UpdateBootImage.exe** to ensure the 1E components and settings are installed in the reloaded boot image. **Note** To include a client certificate, it must be provided as a PFX file in a Public Key Certificate Standard (PKCS #12) format, with private key exportable, and a known password. For details of CM certificates please refer to **Boot images for deploying operating systems** in PKI certificate requirements for System Center Configuration Manager (https://docs.microsoft.com/en-us/mem/configmgr/core/plan-design/network/pki-certificate-requirements.
UpdateBootImage GUI	Included in the **PXE Everywhere download zip** with the installers for PXE Everywhere Central and Responder. **Note** Use v1.0.0.6 with PXE Everywhere 4.0	This tool provides a GUI where a user defines the parameters required by the **UpdateBootImage** tool. When executed it copies a command-line to the clipboard, which you then copy into an elevated command prompt and execute it. The tool is provided to reduce the chance of errors when typing in the long command-line required by the UpdateBootImage tool. The executable name is **1E.PS.UpdateBootImageGUI.exe** and requires .NET Framework 4.5 or later.
CreateBCD	Included in the installation of **1E Client** with PXE Everywhere enabled.	This tool is run by a **Stage boot image** Task Sequence on PXE Everywhere Agents to copy the 1E PXE Everywhere boot image referenced by the Task Sequence to the Images folder in the Agent's TFTPTOOT, configure a suitable

1E tool	Where to find it	What it does
		TFTP Block Size, and create a boot configuration database on the Agent. CreateBCD only works within the context of a Configuration Manager task sequence. It will run outside a Task Sequence but have no effect. **Warning** **CreateBCD** does not validate the boot image - it will not detect a corrupt .wim file.

12.5.6.1 UpdateBootImage

This tool is used to update Windows PE boot images for use with PXE Everywhere. It uses the native Configuration Manager API to add a certificate, and update the **variables.dat** file included in the image. When the PXE client loads the boot image, the Configuration Manager executables load the encrypted variables file and attempt to connect to the specified Management Point.

The format of the command-line is as follows:

```
UpdateBootImage.exe [-parameter=value]
```

The following table shows command-line parameters and their description.

Parameter	Required / Optional	Description
BootImageID	Required	The package ID of the PXE Everywhere boot image, as created above.
CertExpiry	Optional	Used to define the Certificate expiration in days, Default = 365 (1 Year), minimum of 1 day is enforced. **Note** CertExpiry is only needed for self-signed certificates. It is not needed for PKI certificates.
CertPassword	Required (HTTPS only)	The password used when the .PFX file was exported earlier from the MP, so that it can be imported into the boot image. Only required if using the HTTPS protocol.

Parameter	Required / Optional	Description
CertPath	Required (HTTPS only)	The full path of the .PFX file exported earlier, so that it can be imported into the boot image. Only required if using the HTTPS protocol.
DistributionPoints	Required	A distribution point where the newly created PXE boot image has been distributed. The FQDN of the distribution point can be used and this must match the Server Name used to create the Site System Server.

ManagementPoints	Required	This parameter is used to create boot media that span multiple sites/management points. This should be set to a list of FQDN for all possible management points separated by the * character. This parameter is required for creating PXE Everywhere boot media in Configuration Manager.
		
		For single Primary Site environments, use the static based media option, SMSTSMP, for example:
		
		`-ManagementPoints=SMSTSMP=http://mp.contoso.com`
		
		For multi-site hierarchies, use the dynamic media option, SMSTSLocationMPs and specify at least one MP from each site, for example:
		
		`-ManagementPoints=SMSTSLocationMPs=`
		`http://site1MP.consoto.com*`
		`http://site2MP.contoso.com`

MediaPassword	Optional	The password applied to protect the media – recommended if deploying to Unknown Computers.
ProviderName	Required	Usually the name of the Configuration Manager server that hosts the "SMS Provider" role.
SiteCode	Required	Configuration Manager site code.
WIMFileName	Required	The filename of the boot WIM that you created above.

12.5.6.2 CreateBCD

This tool is run by a **Stage boot image** Task Sequence on PXE Everywhere Agents to copy the 1E PXE Everywhere boot image referenced by the Task Sequence to the Images folder in the Agent's

TFTPTOOT, configure a suitable TFTP Block Size, and create a boot configuration database on the Agent.

CreateBCD only works within the context of a Configuration Manager task sequence. It will run outside a Task Sequence but have no effect.

The format of the the command-line is as follows:

```
CreateBCD.exe [-parameter=value]
```

The following table shows command-line parameters and their description.

Option	Required / Optional	Description
-tftpBlocksize=*blocksize*	Optional	Sets the RAMDisk tftp blocksize in bytes.

TFTP Block Size

Some hardware may not support block size values higher than 16384 bytes and hence may fail to PXE boot. We recommend you use a TFTP block size of 8192 bytes for best results.

An known issue has been observed on some Cisco switches when DHCP Snooping is enabled and a block size greater than 1471 is used. The issue is referenced in the following two Cisco bug reports. If you are affected by this Cisco issue, change the tftpBlockSize to 1471 or lower.

https://quickview.cloudapps.cisco.com/quickview/bug/CSCvk53444.

https://quickview.cloudapps.cisco.com/quickview/bug/CSCtw63707

The issue may also be present in TP-Link switches.

The actual block size used for the tftp protocol is the lesser value of the **tftpBlockSize** and the **MaxBlockSize** registry values. Effectively, **MaxBlockSize** limits the **tftpBlockSize** specified in the **CreateBCD.exe** utility.

There is only one command-line switch for **CreateBCD.exe** which is used to set the **tftpBlockSize** for the RAMDisk (boot image). The notation for this is *`CreateBCD.exe -tftpBlocksize=blocksize`* where blocksize is measured in bytes.

12.5.7 PXE Everywhere release information

12.5.7.1 PXE Everywhere 8.1 release information – last updated 11-August-2022

These release notes contain late-breaking information about PXE Everywhere that you need to have to successfully install and use the product. For the most up-to-date information, see the online release notes and Known issues.

12.5.7.1.1 New Features in PXE Everywhere 8.1

12.5.7.1.1.1 PXE Everywhere Central

Now requires .NET Framework 4.8

No other features or feature changes added in this release, but includes any hotfixes from previous versions.

12.5.7.1.1.2 PXE Everywhere Responder

No features or feature changes added in this release, but includes any hotfixes from previous versions.

12.5.7.1.1.3 PXE Everywhere Agent

PXE Everywhere Agent is a client module of 1E Client 8.1, available for x64 and x86 platforms

There are no other changes in this version other than hotfixes.

12.5.7.1.2 Online help

PXE Everywhere comes with online help that shows you how to install, configure and use the product. Click the following link to view the help:

PXE Everywhere documentation

For support queries, please:

Use https://support.1e.com/ where you can search the KB or submit a support case.

Contact support@1e.com.

12.5.7.1.3 Known issues

The current known issues related to the installation and running of PXE Everywhere can be found in the Troubleshooting Known issues page of the PXE Everywhere documentation.

12.5.7.2 PXE Release History

12.5.7.2.1 8.1.2.8 11 Mar 2022 Minor Release

New features:

PXE Everywhere Agent is a client module of 1E Client 8.1, available for x64 and x86 platforms.

There are no changes in this version other than hotfixes.

Contains fixes:

Q22058 - PXE Everywhere - Log4Net Vulnerability - CVE-2018-1285 (TFS 249422)

12.5.7.2.2 8.0.4.10 19 Oct 2021 Major Release

New features:

PXE Everywhere Agent is a client module of 1E Client 8.0, available for x64 and x86 platforms.

There are no changes in this version other than hotfixes.

Contains fixes:

Q21606 - Standardize Nomad date logging (TFS 231355)

12.5.7.2.3 4.0.100.22 3128 Jul 2020 Maintenance Release

New features:

PXE Everywhere Agent is now a client module of 1E Client 5.2 available for x64 and x86 platforms

Contains fixes:

Q21141 - PXE boot fails when the windows firewall is enabled (TFS 212739)

Q21358 - PXE boot may fail if multiple network cards are present in the system (TFS 215056)

Q21328 - Enabling the PXE Module in the 1E Client 5.1 creates an additional 1E.Client.log in C:/Temp folder (TFS 218205)

12.5.7.2.4 4.0.0.99 28 Jul 2020 Major Release

New features:

PXE Everywhere Agent is now a client module of 1E Client 5.1 available for x64 and x86 platforms

PXE Everywhere Static Responder (to support DHCP Snooping) now has its own installer

PXE Everywhere replaces PXELite name

UpdateBootImageGUI is included in the PXE Everywhere download zip

Contains fixes:

Q20742 - PXE Boot fails on Microsoft Surface Pro systems (TFS 195659)

Q20475 - UpdateBootImage.exe fails with Configuration Manager 1902 (TFS 175421)

12.5.7.2.5 3.2.0.56 20 Mar 2019 Major Release

New features:

Support for networks with DHCP Snooping enabled

Contains fixes:

Q20241 - Reusing the same NIC for multiple PXE initiated deployments in System Center Configuration Manager OSD (TFS - 26469)

Q20241 - PXE Central install does not function properly with ConfigMgr CAS database (TFS - 133118)

Q20241 - PXE Central does not provide BootID to devices where Unknown0=1 (TFS - 127155)

Q20235 - PXE Everywhere answers election requests on non-preferred network (TFS - 133541)

Q20235 - PXE Everywhere is not RFC 4578 compliant which may be causing PXE Boot failures (TFS - 143777)

Q20235 - PXE Agent licensing changes (TFS - 142988)

PXE Server returns the wrong adapter's IP in DHCP messages (TFS - 171559)

12.5.7.2.6 3.1.300.521 Mar 2017 Maintenance Release

Enhancements:

Support for Windows Server 2016

Support for Configuration Manager CB 1606 and CB 1610

12.5.7.2.7 3.1.200.4 02 Sep 2016 Maintenance Release

General enhancements

Contains fixes:

CreateBCD.exe filling-up Tftproot with all contents of C: (TFS - 53617)

12.5.7.2.8 3.1.100.46309 26 May 2016 Minor Release

Enhanced handling of PXE boots for machines that do not comply to the standard PXE protocol

Contains fixes:

PXE Everywhere service stops unexpectedly (TFS - 20300)

PXE Everywhere local host registry value "BindTo" does not work (TFS - 37665)

PXELite local consuming high CPU cycles on PCs and laptops (TFS - 42964)

12.5.7.2.9 3.0.0.9 10 Aug 2015 Major Release

New features:

Full compliance with Federal Information Processing Standards (FIPS)

Full support for Unified Extensible Firmware Interface (UEFI) devices.

Support for ConfigMgr 2012 SP2, ConfigMgr 2012 R2 SP1, Windows 10 and Windows Server 2012 R2

12.5.7.3 PXE Everywhere features by release

A list of features organized by the release they were implemented in. Links through to the features are provided for convenience.

12.5.7.3.1 New in PXE Everywhere 8.1

12.5.7.3.1.1 PXE Everywhere Central

Now requires .NET Framework 4.8

No other features or feature changes added in this release, but includes any hotfixes from previous versions.

12.5.7.3.1.2 PXE Everywhere Responder

No features or feature changes added in this release, but includes any hotfixes from previous versions.

12.5.7.3.1.3 PXE Everywhere Agent

PXE Everywhere Agent is a client module of 1E Client 8.1, available for x64 and x86 platforms

There are no other changes in this version other than hotfixes.

12.5.7.3.2 PXE Everywhere 8.0 features

12.5.7.3.2.1 PXE Everywhere Central

No features or feature changes added in this release, but includes any hotfixes from previous versions.

12.5.7.3.2.2 PXE Everywhere Responder

No features or feature changes added in this release, but includes any hotfixes from previous versions.

12.5.7.3.2.3 PXE Everywhere Agent

PXE Everywhere Agent is a client module of 1E Client 8.0, available for x64 and x86 platforms

Bootshim.efi folder renamed from **BootPrograms** to **NetworkBootPrograms** (1E\Client\Extensibility\PXEEverywhere\NetworkBootPrograms)

There are no other changes in this version other than hotfixes.

12.5.7.3.3 PXE Everywhere 4.0 features

This 4.0.100 maintenance release contains the following new features:

PXE Everywhere Agent is now a client module of 1E Client 5.2, available for x64 and x86 platforms.

The main 4.0 release introduced the following new features:

PXE Everywhere Agent is now a client module of 1E Client 5.1 available for x64 and x86 platforms.

PXE Everywhere Responder (used to support DHCP Snooping) now has its own installer to replace Static Responder mode of the Agent, as described in Installing PXE Everywhere Responder, and has been recompiled as x64 instead of x86.

PXE Everywhere has replaced PXELite name throughout the product, with a few exceptions:

The PXE Everywhere website and Application Pool is still called **PXELite**

The registry root for PXE Everywhere Central is still **PXELiteCentral**

The registry root for PXE Everywhere Responder is still **PXELiteServer**.

UpdateBootImageGUI is included in the PXE Everywhere download zip.

12.5.7.3.4 PXE Everywhere 3.2 features

Introducing the Static Responder mode of PXE Everywhere Agent to support networks with DHCP Snooping enabled

12.5.7.3.5 PXE Everywhere 3.1 features

Support for Windows Server 2016

Support for Configuration Manager Current Branch

12.5.7.3.6 PXE Everywhere 3.0 features

Enhanced handling of PXE boots for machines that do not comply to the standard PXE protocol

Compliance with Federal Information Processing Standards (FIPS)

Support for Unified Extensible Firmware Interface (UEFI) devices.

Support for Configuration Manager 2012 SP2, Configuration Manager 2012 R2 SP1, Windows 10 and Windows Server 2012 R2

12.5.7.3.7 PXE Everywhere 2.3 features

Support for UEFI devices. There is a known limitation for this feature where non-mandatory deployments do not time-out. This would occur in an uncommon configuration where machines were configured so that the NIC card was the first device in the boot order. 1E is aware of the administrative challenge caused by this issue and the problem will be addressed in the next PXE Everywhere release, scheduled for Q2 2015.

12.5.7.3.8 PXE Everywhere 2.2 features

Support for Configuration Manager 2012 R2, Windows 8.1 and Windows Server 2012 R2

Support for setting RAMDisk (boot image) TFTP blocksize - new configurable **tftpblocksize** option in the **CreateBCD.exe** component

> **Note**
>
> This version addresses a vulnerability in the PXE Everywhere Local Host's use of Trivial File Transfer Protocol (FTFP). In earlier versions the TFTP server running on the remote host was vulnerable to a directory traversal attack that could have allowed an attacker to read arbitrary files on the remote host by pre-pending their names with directory traversal sequences. If you are running PXE Everywhere Local Host v2.1 in your environment, we recommend you upgrade all end-points to the latest version of the PXE Everywhere Local Host at your earliest convenience.

12.5.7.3.9 PXE Everywhere 2.1 features

Configuration Manager 2012 SP1 support

Windows 8 and Windows Server 2012 support

Boot image certificate expiration – new configurable option in the UpdateBootImage component

12.5.7.3.10 PXE Everywhere 2.0 features

Configuration Manager 2012 integration – the new version of PXE Everywhere integrates with Configuration Manager 2012 to apply boot images to PXE-booting bare metal machines.

Multiple PXE Everywhere Local Hosts – the new version of PXE Everywhere enables PXE support on all computers on a subnet which elect the most suitable host when a PXE boot request comes in.

Nomad integration – PXE Everywhere, in conjunction with Nomad, helps minimize WAN usage by ensuring that locally cached Packages are used wherever possible when deploying OS images.

12.5.8 Log files

Names and locations of log files created by PXE Everywhere components.

PXE Everywhere component	Folder	Log file
1E Client	C:\ProgramData\1E\Client	1E.Client.log
PXE Everywhere Central	C:\ProgramData\1E\PXELite	WebService.log
PXE Everywhere Responder	C:\ProgramData\1E\PXEEverywhere	PXEEverywhereResponder.log
PXE Everywhere Agent	C:\ProgramData\1E\PXEEverywhere	PXEEverywhere.log

Please also refer to Upgrading PXE Everywhere: Name changes introduced in PXE Everywhere 4.0.

If the issue is related to PXELite boot media creation/updating using CreateBootImage.exe then please provide:

C:\Program Files (x86)\Microsoft Configuration Manager\AdminConsole\AdminUILog\CreateTsMedia.log

If the issue is related to the deployment of PXELite boot image into the TFTP folder of PXELite agent then please provide:

C:\ProgramData\1E\PXElite\CreateBCD.log